

Cisco Secure Firewall ASA Series Command Reference, A-H Commands

First Published: 2005-05-31

Last Modified: 2026-10-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface

This chapter describes how to use the CLI on the Secure Firewall ASA and includes the following sections:

Note The CLI uses similar syntax and other conventions to the Cisco IOS CLI, but the ASA operating system is not a version of Cisco IOS software. Do not assume that a Cisco IOS CLI command works with or has the same function on the ASA.

- Firewall Mode and Security Context Mode, on page 2
- Command Modes and Prompts, on page 3
- Syntax Formatting, on page 5
- Abbreviating Commands, on page 6
- Command-Line Editing, on page 7
- Command Completion, on page 8
- Command Help, on page 9
- Viewing the Running Configuration, on page 10
- Filtering show and more Command Output, on page 11
- Redirecting and Appending show Command Output , on page 12
- Getting a Line Count for show Command Output, on page 13
- Command Output Paging, on page 14
- Entering Numeric Values, on page 15
- Adding Comments, on page 16
- Text Configuration Files, on page 17
- Supported Character Sets, on page 19

Firewall Mode and Security Context Mode

The ASA runs in a combination of the following modes:

- Transparent firewall or routed firewall mode

The firewall mode determines if the ASA runs as a Layer 2 or Layer 3 firewall.

- Multiple context or single context mode

The security context mode determines if the ASA runs as a single device or as multiple security contexts, which act like virtual devices.

Some commands are only available in certain modes.

Command Modes and Prompts

The ASA CLI includes command modes. Some commands can only be entered in certain modes. For example, to enter commands that show sensitive information, you need to enter a password and enter a more privileged mode. Then, to ensure that configuration changes are not entered accidentally, you have to enter a configuration mode. All lower commands can be entered in higher modes, for example, you can enter a privileged EXEC command in global configuration mode.



Note The various types of prompts are all default prompts and when configured, they can be different.

- When you are in the system configuration or in single context mode, the prompt begins with the hostname:

```
ciscoasa
```

- When printing the prompt string, the prompt configuration is parsed and the configured keyword values are printed in the order in which you have set the prompt command. The keyword arguments can be any of the following and in any order: hostname, domain, context, priority, state.

```
asa(config)# prompt hostname context priority state
```

- When you are within a context, the prompt begins with the hostname followed by the context name:

```
ciscoasa/context
```

The prompt changes depending on the access mode:

- User EXEC mode

User EXEC mode lets you see minimum ASA settings. The user EXEC mode prompt appears as follows when you first access the ASA:

```
ciscoasa>
ciscoasa/context>
```

- Privileged EXEC mode

Privileged EXEC mode lets you see all current settings up to your privilege level. Any user EXEC mode command will work in privileged EXEC mode. Enter the **enable** command in user EXEC mode, which requires a password, to start privileged EXEC mode. The prompt includes the number sign (#):

```
ciscoasa#
ciscoasa/context#
```

- Global configuration mode

Global configuration mode lets you change the ASA configuration. All user EXEC, privileged EXEC, and global configuration commands are available in this mode. Enter the **configure terminal** command in privileged EXEC mode to start global configuration mode. The prompt changes to the following:

```
ciscoasa(config)#
ciscoasa/context(config)#
```

- Command-specific configuration modes

From global configuration mode, some commands enter a command-specific configuration mode. All user EXEC, privileged EXEC, global configuration, and command-specific configuration commands are available in this mode. For example, the **interface** command enters interface configuration mode. The prompt changes to the following:

```
ciscoasa(config-if)#
ciscoasa/context(config-if)#
```

Syntax Formatting

Command syntax descriptions use the conventions listed in Table 7-1.

Table 1: Syntax Conventions

Convention	Description
bold	Bold text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical bar indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Abbreviating Commands

You can abbreviate most commands down to the fewest unique characters for a command; for example, you can enter **wr t** to view the configuration instead of entering the full command **write terminal**, or you can enter **en** to start privileged mode and **conf t** to start configuration mode. In addition, you can enter **0** to represent **0.0.0.0**.

Command-Line Editing

The ASA uses the same command-line editing conventions as Cisco IOS software. You can view all previously entered commands with the show history command or individually with the up arrow or **^p** command. Once you have examined a previously entered command, you can move forward in the list with the down arrow or ^n command. When you reach a command you wish to reuse, you can edit it or press the Enter key to start it. You can also delete the word to the left of the cursor with **^w**, or erase the line with ^u.

The ASA permits up to 512 characters in a command; additional characters are ignored.

Command Completion

To complete a command or keyword after entering a partial string, press the **Tab** key. The ASA only completes the command or keyword if the partial string matches only one command or keyword. For example, if you enter **s** and press the **Tab** key, the ASA does not complete the command because it matches more than one command. However, if you enter **dis**, the **Tab** key completes the **disable** command.

Command Help

Help information is available from the command line by entering the following commands:

- **help** *command_name*

Shows help for the specific command.

- *command_name* **?**

Shows a list of arguments available.

- *string***?** (no space)

Lists the possible commands that start with the string.

- **?** and **+?**

Lists all commands available. If you enter **?**, the ASA shows only commands available for the current mode. To show all commands available, including those for lower modes, enter **+?**.



Note If you want to include a question mark (?) in a command string, you must press **Ctrl-V** before typing the question mark so that you do not inadvertently invoke CLI help.

Viewing the Running Configuration

To view the running configuration, use one of the following commands.

To filter the command output, see the "Filtering show and more Command Output" section on page 7-5.

Command	Purpose
show running-config[**all**][*command*]	Shows the running configuration. If you specify **all**, then all default settings are shown as well. If you specify a *command* , then the output only includes related commands. **Note** Many passwords are shown as *****. To view the passwords in plain text, or in encrypted form if you have a master passphrase enabled, use the **more** command below.
more system:running-config	Shows the running configuration. Passwords are shown in plain text or in encrypted form if you have a master passphrase enabled.

Filtering show and more Command Output

You can use the vertical bar (|) with any show command and include a filter option and filtering expression. The filtering is performed by matching each output line with a regular expression, similar to Cisco IOS software. By selecting different filter options you can include or exclude all output that matches the expression. You can also display all output beginning with the line that matches the expression.

The syntax for using filtering options with the show command is as follows:

```
ciscoasa# show command
 | {include | exclude | begin | grep [-v]} regexp
```

or

```
ciscoasa# more system:running-config
 | {include | exclude | begin | grep [-v]} regexp
```



Note The **more** command can view the contents of any file, not just the running configuration; see the command reference for more information.

In this command string, the first vertical bar (|) is the operator and must be included in the command. This operator directs the output of the show command to the filter. In the syntax diagram, the other vertical bars (|) indicate alternative options and are not part of the command.

The include option includes all output lines that match the regular expression. The grep option without -v has the same effect. The exclude option excludes all output lines that match the regular expression. The grep option with -v has the same effect. The begin option shows all the output lines starting with the line that matches the regular expression.

Replace regexp with any Cisco IOS regular expression. The regular expression is not enclosed in quotes or double-quotes, so be careful with trailing white spaces, which will be taken as part of the regular expression.

When creating regular expressions, you can use any letter or number that you want to match. In addition, certain keyboard characters called *metacharacters* have special meaning when used in regular expressions.

Use **Ctrl+V** to escape all of the special characters in the CLI, such as a question mark (?) or a tab. For example, type **d[Ctrl+V]?g** to enter **d?g** in the configuration.

Redirecting and Appending show Command Output

Instead of displaying the output of a **show** command on the screen, you can redirect it to a file on the device or in a remote location. When redirecting to a file on the device, you can also append the command output to the file.

If there is a lot of output to show, command completion can take a long time. For example, you might think the system is stuck if you try to show a million access control entries, or a very large ASP table.

show *command* | {**append** | **redirect**} *url*

- **append** *url* adds the output to an existing file. Specify the file using one of the following:
  - **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*]—Both **flash** and **disk0** indicate the internal Flash memory. You can use either option.
  - **disk1:/**[[*path*/]*filename*]—Indicates external memory.
- **redirect** *url* creates the specified file, or overwrites it if the file already exists.
  - **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*]—Both **flash** and **disk0** indicate the internal Flash memory. You can use either option.
  - **disk1:/**[[*path*/]*filename*]—Indicates external memory.
  - **smb:**/[[*path*/]*filename*]—Indicates Server Message Block, a UNIX server local file system.
  - **ftp://**[[*user*[**:***password*]**@**]*server*[*:port*]/[*path*/]*filename*[**;type=***xx*]]—Indicates an FTP server. The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode).
  - **scp://**[[*user* [**:***password*]**@**]*server* [*/path*]/*filename* [**;int=***interface_name*]]—Indicates an SCP server. The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.
  - **tftp://**[[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*[**;int=***interface_name*]]—Indicates a TFTP server.

Getting a Line Count for show Command Output

Instead of seeing actual **show** command output, you might simply want a count of the number of lines in the output, or the number of lines that match a regular expression. You can then easily compare the line count with the count from previous times you entered the command. This can be a quick check as you make configuration changes. You can either use the **count** keyword, or add **-c** to the **grep** keyword.

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

Replace regular_expression with any Cisco IOS regular expression. The regular expression is not enclosed in quotes or double-quotes, so be careful with trailing white spaces, which will be taken as part of the regular expression. The regular expression is optional; if you do not include one, the count returns the total number of lines in the unfiltered output.

When creating regular expressions, you can use any letter or number that you want to match. In addition, certain keyboard characters called metacharacters have special meaning when used in regular expressions. Use **Ctrl+V** to escape all of the special characters in the CLI, such as a question mark (?) or a tab. For example, type **d[Ctrl+V]?g** to enter **d?g** in the configuration.

For example, to show the total number of all lines in the **show running-config** output:

```
ciscoasa# show running-config | count

Number of lines which match regexp = 271
```

The following example shows how you can quickly check how many interfaces are up. The first example shows how to use the **grep** keyword with a regular expression to filter on only those lines that show an up status. The next example adds the **-c** option to simply show the count rather than the actually lines of output.

```
ciscoasa# show interface | grep is up

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up

Number of lines which match regexp = 2
```

Command Output Paging

For commands such as help or ?, show, show xlate, or other commands that provide long listings, you can determine if the information displays a screen and pauses, or lets the command run to completion. The pager command lets you choose the number of lines to display before the More prompt appears.

When paging is enabled, the following prompt appears:

```
<--- More --->
```

The More prompt uses syntax similar to the UNIX more command:

- To view another screen, press the **Space** bar.
- To view the next line, press the **Enter** key.
- To return to the command line, press the q key.

Entering Numeric Values

Many commands have parameters that require a numeric value. Unless a non-decimal number is explicitly required, the best practice is to enter the value in decimal. Thus, we provide value ranges in decimal only. For example:

igmp limit *number*

Where *number* is the number of IGMP states allowed on the interface. Valid values range from 0 to 5000. The default value is 500.

You are expected to enter a value in this format within the range, such as:

```
igmp limit 1000
```

Some commands will also take octal or hexadecimal values instead of decimal. How a number is interpreted is based on the following rules:

- Decimal—Numbers like 500 are treated as standard base-10.
- Octal—Numbers prefixed with a zero (0), such as 0500, are interpreted as base-8.
- Hexadecimal—Numbers prefixed with 0x, like 0x500, are interpreted as base-16.

However, if a command does take decimal, octal and hexadecimal numbers are converted to decimal in the running configuration.

Adding Comments

You can precede a line with a colon (:) to create a comment. However, the comment only appears in the command history buffer and not in the configuration. Therefore, you can view the comment with the show history command or by pressing an arrow key to retrieve a previous command, but because the comment is not in the configuration, the write terminal command does not display it.

Text Configuration Files

This section describes how to format a text configuration file that you can download to the ASA, and includes the following topics:

- How Commands Correspond with Lines in the Text File
- Command-Specific Configuration Mode Commands
- Automatic Text Entries
- Line Order
- Commands Not Included in the Text Configuration
- Passwords
- Multiple Security Context Files

How Commands Correspond with Lines in the Text File

The text configuration file includes lines that correspond with the commands described in this guide.

In examples, commands are preceded by a CLI prompt. The prompt in the following example is "ciscoasa(config)#":

```
ciscoasa(config)# context a
```

In the text configuration file you are not prompted to enter commands, so the prompt is omitted:

```
context a
```

Command-Specific Configuration Mode Commands

Command-specific configuration mode commands appear indented under the main command when entered at the command line. Your text file lines do not need to be indented, as long as the commands appear directly following the main command. For example, the following unindented text is read the same as indented text:

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

Automatic Text Entries

When you download a configuration to the ASA, it inserts some lines automatically. For example, the ASA inserts lines for default settings or for the time the configuration was modified. You do not need to enter these automatic entries when you create your text file.

Line Order

For the most part, commands can be in any order in the file. However, some lines, such as ACEs, are processed in the order they appear, and the order can affect the function of the access list. Other commands might also have order requirements. For example, you must enter the **nameif** command for an interface first because many subsequent commands use the name of the interface. Also, commands in a command-specific configuration mode must directly follow the main command.

Commands Not Included in the Text Configuration

Some commands do not insert lines in the configuration. For example, a runtime command such as **show running-config** does not have a corresponding line in the text file.

Passwords

The login, enable, and user passwords are automatically encrypted before they are stored in the configuration. For example, the encrypted form of the password “cisco” might look like jMorNbK0514fadBh. You can copy the configuration passwords to another ASA in its encrypted form, but you cannot unencrypt the passwords yourself.

If you enter an unencrypted password in a text file, the ASA does not automatically encrypt it when you copy the configuration to the ASA. The ASA only encrypts it when you save the running configuration from the command line using the **copy running-config startup-config** or **write memory** command.

multiple-security-context-files

For multiple security contexts, the entire configuration consists of the following multiple parts:

- The security context configurations
- The system configuration, which identifies basic settings for the ASA, including a list of contexts
- The admin context, which provides network interfaces for the system configuration

The system configuration does not include any interfaces or network settings for itself. Rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses a context that is designated as the admin context.

Each context is similar to a single context mode configuration. The system configuration differs from a context configuration in that the system configuration includes system-only commands (such as a list of all contexts) while other typical commands are not present (such as many interface parameters).

Supported Character Sets

The ASA CLI currently supports UTF-8 encoding only. UTF-8 is the particular encoding scheme for Unicode symbols, and has been designed to be compatible with an ASCII subset of symbols. ASCII characters are represented in UTF-8 as one-byte characters. All other characters are represented in UTF-8 as multibyte symbols.

The ASCII printable characters (0x20 to 0x7e) are fully supported. The printable ASCII characters are the same as ISO 8859-1. UTF-8 is a superset of ISO 8859-1, so the first 256 characters (0-255) are the same as ISO 8859-1. The ASA CLI supports up to 255 characters (multibyte characters) of ISO 8859-1.



PART I

A - B Commands

- aa - ac, on page 23
- ad - aq, on page 151
- ar - az, on page 261
- b, on page 389



aa - ac

- aaa accounting command, on page 25
- aaa accounting console, on page 27
- aaa accounting include, exclude, on page 29
- aaa accounting match, on page 32
- aaa authentication console, on page 34
- aaa authentication include, exclude, on page 38
- aaa authentication listener, on page 44
- aaa authentication listener no-logout-button, on page 47
- aaa authentication login-history, on page 48
- aaa authentication match, on page 50
- aaa authentication secure-http-client (Deprecated), on page 54
- aaa authorization command, on page 56
- aaa authorization exec, on page 60
- aaa authorization exec ssh-x509, on page 63
- aaa authorization http, on page 66
- aaa authorization include, exclude, on page 68
- aaa authorization match, on page 72
- aaa kerberos import-keytab, on page 74
- aaa local authentication attempts max-fail, on page 77
- aaa mac-exempt, on page 79
- aaa proxy-limit, on page 81
- aaa sdi import-node-secret, on page 83
- aaa-server, on page 85
- aaa-server active, fail, on page 88
- aaa-server host, on page 90
- absolute, on page 94
- accept-subordinates, on page 96
- access-group, on page 98
- access-list alert-interval, on page 103
- access-list deny-flow-max, on page 105
- access-list ethertype, on page 107
- access-list extended, on page 111
- access-list remark, on page 120

- access-list rename, on page 122
- access-list standard, on page 123
- access-list webtype, on page 125
- accounting-mode, on page 128
- accounting-port, on page 130
- accounting-server-group, on page 132
- acl-netmask-convert, on page 134
- action, on page 136
- action cli command, on page 138
- action-uri, on page 140
- activate-tunnel-group-script, on page 142
- activation-key, on page 143
- activex-relay, on page 149

aaa accounting command

To send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI, use the **aaa accounting command** command in global configuration mode. To disable support for command accounting, use the **no** form of this command.

aaa accounting command [**privilege** *level*] *tacacs + -server-tag*
no aaa accounting command [**privilege** *level*] *tacacs + -server-tag*

Syntax Description

privilege *level*	If you customize the command privilege level using the **privilege** command, you can limit which commands the ASA accounts for by specifying a minimum privilege level. The ASA does not account for commands that are below the minimum privilege level. **Note** If you enter a deprecated command and enabled the **privilege** keyword, then the ASA does not send accounting information for the deprecated command. If you want to account for deprecated commands, be sure to disable the **privilege** keyword. Many deprecated commands are still accepted at the CLI, and are often converted into the currently accepted command at the CLI; they are not included in CLI help or this guide.
tacacs+-server-tag	Specifies the server or group of TACACS+ servers to which accounting records are sent, as specified by the **aaa-server protocol** command.

Command Default

The default privilege level is 0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you configure the **aaa accounting command** command, each command other than **show** commands entered by an administrator is recorded and sent to the accounting server or servers.

Examples

The following example specifies that accounting records will be generated for any supported command, and that these records are sent to the server from the group named adminserver:

```
ciscoasa(config)# aaa accounting command adminserver
```

Related Commands

Command	Description
aaa accounting	Enables or disables TACACS+ or RADIUS user accounting (on a server designated by the aaa-server command).
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa accounting console

To enable support for AAA accounting for administrative access, use the **aaa accounting console** command in global configuration mode. To disable support for aaa accounting for administrative access, use the **no** form of this command.

aaa accounting { **serial** | **telnet** | **ssh** | **enable** } **console** *server-tag*
no aaa accounting { **serial** | **telnet** | **ssh** | **enable** } **console** *server-tag*

Syntax Description

enable	Enables the generation of accounting records to mark the entry to and exit from privileged EXEC mode.
serial	Enables the generation of accounting records to mark the establishment and termination of admin sessions that are established via the serial console interface.
server-tag	Specifies the server group to which accounting records are sent, defined by the **aaa-server protocol** command. Valid server group protocols are RADIUS and TACACS+.
ssh	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over SSH.
telnet	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over Telnet.

Command Default

By default, AAA accounting for administrative access is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must specify the name of the server group, previously specified in the **aaa-server** command.

Examples

The following example specifies that accounting records will be generated for enable access, and that these records are sent to the server named adminserver:

```
ciscoasa(config)# aaa accounting enable console adminserver
```

Related Commands

Command	Description
aaa accounting match	Enables or disables TACACS+ or RADIUS user accounting (on a server designated by the aaa-server command),
aaa accounting command	Specifies that each command, or commands of a specified privilege level or higher, entered by an administrator/user is recorded and sent to the accounting server or servers.
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa accounting include, exclude

To enable accounting for TCP or UDP connections through the ASA, use the **aaa accounting include** command in global configuration mode. To exclude addresses from accounting, use the **aaa accounting exclude** command. To disable accounting, use the **no** form of this command.

aaa accounting { **include** | **exclude** } *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*
no aaa accounting { **include** | **exclude** } *service interface_name inside_ip inside_mask outside_ip outside_mask server_tag*

Syntax Description

exclude	Excludes the specified service and address from accounting if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require accounting. Traffic that is not specified by an include statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require accounting.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server_tag	Specifies the AAA server group defined by the **aaa-server host** command.

service	Specifies the services that require accounting. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp/**port • **udp/**port

Command Default

By default, AAA accounting for administrative access is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the ASA. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the ASA for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

To enable accounting for traffic that is specified by an ACL, use the **aaa accounting match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by Adaptive Security Device Manager (ASDM).

You cannot use the **aaa accounting include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa accounting match** command.

Examples

The following example enables accounting on all TCP connections:

```
ciscoasa(config)# aaa-server mygroup protocol tacacs+
ciscoasa(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

Related Commands

Command	Description
aaa accounting match	Enables accounting for traffic specified by an ACL.
aaa accounting command	Enables accounting of administrative access.
aaa-server host	Configures the AAA server.
clear configure aaa	Clears the AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa accounting match

To enable accounting for TCP and UDP connections through the ASA, use the **aaa accounting match** command in global configuration mode. To disable accounting for traffic, use the **no** form of this command.

aaa accounting match acl_name *interface_name server_tag*
no aaa accounting match acl_name *interface_name server_tag*

Syntax Description

acl_name	Specifies the traffic that requires accounting by matching an ACL name. Permit entries in the ACL are accounted, while deny entries are exempt from accounting. This command is only supported for TCP and UDP traffic. A warning message is displayed if you enter this command and it references an ACL that permits other protocols.
interface_name	Specifies the interface name from which users require accounting.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the ASA. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the ASA for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

Accounting information is sent only to the active server in a server group unless you enable simultaneous accounting using the **accounting-mode** command in aaa-server protocol configuration mode.

You cannot use the **aaa accounting match** command in the same configuration as the **aaa accounting include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

Examples

The following example enables accounting for traffic matching a specific ACL acl2:

```
ciscoasa(config)# access-list acl12 extended permit tcp any any
ciscoasa(config)# aaa accounting match acl2 outside radserver1
```

Related Commands

Command	Description
aaa accounting include, exclude	Enables accounting by specifying the IP addresses directly in the command.
access-list extended	Creates an ACL.
clear configure aaa	Removes AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication console

To authenticate users who access the ASA CLI over a serial, SSH, HTTPS (ASDM), or Telnet connection, or to authenticate users who access privileged EXEC mode using the **enable** command, use the **aaa authentication console** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication { **serial** | **enable** | **telnet** | **ssh** | **http** } **console** { **LOCAL** | *server_group* [**LOCAL**] }
no aaa authentication { **serial** | **enable** | **telnet** | **ssh** | **http** } **console** { **LOCAL** | *server_group* [**LOCAL**] }

Syntax Description

enable	Authenticates users who access privileged EXEC mode when they use the **enable** command.
http	Authenticates ASDM users who access the ASA over HTTPS. By default, ASDM accepts a blank username and the enable password, and can also use the local database for authentication even if you do not configure this command. This command disallows the blank username/enable password login. If the aaa commands are defined, but the HTTPS authentication requests a time out, which implies the AAA servers might be down or not available, you can gain access to the ASA using a blank username and the enable password. By default, the enable password is not set.

LOCAL	Uses the local database for authentication. The **LOCAL** keyword is case sensitive. If the local database is empty, the following warning message appears:
	`Warning:local database is empty! Use 'username' command to define local users.`
	If the local database becomes empty when the **LOCAL** keyword is still present in the configuration, the following warning message appears:
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	Specifies the AAA server group tag defined by the **aaa-server** command. HTTPS management authentication does not support the SDI protocol for a AAA server group. If you use the **LOCAL** keyword in addition to the *server-tag* argument, you can configure the ASA to use the local database as a fallback method if the AAA server is unavailable. The **LOCAL** keyword is case sensitive. We recommend that you use the same username and password in the local database as the AAA server because the ASA prompt does not give any indication which method is being used.
serial	Authenticates users who access the ASA using the serial console port.

ssh	Authenticates users with passwords who access the ASA using SSH. For a local **username**, you can enable public key authentication instead of password authentication using the **ssh authentication** command. In Version 9.6(2) and 9.7(1), the **aaa authentication ssh console LOCAL** command is required for **ssh authentication**. For 9.6(1) and earlier and for 9.6(3)/9.8(1) and later, you do not have to configure the **aaa authentication ssh console LOCAL** command for public key authentication; this command only applies to users with passwords, and you can specify any server type, not just LOCAL. For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS.
telnet	Authenticates users who access the ASA using Telnet. If the **aaa authentication telnet console** command is not defined, you can gain access to the ASA CLI with the ASA login password (set with the **password** command).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	You can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or **Configuration > Device Management > Users/AAA > AAA Access > Authentication** (ASDM); then define a local user by entering the **username** command (CLI) or choosing **Configuration > Device Management > Users/AAA > User Accounts** (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.
9.6(2)	The **aaa authentication ssh console LOCAL** command is required for **ssh authentication**. In Version 9.6(2) and later, you can create a **username** without any password defined, so you can require public key authentication only.
9.6(3)/9.8(1)	Separate authentication for users with SSH public key authentication and users with passwords. You no longer have to explicitly enable AAA SSH authentication (**aaa authentication ssh console)**; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with passwords, and you can use any AAA server type.

Usage Guidelines

Before the ASA can authenticate a Telnet, SSH, or HTTPS user, you must first configure access to the ASA using the **telnet**, **ssh**, or **http** commands. These commands identify the IP addresses that are allowed to communicate with the ASA.

Logging in to the ASA

After you connect to the ASA, you log in and access user EXEC mode.

- If you do not enable any authentication for serial access, you do not enter a username or password.
- If you do not enable any authentication for Telnet, you do not enter a username; you enter the login password (set with the **password** command).
- If you enable Telnet or SSH authentication using this command, you enter the username and password as defined on the AAA server or local user database.

Accessing Privileged EXEC Mode

To enter privileged EXEC mode, enter the **enable** command or the **login** command (if you are using the local database only).

- If you do not configure enable authentication, enter the system enable password when you enter the **enable** command (set by the **enable password** command). However, if you do not use enable authentication, after you enter the **enable** command, you are no longer logged in as a particular user. To maintain your username, use enable authentication.
- If you configure enable authentication, the ASA prompts you for your username and password.

For authentication using the local database, you can use the **login** command, which maintains the username but requires no configuration to turn on authentication.

Accessing ASDM

By default, you can log into ASDM with a blank username and the enable password set by the **enable password** command. However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

HTTPS authentication does not support the SDI protocol for a AAA server group. The maximum username prompt for HTTPS authentication is 30 characters. The maximum password length is 16 characters.

No Support in the System Execution Space for AAA Commands

In multiple context mode, you cannot configure any AAA commands in the system configuration.

Number of Login Attempts Allowed

As the following table shows, the action of the prompts for authenticated access to the ASA CLI differ, depending on the option you choose with the **aaa authentication console** command.

Option	Number of Login Attempts Allowed
enable	Three tries before access is denied
serial	Continual until success
ssh	Three tries before access is denied
telnet	Continual until success
http	Continual until success

Examples

The following example shows use of the aaa authentication console command for a Telnet connection to a RADIUS server with the server tag “radius”:

```
ciscoasa(config)# aaa authentication telnet console radius
```

The following example identifies the server group “AuthIn” for enable authentication:

```
ciscoasa(config)# aaa authentication enable console AuthIn
```

The following example shows use of the aaa authentication console command with fallback to the LOCAL user database if all the servers in the group “svrgrp1” fail:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs
ciscoasa(config)# aaa authentication ssh console svrgrp1 LOCAL
```

Related Commands

Command	Description
aaa authentication	Enables or disables user authentication.
aaa-server host	Specifies the AAA server to use for user authentication.
clear configure aaa	Remove or resets the configured AAA accounting values.
ldap map-attributes	Maps LDAP attributes to RADIUS attributes that the ASA can understand.
service-type	Limits a local user CLI access.
show running-config aaa	Displays the AAA configuration.

aaa authentication include, exclude

To enable authentication for connections through the ASA, use the **aaa authentication include** command in global configuration mode. To disable authentication, use the **no** form of this command. To exclude addresses from authentication, use the **aaa authentication exclude** command. To not exclude addresses from authentication, use the **no** form of this command.

aaa authentication { **include | exclude** } *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] { *server_tag* | **LOCAL** }
no aaa authentication { **include | exclude** } *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] { *server_tag* | **LOCAL** }

Syntax Description

exclude	Excludes the specified service and address from authentication if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authentication. Traffic that is not specified by an include statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authentication.
LOCAL	Specifies the local user database.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server_tag	Specifies the AAA server group defined by the **aaa-server** command.

service Specifies the services that require authentication. You can specify one of the following values:

- **any** or **tcp/0** (specifies all TCP traffic)
- **ftp**
- **http**
- **https**
- **ssh**
- **telnet**
- **tcp/**port[-*port*]
- **udp/**port[-*port*]
- **icmp/**type
- *protocol* [/port[-*port*]]

Although you can configure the ASA to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication. See the "Usage Guidelines" section for more information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To enable authentication for traffic that is specified by an ACL, use the **aaa authentication match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authentication include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authentication match** command.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the ASA to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the ASA to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication.

The authentication ports that the ASA supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

ASA Authentication Prompts

For Telnet and FTP, the ASA generates an authentication prompt.

For HTTP, the ASA uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the ASA generates a custom login screen. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the ASA.

You might want to continue to use basic HTTP authentication if: you do not want the ASA to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the ASA; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the ASA redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.

Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the ASA in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the ASA username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the ASA password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> asa1@partreq
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	Four tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the ASA checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the ASA intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant ACLs permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the ASA intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the ASA allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the ASA sends an error message to the web browser indicating that the user must be authenticated before using the requested service.

Authenticating Directly with the ASA

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the ASA but want to authenticate other types of traffic, you can authenticate with the ASA directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the ASA at the following URLs when you enable AAA for the interface:

http://*interface_ip*[:*port*]**/netaccess/connstatus.html**
https://*interface_ip*[:*port*]**/netaccess/connstatus.html**

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the ASA, and the ASA provides a Telnet prompt.

Examples

The following example includes for authentication TCP traffic on the outside interface, with an inside IP address of 192.168.0.0 and a netmask of 255.255.0.0, with an outside IP address of all hosts, and using a server group named tacacs+. The second command line excludes Telnet traffic on the outside interface with an inside address of 192.168.38.0, with an outside IP address of all hosts:

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
ciscoasa(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
 tacacs+
```

The following examples demonstrate ways to use the interface-name parameter. The ASA has an inside network of 192.168.1.0, an outside network of 209.165.201.0 (subnet mask 255.255.255.224), and a perimeter network of 209.165.202.128 (subnet mask 255.255.255.224).

This example enables authentication for connections originated from the inside network to the outside network:

```
ciscoasa(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the inside network to the perimeter network:

```
ciscoasa(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the inside network:

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the perimeter network:

```
ciscoasa(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
 209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the perimeter network to the outside network:

```
ciscoasa(config)#aaa authentication include tcp/0 perimeter 209.165.202.128 255.255.255.224
 209.165.201.0 255.255.255.224 tacacs+
```

Related Commands

Command	Description
aaa authentication console	Enables authentication for management access.

Command	Description
aaa authentication match	Enables user authentication for through traffic.
aaa authentication secure-http-client	Provides a secure method for user authentication to the ASA before allowing HTTP requests to traverse the ASA.
aaa-server	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication listener

To enable HTTP/HTTPS listening ports to authenticate network users, use the **aaa authentication listener** command in global configuration mode. When you enable a listening port, the ASA serves an authentication page for direct connections and optionally for through traffic. To disable the listeners, use the **no** form of this command.

aaa authentication listener { **http** | **https** } *interface_name* [**port** *portnum*] [**redirect**]
no aaa authentication listener { **http** | **https** } *interface_name* [**port** *portnum*] [**redirect**]

Syntax Description

{**http** | **https**}	Specifies the protocol that you want to listen for, either HTTP or HTTPS. Enter this command separately for each protocol.
interface_name	Specifies the interface on which you enable listeners.
port *portnum*	Specifies the port number that the ASA listens on for direct or redirected traffic; the defaults are 80 (HTTP) and 443 (HTTPS). You can use any port number and retain the same functionality, but be sure your direct authentication users know the port number; redirected traffic is sent to the correct port number automatically, but direct authenticators must specify the port number manually.
redirect	Redirects through traffic to an authentication web page served by the ASA. Without this keyword, only traffic directed to the ASA interface can access the authentication web pages.

Command Default

By default, no listener services are enabled, and HTTP connections use basic HTTP authentication. If you enable the listeners, the default ports are 80 (HTTP) and 443 (HTTPS).

If you are upgrading from 7.2(1), then the listeners are enabled on ports 1080 (HTTP) and 1443 (HTTPS). The **redirect** option is also enabled.

Starting with 9.24(10), HTTP capability is eliminated and only HTTPS is supported for this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(2)	This command was added.
9.24(10)	The **http** parameter was removed. You can use HTTPS only.

Usage Guidelines

Without the **aaa authentication listener** command, when HTTP/HTTPS users need to authenticate with the ASA after you configure the **aaa authentication match** or **aaa authentication include** command, the ASA uses basic HTTP authentication. For HTTPS, the ASA generates a custom login screen.

If you configure the **aaa authentication listener** command with the **redirect** keyword, the ASA redirects all HTTP/HTTPS authentication requests to web pages served by the ASA.

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the ASA.

You might want to continue to use basic HTTP authentication if: you do not want the ASA to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the ASA; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

If you enter the **aaa authentication listener** command *without* the **redirect** option, then you only enable direct authentication with the ASA, while letting through traffic use basic HTTP authentication. The **redirect** option enables both direct and through-traffic authentication. Direct authentication is useful when you want to authenticate traffic types that do not support authentication challenges; you can have each user authenticate directly with the ASA before using any other services.



Note For cut-through proxy, when the user logs out from the authentication page, the connection stays active. The user must also log out of the SSH session to completely clear the connection.

If you enable the **redirect** option, you cannot also configure static PAT for the same interface where you translate the interface IP address and the same port that is used for the listener; NAT succeds, but authentication fails. For example, the following configuration is unsupported:

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside redirect
```

The following configuration is supported; the listener uses port 1080 instead of the default 80:

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside port 1080 redirect
```

Examples

The following example configures the ASA to redirect HTTP and HTTPS connections to the default ports:

```
ciscoasa(config)# aaa authentication listener http inside redirect
ciscoasa(config)# aaa authentication listener https inside redirect
```

The following example allows authentication requests directly to the ASA; through traffic uses basic HTTP authentication:

```
ciscoasa(config)# aaa authentication listener http inside
ciscoasa(config)# aaa authentication listener https inside
```

The following example configures the ASA to redirect HTTP and HTTPS connections to non-default ports:

```
ciscoasa(config)# aaa authentication listener http inside port 1100 redirect
ciscoasa(config)# aaa authentication listener https inside port 1400 redirect
```

Related Commands

Command	Description
aaa authentication listener no-logout-button	Remove the logout button from the cut-through proxy login page.
aaa authentication match	Configures user authentication for through traffic.
aaa authentication secure-http-client	Enables SSL and secure username and password exchange between HTTP clients and the ASA.
clear configure aaa	Removes the configured AAA configuration.
show running-config aaa	Displays the AAA configuration.
virtual http	Supports cascading HTTP authentications with basic HTTP authentication.

aaa authentication listener no-logout-button

To remove the logout button from the cut-through proxy portal page, use the **aaa authentication listener no-logout-button** command in global configuration mode. To restore the logout button, use the **no** form of this command.

aaa authentication listener no-logout-button *interface_name*
no aaa authentication listener no-logout-button *interface_name*

Syntax Description

interface_name	Specifies the interface on which you enabled the authentication listener.

Command Default

By default, the portal page has a logout button.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

By default, the cut-through proxy portal page (/netaccess/connstatus.html) presents session information and a logout button if it is accessed when a cut-through-proxy session is already active for the connecting host. You can use this command to remove the logout button.

This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address.

Examples

The following example enables the HTTP and HTTPS listeners on the inside interface and configures the ASA to redirect all HTTP/HTTPS traffic that requires authentication.

```
ciscoasa(config)# aaa authentication listener http inside redirect
ciscoasa(config)# aaa authentication listener https inside redirect
ciscoasa(config)# aaa authentication listener no-logout-button inside
```

Related Commands

Command	Description
aaa authentication listener http/https	Enables HTTP/HTTPS listening ports to authenticate network users

aaa authentication login-history

To set the login history duration, use the **aaa authentication login-history** command in global configuration mode. To disable the login history, use the **no** form of this command.

aaa authentication login-history duration *days*
no aaa authentication login-history [**duration** *days*]

Syntax Description

duration *days*	Sets the days between 1 and 365. The default is 90.

Command Default

The default is 90 days.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.8(1)	We introduced this command.

Usage Guidelines

This feature applies to usernames in the local database or from a AAA server when you enable local AAA authentication for one or more of the CLI management methods (SSH, Telnet, serial console).

ASDM logins are not saved in the history.

The login history is only saved per unit; in failover and clustering environments, each unit maintains its own login history only.

Login history data is not maintained over reloads.

To view the login history, use the **show aaa login-history** command.

Examples

The following example sets the login history to 365 days:

```
ciscoasa(config)# aaa authentication login-history duration 365
```

When a user logs in, they see their own login history, such as this SSH example:

```
cugel@10.86.194.108's password:
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
```

```
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

Related Commands

Command	Description
aaa authentication login-history	Saves the local **username** login history.
password-history	Stores previous **username** passwords. This command is not user-configurable.
password-policy reuse-interval	Prohibits the reuse of a **username** password.
password-policy username-check	Prohibits a password that matches a **username** name.
show aaa login-history	Shows the local **username** login history.
username	Configures a local user.

aaa authentication match

To enable authentication for connections through the ASA, use the **aaa authentication match** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication match *acl_name interface_name* { *server_tag* | **LOCAL** } **user-identity**
no aaa authentication match *acl_name interface_name* { *server_tag* | **LOCAL** } **user-identity**

Syntax Description

acl_name	Specifies an extended ACL name.
interface_name	Specifies the interface name from which to authenticate users.
LOCAL	Specifies the local user database.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.
user-identity	Specifies the user identity that is mapped to the identity firewall.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	The **user-identity** keyword was added.

Usage Guidelines

You cannot use the **aaa authentication match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the ASA to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the ASA to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication.

The authentication ports that the ASA supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS (requires the **aaa authentication listener** command)

ASA Authentication Prompts

For Telnet and FTP, the ASA generates an authentication prompt.

For HTTP, the ASA uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the ASA generates a custom login screen. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the ASA.

You might want to continue to use basic HTTP authentication if: you do not want the ASA to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the ASA; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the ASA redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.



Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the ASA in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the ASA username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the ASA password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> asa1@partreq
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	Four tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the ASA checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the ASA intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant ACLs permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the ASA intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the ASA allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the ASA sends to the web browser an error message indicating that the user must be authenticated before using the requested service.

Authenticating Directly with the ASA

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the ASA but want to authenticate other types of traffic, you can authenticate with the ASA directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the ASA at the following URLs when you enable AAA for the interface:

http://*interface_ip*[:*port*]**/netaccess/connstatus.html**
https://*interface_ip*[:*port*]**/netaccess/connstatus.html**

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the ASA, and the ASA provides a Telnet prompt.

Examples

The following set of examples illustrates how to use the **aaa authentication match** command:

```
ciscoasa(config)# show access-list
```

```
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)
ciscoasa(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

In this context, the following command:

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

is equivalent to this command:

```
ciscoasa(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
 tacacs
```

The aaa command statement list is order-dependent between access-list command statements. If you enter the following command:

```
ciscoasa(config)# aaa authentication match mylist outbound TACACS+
```

before this command:

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

the ASA tries to find a match in the **mylist acc**ess-list command statement group before it tries to find a match in the **yourlist** access-list command statement group.

To enable authentication for connections through the ASA and match it to the Identity Firewall feature, enter the following command:

```
ciscoasa(config)# aaa
 authenticate
 match
 access
_list
_name
 inside
 user-identity
```

Related Commands

Command	Description
aaa authorization	Enables user authorization services.
access-list extended	Creates an ACL.
clear configure aaa	Removes the configured AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication secure-http-client (Deprecated)

To enable SSL and secure username and password exchange between HTTP clients and the ASA, use the **aaa authentication secure-http-client** command in global configuration mode. To disable this function, use the **no** form of this command.

aaa authentication secure-http-client
no aaa authentication secure-http-client

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.24(10)	This command was removed. Cut-through proxy now always uses SSL/TLS connections.

Usage Guidelines

The **aaa authentication secure-http-client** command offers a secure method for user authentication to the ASA before allowing user HTTP-based web requests to traverse the ASA. This command is used for HTTP cut-through proxy authentication through SSL.

The **aaa authentication secure-http-client** command has the following limitations:

- At runtime, a maximum of 64 HTTPS authentication processes is allowed. If all 64 HTTPS authentication processes are running, the 65th, new HTTPS connection requiring authentication is not allowed.
- When **uauth timeout 0** is configured (the **uauth timeout** is set to 0), HTTPS authentication might not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is let through, but the subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even if the correct username and password are entered each time. To work around this, set the **uauth timeout** to 1 second with the **timeout uauth 0:0:1** command. However, this workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.
- Because HTTPS authentication occurs on the SSL port 443, users must not configure an **access-list** command statement to block traffic from the HTTP client to HTTP server on port 443. Furthermore, if static PAT is configured for web traffic on port 80, it must also be configured for the SSL port. In the

following example, the first line configures static PAT for web traffic and the second line must be added to support the HTTPS authentication configuration:

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

Examples

The following example configures HTTP traffic to be securely authenticated:

```
ciscoasa(config)# aaa authentication secure-http-client
ciscoasa(config)# aaa authentication include http
...
```

where "..." represents your values for *authen_service if_name local_ip local_mask foreign_ip foreign_mask*] *server_tag*.

The following command configures HTTPS traffic to be securely authenticated:

```
ciscoasa (config)# aaa authentication include https
...
```

where "..." represents your values for *authentication -service interface-name local-ip local-mask foreign-ip foreign-mask*] *server-tag*.

Note The **aaa authentication secure-https-client** command is not needed for HTTPS traffic.

Related Commands

Command	Description
aaa authentication	Enables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the aaa-server command.
virtual telnet	Accesses the ASA virtual server.

aaa authorization command

To enable command authorization, use the **aaa authorization command** command in global configuration mode. To disable command authorization, use the **no** form of this command.

aaa authorization command { **LOCAL** | *tacacs + server-tag* [**LOCAL**] }
no aaa authorization command { }] **LOCAL** [*server-tag + tacacs* | **LOCAL**

Syntax Description

LOCAL	Enables local command privilege levels set by the **privilege** command. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the ASA places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user privilege level and below. If you specify **LOCAL** after a TACACS+ server group tag, the local user database is used for command authorization only as a fallback when the TACACS+ server group is unavailable.
tacacs+ server_tag	Specifies a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server** command.

Command Default

Fallback to the local database for authorization is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	Support added for fallback to LOCAL authorization when a TACACS+ server group is temporarily unavailable.
8.0(2)	Support for privilege levels defined on RADIUS or LDAP servers was added.

Usage Guidelines

The **aaa authorization command** command specifies whether command execution at the CLI is subject to authorization. By default when you log in, you can access user EXEC mode, which offers only a minimal number of commands. When you enter the **enable** command (or the **login** command when you use the local database), you can access privileged EXEC mode and advanced commands, including configuration commands. If you want to control the access to commands, the ASA lets you configure command authorization, where you can determine which commands are available to a user.

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the ASA. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the ASA places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user privilege level and below. Note that all users access user EXEC mode when they first log in (commands at level 0 or 1). The user needs to authenticate again with the **enable** command to access privileged EXEC mode (commands at level 2 or higher), or they can log in with the **login** command (local database only).



Note You can use local command authorization without any users in the local database and without CLI or enable authentication. Instead, when you enter the **enable** command, you enter the system enable password, and the ASA places you in level 15. You can then create enable passwords for every level, so that when you enter **enable** *n* (2 to 15), the ASA places you in level *n* . These levels are not used unless you turn on local command authorization. (See the **enable** command for more information.)

- TACACS+ server privilege levels—On the TACACS+ server, configure the commands that a user or group can use after they authenticate for CLI access. Every command that a user enters at the CLI is checked with the TACACS+ server.

Security Contexts and Command Authorization

The following are important points to consider when implementing command authorization with multiple security contexts:

- AAA settings are discrete per context, not shared between contexts.

When configuring command authorization, you must configure each security context separately. This provides you the opportunity to enforce different command authorizations for different security contexts.

When switching between security contexts, administrators should be aware that the commands permitted for the username specified when they login may be different in the new context session or that command authorization may not be configured at all in the new context. Failure to understand that command authorizations may differ between security contexts could confuse an administrator. This behavior is further complicated by the next point.

- New context sessions started with the **changeto** command always use the default “enable_15” username as the administrator identity, regardless of what username was used in the previous context session. This behavior can lead to confusion if command authorization is not configured for the enable_15 user or if authorizations are different for the enable_15 user than for the user in the previous context session.

This behavior also affects command accounting, which is useful only if you can accurately associate each command that is issued with a particular administrator. Because all administrators with permission to use the **changeto** command can use the enable_15 username in other contexts, command accounting records may not readily identify who was logged in as the enable_15 username. If you use different accounting servers for each context, tracking who was using the enable_15 username requires correlating the data from several servers.

When configuring command authorization, consider the following:

- An administrator with permission to use the **changeto** command effectively has permission to use all commands permitted to the enable_15 user in each of the other contexts.

- If you intend to authorize commands differently per context, ensure that in each context the enable_15 username is denied the use of commands that are also denied to administrators who are permitted to use the **changeto** command.

When switching between security contexts, administrators can exit privileged EXEC mode and enter the **enable** command again to use the username they need.

Note The system execution space does not support **aaa** commands; therefore, command authorization is not available in the system execution space.

Local Command Authorization Prerequisites

- Configure enable authentication for local, RADIUS, or LDAP authentication using the **aaa authentication enable console** command.

Enable authentication is essential to maintain the username after the user accesses the **enable** command.

Alternatively, you can use the **login** command (which is the same as the **enable** command with authentication), which requires no configuration. We do not recommend this option because it is not as secure as enable authentication.

You can also use CLI authentication (**aaa authentication** {**ssh** | **telnet** | **serial**} **console**), but it is not required.

- You can use the **aaa authorization exec** command to enable support of administrative user privilege levels from RADIUS if RADIUS is used for authentication, but it is not required. This command also enables management authorization for local, RADIUS, LDAP (mapped), and TACACS+ users.
- See the following prerequisites for each user type:
- See the **privilege** command for information about setting command privilege levels.

TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the ASA sends the command and username to the TACACS+ server to determine if the command is authorized.

When configuring command authorization with a TACACS+ server, do not save your configuration until you are sure it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the ASA.

Be sure that your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the ASA. For example, in your TACACS+ server pool, include one server connected to interface 1, and another to interface 2. You can also configure local command authorization as a fallback method if the TACACS+ server is unavailable. In this case, you need to configure local users and command privilege levels.

See the CLI configuration guide for information about configuring the TACACS+ server.

TACACS+ Command Authorization Prerequisites

- Configure CLI authentication using the **aaa authentication** {**ssh** | **telnet** | **serial**} **console** command.
- Configure **enable** authentication using the **aaa authentication enable console** command.

Examples

The following example shows how to enable command authorization using a TACACS+ server group named tplus1:

```
ciscoasa(config)# aaa authorization command tplus1
```

The following example shows how to configure administrative authorization to support fallback to the local user database if all servers in the tplus1 server group are unavailable.

```
ciscoasa(config)# aaa authorization command tplus1 LOCAL
```

Related Commands

Command	Description
aaa authentication console	Enables CLI, ASDM, and enable authentication.
aaa authorization exec	Enables support of administrative user privilege levels from RADIUS.
aaa-server host	Configures host-related attributes.
aaa-server	Configures group-related server attributes.
enable	Enters privileged EXEC mode.
ldap map-attributes	Maps LDAP attributes to RADIUS attributes that the ASA can use.
login	Enters privileged EXEC mode using the local database for authentication.
service-type	Limits local database user CLI, ASDM, and enable access.
show running-config aaa	Displays the AAA configuration.

aaa authorization exec

To enable management authorization, use the **aaa authorization exec** command o in global configuration mode. To disable management authorization, use the **no** form of these commands.

aaa authorization exec { **authentication-server** | **LOCAL** } [**auto-enable**]
no aaa authorization exec { **authentication-server** | **LOCAL** } [**auto-enable**]

Syntax Description

authentication-server	Indicates that the authorization attributes will be retrieved from the server that was used to authenticate the user.
auto-enable	Enables administrators who have sufficient authorization privileges to enter privileged EXEC mode by entering their authentication credentials once.
LOCAL	Indicates that the authorization attributes will be retrieved from the local user database of the ASA, regardless of how authentication is done.

Command Default

By default, this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(2)	The **LOCAL** option was added.
9.2(1)	The **auto-enable** option was added.
9.4(1)	This CLI will only apply to management sessions other than HTTP.

Usage Guidelines

When using the **aaa authorization exec** command, the service-type credentials of the user are checked before allowing console access.

When you disable management authorization with the **no aaa authorization exec** command, note the following:

- The service-type credentials of the user are not checked before allowing console access.
- If command authorization is configured, privilege-level attributes are still applied if they are found in the AAA server for RADIUS, LDAP, and TACACS+ users.

If you configure **aaa authentication console** commands to authenticate users when they access the CLI, ASDM, or the **enable** command, then the **aaa authorization exec** command can limit management access depending on the user configuration.



Note Serial access is not included in *management* authorization, so if you configure **aaa authentication serial console**, then any user who authenticates can access the console port. If you configure *command* authorization, then console users are still subject to command usage limits.

To configure the user for management authorization, see the following requirements for each AAA server type or local user:

- LDAP mapped users—To map LDAP attributes, see the **ldap attribute-map** command.
- RADIUS users—Use the IETF RADIUS numeric **service-type** attribute, which maps to one of the following values:
  - Service-Type 5 (Outbound) denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed). Remote access (IPsec and SSL) users can still authenticate and terminate their remote access sessions.
  - Service-Type 6 (Administrative) allows full access to any services specified by the **aaa authentication console** commands.
  - Service-Type 7 (NAS prompt) allows access to the CLI when you configure the **aaa authentication** {**telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure **enable** authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.



Note The only recognized service-types are Login (1), Framed (2), Administrative (6), and NAS-Prompt (7). Using any other service-types results in denied access.

- TACACS+ users—Request authorization with the “service=shell” entry, and the server responds with PASS or FAIL, as follows:
  - PASS, privilege level 1 allows full access to any services specified by the **aaa authentication console** commands.
  - PASS, privilege level 2 and higher allows access to the CLI when you configure the **aaa authentication** {**telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure enable authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.
  - FAIL denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed).

- Local users—Set the **service-type** command, which is in the username configuration mode of the **username** command. By default, the **service-type** is **admin**, which allows full access to any services specified by the **aaa authentication console** commands.

Examples

The following example enables management authorization using the local database:

```
ciscoasa(config)# aaa authorization exec LOCAL
```

Related Commands

Command	Description
aaa authentication console	Enables console authentication.
ldap attribute-map	Maps LDAP attributes.
service-type	Limits CLI access for a local user.
show running-config aaa	Displays the AAA configuration.

aaa authorization exec ssh-x509

To enable SSH authorization for X.509v3-certificate-authenticated users, use the **aaa authorization exec ssh-x509** command in global configuration mode. To disable X.509 SSH authorization, use the **no** form of this command.

aaa authorization exec ssh-x509 { *server_group* | **LOCAL** } [**auto-enable**]
no aaa authorization exec ssh-x509 { *server_group* | **LOCAL** } [**auto-enable**]

Syntax Description

server_group	Indicates that the authorization attributes will be retrieved from a AAA server group.
auto-enable	Enables administrators who have sufficient authorization privileges to enter privileged EXEC mode.
LOCAL	Indicates that the authorization attributes will be retrieved from the local user database of the ASA.

Command Default

By default, this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.20(4)/9.24(1)	This command was added.

Usage Guidelines

SSH authentication using an X.509v3 certificate requires that the user is also authorized using either a AAA server or the local database. Add a user that matches the username derived from the certificate. Console privileges are assigned based on the attributes returned from the authorization server.

See the following attributes for each AAA server type or local user:

- LDAP-mapped users—To map LDAP attributes, see the **ldap attribute-map** command.
- RADIUS users—Use the IETF RADIUS numeric **service-type** attribute, which maps to one of the following values:
  - Service-Type 5 (Outbound) denies SSH access.
  - Service-Type 6 (Administrative) allows SSH access, including access to privileged EXEC mode with the **enable** command.

- Service-Type 1, 2, or 7 (Login, Framed, or NAS prompt) allows access to SSH but denies privileged EXEC access with the **enable** command if you configure enable authentication (**aaa authentication enable console**).

Note The only recognized service-types are Login (1), Framed (2), Administrative (6), and NAS-Prompt (7). Using any other service-types results in denied access.

- TACACS+ users—Request authorization with the "service=shell" entry, and the server responds with PASS or FAIL, as follows:
  - PASS, privilege level 1 allows SSH access, including access to privileged EXEC mode with the **enable** command.
  - PASS, privilege level 2 and higher allows access to SSH but denies privileged EXEC access with the **enable** command if you configure enable authentication (**aaa authentication enable console**).
  - FAIL denies SSH access.
- Local users—Enter **username** *name* **attributes** and then the **service-type** command.
  - **service-type admin**—(Default) Allows SSH access, including access to privileged EXEC mode with the **enable** command.
  - **service-type nas-prompt**—Allows access to SSH but denies privileged EXEC access with the **enable** command if you configure enable authentication (**aaa authentication enable console**).
  - **service-type remote-access**—Denies SSH access.

Examples

The following example enables SSH X.509 authentication with authorization using the local database:

```
ciscoasa(config)# crypto ca trustpoint lets-encrypt_CA
ciscoasa(config-ca-trustpoint)# validation-usage ssh-client ipsec-client ssl-client ssl-server
ciscoasa(config-ca-trustpoint)# exit
ciscoasa(config)# username dwinchester attributes
ciscoasa(config-username)# service-type admin
ciscoasa(config-username)# exit
ciscoasa(config)# aaa authorization exec ssh-x509 LOCAL auto-enable
ciscoasa(config)# ssh trustpoint sign lets-encrypt_CA
ciscoasa(config)# ssh username-from-certificate cn upn
```

Related Commands

Command	Description
aaa authentication console enable	Enables enable authentication.
aaa authorization exec ssh-x509	Sets the authorization server for SSH users authenticated using a certificate.
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debugging information and error messages for SSH commands.

Command	Description
ldap attribute-map	Maps LDAP attributes.
service-type	Limits CLI access for a local user.
show running-config aaa	Displays the AAA configuration.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh trustpoint sign	Sets the trustpoint for SSH certificate authentication.
ssh username-from-certificate	Sets which field to dervice the username from when using SSH certificate authentication.
validation-usage ssh-client	Enables the trustpoint to validate SSH clients when using certificate authentication.

aaa authorization http

To enable authorization for ASDM, use the **aaa authorization http** command. To disable authorization of username for ASDM, use the no form of the command:

aaa authorization http console LOCAL | <aaa-server-group>

[no] aaa authorization http console LOCAL | <aaa-server-group>

Syntax Description

aaa-server-group	Defined already, and the protocol configured for the aaa-server-group must be LDAP, RADIUS, or TACACS+. The command will have no effect if the protocol is not LDAP, RADIUS, or TACACS+.
console	Specify this keyword to identify a server group for administrative authorization.
LOCAL	Predefined server tag for AAA protocol 'local'

Command Default

Authorization of username for ASDM is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

This command is not available on platforms that do no support webvpn (ASA 1000v) and platforms with No Payload Encryption (NPE) enabled.

Examples

```
5520-1(config)# aaa ?
configure mode commands/options:
  accounting      Configure user accounting parameters
  authentication  Configure user authentication parameters
  authorization   Configure user authorization parameters
  local           AAA Local method options
  mac-exempt      Configure MAC Exempt parameters
  proxy-limit     Configure number of concurrent proxy connections allowed per
                  user
5520-1(config)# aaa authorization ?
configure mode commands/options:
  command  Specify this keyword to allow command authorization to be configured
           for all administrators on all consoles
```

```
  exclude  Exclude the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  exec     Perform administrative authorization for console connections(ssh,
           telnet and enable) configured for authentication to RADIUS,
           LDAP, TACACS or LOCAL authentication servers.
  include  Include the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  match    Specify this keyword to configure an ACL to match
  http     Perform administrative authorization for http connections

5520-1(config)# aaa authorization http ?
configure mode commands/options:
  console  Specify this keyword to identify a server group for administrative
           authorization
5520-1(config)# aaa authorization http console ?
configure mode commands/options:
  LOCAL  Predefined server tag for AAA protocol 'local'
  WORD   Name of RADIUS,LDAP or TACACS+ aaa-server group for administrative
         authorization
```

aaa authorization include, exclude

To enable authorization for connections through the ASA, use the **aaa authorization include** command in global configuration mode. To disable authorization, use the **no** form of this command. To exclude addresses from authorization, use the **aaa authorization exclude** command. To not exclude addresses from authorization, use the **no** form of this command.

aaa authorization { **include** | **exclude** } *service interface_name inside_ip inside_mask* [*outside_ip outside_mask server_tag*
no aaa authorization { **include** | **exclude** } *service interface_name inside_ip inside_mask* [*outside_ip outside_mask server_tag*

Syntax Description

exclude	Excludes the specified service and address from authorization if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authorization. Traffic that is not specified by an include statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authorization.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server_tag	Specifies the AAA server group defined by the **aaa-server** command.

service Specifies the services that require authorization. You can specify one of the following values:

- **any** or **tcp/0** (specifies all TCP traffic)
- **ftp**
- **http**
- **https**
- **ssh**
- **telnet**
- **tcp/**port[-*port*]
- **udp/**port[-*port*]
- **icmp/**type
- *protocol* [/port[-*port*]]

Note
Specifying a port range might produce unexpected results at the authorization server. The ASA sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Command Default

An IP address of **0** means "all hosts." Setting the local IP address to **0** lets the authorization server decide which hosts are authorized.

Fallback to the local database for authorization is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **exclude** parameter allows the user to specify a port to exclude to a specific host or hosts.

Usage Guidelines

To enable authorization for traffic that is specified by an ACL, use the **aaa authorization match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authorization include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authorization match** command.

You can configure the ASA to perform network access authorization with TACACS+. Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the ASA. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the ASA checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the ASA sends the username to the TACACS+ server. The TACACS+ server responds to the ASA with a permit or a deny for that traffic, based on the user profile. The ASA enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

For each IP address, one **aaa authorization include** command is permitted.

If the first attempt at authorization fails and a second attempt causes a timeout, use the service resetinbound command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```



Note Specifying a port range might produce unexpected results at the authorization server. The ASA sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the TACACS+ protocol:

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authorization include any inside 0 0 0 0
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authentication ssh console tplus1
```

In this example, the first command statement creates a server group named tplus1 and specifies the TACACS+ protocol for use with this group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next three command statements specify that any users starting connections through the outside interface to any foreign host will be authenticated using the tplus1 server group, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that SSH access to the ASA console requires authentication from the tplus1 server group.

The following example enables authorization for DNS lookups from the outside interface:

```
ciscoasa(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

The following example enables authorization of ICMP echo-reply packets arriving at the inside interface from inside hosts:

```
ciscoasa(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

This means that users cannot ping external hosts if they have not been authenticated using Telnet, HTTP, or FTP.

The following example enables authorization only for ICMP echoes (pings) that arrive at the inside interface from an inside host:

```
ciscoasa(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

Related Commands

Command	Description
aaa authorization command	Specifies whether or not command execution is subject to authorization, or configures administrative authorization to support fallback to the local user database if all servers in the specified server group are disabled.
aaa authorization match	Enables or disables the LOCAL or TACACS+ user authorization services for a specific access-list command name.
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa authorization match

To enable authorization for connections through the ASA, use the **aaa authorization match** command in global configuration mode. To disable authorization, use the **no** form of this command.

aaa authorization match *acl_name interface_name server_tag*
no aaa authorization match *acl_name interface_name server_tag*

Syntax Description

acl_name	Specifies an extended ACL name. See the access-list extended command. The **permit** ACEs mark matching traffic for authorization, while **deny** entries exclude matching traffic from authorization.
interface_name	Specifies the interface name from which users require authentication.
server_tag	Specifies the AAA server group tag as defined by the **aaa-server** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You cannot use the **aaa authorization match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You can configure the ASA to perform network access authorization with TACACS+. RADIUS authorization with the **aaa authorization match** command only supports authorization of VPN management connections to the ASA.

Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the ASA. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the ASA checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the ASA sends the username to the TACACS+ server. The TACACS+ server

responds to the ASA with a permit or a deny for that traffic, based on the user profile. The ASA enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

If the first attempt at authorization fails and a second attempt causes a timeout, use the service resetinbound command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```



Note Specifying a port range might produce unexpected results at the authorization server. The ASA sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the tplus1 server group with the aaa commands:

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authorization match myacl inside tplus1
```

In this example, the first command statement defines the tplus1 server group as a TACACS+ group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next two command statements specify that any connections traversing the inside interface to any foreign host are authenticated using the tplus1 server group, and that all these connections are logged in the accounting database. The last command statement specifies that any connections that match the ACEs in myacl are authorized by the AAA servers in the tplus1 server group.

Related Commands

Command	Description
aaa authorization	Enables or disables user authorization.
clear configure aaa	Resets all aaa configuration parameters to the default values.
clear uauth	Deletes AAA authorization and authentication caches for one user or all users, which forces users to reauthenticate the next time that they create a connection.
show running-config aaa	Displays the AAA configuration.
show uauth	Displays the username provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is only authenticated or has cached services.

aaa kerberos import-keytab

To import a Kerberos keytab file so that it can be used to authenticate the Kerberos server, use the **aaa kerberos import-keytab** command in global configuration mode. To remove an imported keytab file, use the **clear aaa kerberos keytab** command.

aaa kerberos import-keytab *file*

Syntax Description

url The location or URL of the file to be imported. Supported locations for importing the file are the following; include the complete path and file name as appropriate for the location.

- disk0:
- disk1:
- flash:
- ftp://
- http://
- https://
- scp://
- smb://
- tftp://

Command Default

No default values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.8(4)	This command was added.

Usage Guidelines

You can configure a Kerberos AAA server group to authenticate the servers in the group using the **validate-kdc** command. To accomplish the authentication, you must also import a keytab file that you exported from the Kerberos Key Distribution Center (KDC). By validating the KDC, you can prevent an attack where the attacker spoofs the KDC so that user credentials are authenticated against the attacker's Kerberos server.

When you enable KDC validation, after obtaining the ticket-granting ticket (TGT) and validating the user, the system also requests a service ticket on behalf of the user for **host**/*ASA_hostname*. The system then validates the returned service ticket against the secret key for the KDC, which is stored in a keytab file that you generated from the KDC and then uploaded to the ASA. If KDC authentication fails, the server is considered untrusted and the user is not authenticated.

To accomplish KDC authentication, you must do the following:

1. (On the KDC.) Create a user account in the Microsoft Active Directory for the ASA (go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**). For example, if the fully-qualified domain name (FQDN) of the ASA is asahost.example.com, create a user named asahost.
2. (On the KDC.) Create a host service principal name (SPN) for the ASA using the FQDN and user account:

```
C:> setspn -A HOST/asahost.example.com asahost
```

3. (On the KDC.) Create a keytab file for the ASA (line feeds added for clarity):

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

4. (On the ASA.) Import the keytab (in this example, new.keytab) to the ASA using the **aaa kerberos import-keytab** command.
5. (On the ASA.) Add the **validate-kdc** command to the Kerberos AAA server group configuration. The keytab file is used only by server groups that contain this command.

Note You cannot use KDC validation in conjunction with Kerberos Constrained Delegation (KCD). The **validate-kdc** command will be ignored if the server group is used for KCD.

Examples

The following example shows how to import a keytab named new.keytab that resides on an FTP server, and enable KDC validation in a Kerberos AAA server group.

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab

ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos

ciscoasa(config-aaa-server-group)# validate-kdc
```

Related Commands

Command	Description
clear aaa kerberos keytab	Clears the imported Kerberos keytab file.
show aaa kerberos keytab	Shows information about the Kerberos keytab file.

Command	Description
validate-kdc	Configures a Kerberos AAA server group to perform Kerberos Key Distribution Center (KDC) validation.

aaa local authentication attempts max-fail

To limit the number of consecutive failed local login attempts that the ASA allows any given user account, use the **aaa local authentication attempts max-fail** command in global configuration mode. To disable this feature and allow an unlimited number of consecutive failed local login attempts, use the **no** form of this command.

aaa local authentication attempts max-fail *number*

Syntax Description

number The maximum number of times a user can enter a wrong password before being locked out. This number can be in the range 1-16.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.17(1)	Users will be unlocked after 10 minutes and privilege level 15 users are also now affected.

Usage Guidelines

This command only affects authentication with the local user database. If you omit this command, there is no limit on the number of times a user can enter an incorrect password.

After a user makes the configured number of attempts with the wrong password, the user is locked out and cannot log in successfully until the administrator unlocks the username, or until 10 minutes passes. Locking or unlocking a username results in a syslog message.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the ASA reboots.

Examples

The following example shows use of the aaa local authentication attempts max-limits command to set the maximum number of failed attempts allowed to 2:

```
ciscoasa(config)# aaa local authentication attempts max-limits 2
```

Related Commands

Command	Description
clear aaa local user lockout	Clears the lockout status of the specified users and set their failed-attempts counter to 0.
clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the user locked-out status.
show aaa local user	Shows the list of usernames that are currently locked.

aaa mac-exempt

To specify the use of a predefined list of MAC addresses to exempt from authentication and authorization, use the **aaa mac-exempt** command in global configuration mode. To disable the use of a list of MAC addresses, use the **no** form of this command.

aaa mac-exempt match *id*
no aaa mac-exempt match *id*

Syntax Description

id	Specifies a MAC list number configured with the **mac-list** command.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can only add one **aaa mac-exempt** command. Configure the MAC list number using the **mac-list** command before using the **aaa mac-exempt** command. Permit entries in the MAC list exempt the MAC addresses from authentication and authorization, while deny entries require authentication and authorization for the MAC address, if enabled. Because you can only add one instance of the **aaa mac-exempt** command, be sure that the MAC list includes all the MAC addresses that you want to exempt.

Examples

The following example bypasses authentication for a single MAC address:

```
ciscoasa(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# aaa mac-exempt match abc
```

The following entry bypasses authentication for all Cisco IP Phones, which have the hardware ID 0003.E3:

```
ciscoasa(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
ciscoasa(config)# aaa mac-exempt match acd
```

The following example bypasses authentication for a a group of MAC addresses except for 00a0.c95d.02b2:

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(config)# aaa mac-exempt match 1
```

Related Commands

Command	Description
aaa authentication	Enables user authentication.
aaa authorization	Enables user authorization services.
aaa mac-exempt	Exempts a list of MAC addresses from authentication and authorization.
show running-config mac-list	Displays a list of MAC addresses previously specified in the **mac-list** command.
mac-list	Specifies a list of MAC addresses to be used to exempt MAC addresses from authentication and/or authorization.

aaa proxy-limit

To limit the number of concurrent authentication attempts (at the same time) for a given IP address, use the **aaa proxy-limit** command in global configuration mode. To return to the default proxy-limit value, use the **no** form of this command.

aaa proxy-limit *proxy_limit*
aaa proxy-limit disable
no aaa proxy-limit

Syntax Description

disable	Specifies that no proxies are allowed.
proxy_limit	Specifies the number of concurrent proxy connections allowed per user, from 1 to 128.

Command Default

The default proxy-limit value is 16.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If a source address is a proxy server, consider excluding this IP address from authentication or increasing the number of allowable outstanding AAA requests.

For example, if two users were at the same IP address (perhaps connected to a terminal server) and both open a browser or connection and try to begin authenticating at exactly the same time, only one would be allowed, and the second would be blocked.

The first session from that IP address will be proxied and sent the auththentication request, while the other session would time out. This has nothing to do with how many connections a single username has.

Examples

The following example shows how to set the maximum number of outstanding authentication attempts (at the same time) for a given IP address:

```
ciscoasa(config)# aaa proxy-limit 6
```

Related Commands

Command	Description
aaa authentication	Enables, disables, or views LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the aaa-server command, or ASDM user authentication.
aaa authorization	Enables or disables LOCAL or TACACS+ user authorization services.
aaa-server host	Specifies a AAA server.
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa sdi import-node-secret

To import a node secret file that you exported from an RSA Authentication Manager for use with an SDI AAA server group, use the **aaa sdi import-node-secret** command in global configuration mode. To remove an imported node secret file, use the **clear aaa sdi node-secret** command.

aaa sdi import-node-secret *filepath rsa_server_address password*

Syntax Description

filepath	The complete path to the unzipped node secret file that was exported from the RSA Authentication Manager. Supported locations for importing the file are the following; include the complete path and file name as appropriate for the location. • disk0: • disk1: • flash: • ftp:// • http:// • https:// • scp:// • smb:// • tftp://
rsa_server_address	The IP address or fully-qualified hostname of the RSA Authentication Manager server to which the node secret belongs.
password	The password used to protect the file when you exported it.

Command Default

No default values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.15(1)	This command was added.

Usage Guidelines

You can manually import the node-secret file that is generated by the RSA Authentication Manager (SecurID) server.

You must export the node secret file from the RSA Authentication Manager server. For details, see the RSA Authentication Manager documentation. Then, either upload the unzipped file to the ASA, or place it on a server from which you can import it using this command.

Examples

The following example shows how to import the nodesecret.rec file for the rsaam.example.com server, using mysecret as the password.

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret

nodesecret.rec imported successfully
ciscoasa#
```

Related Commands

Command	Description
clear aaa sdi node-secret	Clears an imported SDI node secret file.
show aaa sdi node-secrets	Shows information about SecurID servers that have an imported node secret file.

aaa-server

To create a AAA server group and configure AAA server parameters that are group-specific and common to all group hosts, use the **aaa-server** command in global configuration mode. To remove the designated group, use the **no** form of this command.

aaa-server *server-tag* **protocol** *server-protocol*
no aaa-server *server-tag* **protocol** *server-protocol*

Syntax Description

protocol *server-protocol*	Specifies the AAA protocol that the servers in the group support: • **http-form** • **kerberos** • **ldap** • **nt** (Note that this option is no longer available as of the 9.3(1) release.) • **radius** • **sdi** (RSA SecurID using the authentication and server management protocol (ACE)) • **tacacs+**
server-tag	Specifies the server group name, which is matched by the name specified by the **aaa-server host** commands. Other AAA commands make reference to the AAA server group name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	The **http-form** protocol was added.
8.2(2)	The maximum number of AAA server groups was increased from 15 to 100 for single mode.
8.4(2)	The **ad-agent-mode** option in aaa-server group configuration mode was added.

Release	Modification
9.3(1)	The **nt** option is no longer available. Windows NT domain authentication support has been deprecated.
9.13(1)	The limit on the number of allowed server groups was increase from 100 to 200 for single mode, and from 4 to 8 in multiple mode. In addition, the limit for the number of servers in a group was increased from 4 to 8 in multiple mode. The per-group server limit in single mode remains unchanged at 16.

Usage Guidelines

You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode. Starting with 9.13(1), the limits are increased to 200 groups in single mode, 8 groups in multiple mode.

Each group can have up to 16 servers in single mode or 4 servers in multiple mode. Starting with 9.13(1), the limit for multiple mode is 8 servers per group. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

You control AAA server configuration by defining a AAA server group protocol with the **aaa-server** command, and then you add servers to the group using the **aaa-server host** command. When you enter the **aaa-server protocol** command, you enter aaa-server group configuration mode.

If you are using the RADIUS protocol and are in the aaa-server group configuration mode, note the following:

- To enable multi-session accounting for clientless SSL and Secure Client sessions, enter the **interim-accounting-update** option. If you choose this option, interim accounting records are sent to the RADIUS server in addition to the start and stop records.
- To specify the shared secret between the ASA and the AD agent and indicate that a RADIUS server group includes AD agents that are not full-function RADIUS servers, enter the **ad-agent-mode** option. Only a RADIUS server group that has been configured using this option can be associated with user identity. As a result, the **test aaa-server** {**authentication** | **authorization**} *aaa-server-group* command is not available when a RADIUS server group that is not configured using the **ad-agent-mode** option is specified.

Examples

The following example shows the use of the **aaa-server** command to modify details of a TACACS+ server group configuration:

```
ciscoasa
(config)#
aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# reactivation mode timed
ciscoasa(config-aaa-server-group)# max-failed attempts 2
```

Related Commands

Command	Description
accounting-mode	Indicates whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
reactivation-mode	Specifies the method by which failed servers are reactivated.
max-failed-attempts	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.

Command	Description
clear configure aaa-server	Removes all AAA server configurations.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

aaa-server active, fail

To reactivate a AAA server that is marked failed, use the **aaa-server active** command in privileged EXEC mode. To fail an active server, use the **aaa-server fail** command in privileged EXEC mode.

aaa-server *server_tag* [**active** | **fail**] **host** { *server_ip* | *name* }

Syntax Description

active	Sets the server to an active state.
fail	Sets the server to a failed state.
host	Specifies the host IP address name or IP address.
name	Specifies the name of the server using either a name assigned locally using the **name** command or a DNS name. Maximum characters is 128 for DNS names and 63 characters for names assigned using the **name** command.
server_ip	Specifies the IP address of the AAA server.
server_tag	Specifies a symbolic name of the server group, which is matched by the name specified by the **aaa-server** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Without this command, servers in a group that failed remain in a failed state until all servers in the group fail, after which all are reactivated.

Examples

The following example shows the state for server 192.168.125.60 and manually reactivates it:

```
ciscoasa
#
show aaa-server group1 host 192.68.125.60
Server Group:  group1
```

```
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
ciscoasa
#
aaa-server active host 192.168.125.60
ciscoasa
#
show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

Related Commands

Command	Description
aaa-server	Creates and modifies AAA server groups.
clear configure aaa-server	Removes all AAA-server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

aaa-server host

To configure a AAA server as part of a AAA server group and to configure AAA server parameters that are host-specific, use the **aaa-server host** command in global configuration mode. To remove a host configuration, use the **no** form of this command.

aaa-server *server-tag* [(*interface-name*)] **host** { *server-ip* | *name* } [*key*] [**timeout** *seconds*]
no aaa-server *server-tag* [(*interface-name*)] **host** { *server-ip* | *name* } [*key*] [**timeout** *seconds*]

Syntax Description

(*interface-name***)**	(Optional) Specifies the network interface where the authentication server resides. The parentheses are required in this parameter. If you do not specify an interface, the default is **inside**, if available. **Note** After you configure the host with an interface, if you need to change the interface, you must first remove the host command using the **no** form. You can then add a new host entry with the correct interface. If you simply try to change the interface without first removing the command, your change is accepted but ignored.
key	(Optional) Specifies a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the RADIUS or TACACS+ server. Any characters entered past 127 are ignored. The key is used between the ASA and the server for encrypting data between them. the key must be the same on both the ASA and server systems. Spaces are not permitted in the key, but other special characters are allowed. You can add or modify the key using the **key** command in host mode.
name	Specifies the name of the server using either a name assigned locally using the **name** command or a DNS name. Maximum characters is 128 for DNS names and 63 characters for names assigned using the **name** command. If you use a DNS name, the name is resolved to an IP address only when the server transitions to active, either when you initially create it or it returns to active state from failed state. The name is not resolved just because the time-to-live (TTL) for the name expired.
server-ip	Specifies the IP address of the AAA server.
server-tag	Specifies a symbolic name of the server group, which is matched by the name specified by the **aaa-server** command.
timeout *seconds*	(Optional) The timeout interval for the request. This is the time after which the ASA gives up on the request to the primary AAA server. If there is a standby AAA server, the ASA sends the request to the backup server. You can modify the timeout interval using the **timeout** command in host configuration mode.

Command Default

The default timeout value is 10 seconds.

The default interface is inside.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	Support for DNS names was added.
9.0(1)	Support for user identity was added.
9.9(2)	Support for IPv6 addressing of and connectivity to Radius servers added.
9.13(1)	The limit on the number of allowed server groups was increase from 100 to 200 for single mode, and from 4 to 8 in multiple mode. In addition, the limit for the number of servers in a group was increased from 4 to 8 in multiple mode. The per-group server limit in single mode remains unchanged at 16.

Usage Guidelines

You control AAA server configuration by defining a AAA server group with the **aaa-server** command, and then you add servers to the group using the **aaa-server host** command. When you use the **aaa-server host** command, you enter the aaa-server host configuration mode, from which you can specify and manage host-specific AAA server connection data.

Each group can have up to 16 servers in single mode or 4 servers in multiple mode. Starting with 9.13(1), the limit for multiple mode is 8 servers per group. When a user logs in, the servers are accessed one at a time starting with the first server that you specify in the configuration, until a server responds.

Examples

The following example configures a Kerberos AAA server group named “watchdogs”, adds a AAA server to the group, and defines the Kerberos realm for the server:

Note Kerberos realm names use numbers and upper-case letters only. Although the ASA accepts lower-case letters for a realm name, it does not translate lower-case letters to upper-case letters. Be sure to use upper-case letters only.

```
ciscoasa
(config)#
aaa-server watchdogs protocol kerberos
ciscoasa
(config-aaa-server-group)#
exit
ciscoasa
(config)#
aaa-server watchdogs host 192.168.3.4
ciscoasa
(config-aaa-server-host)#
kerberos-realm EXAMPLE.COM
```

The following example configures an SDI AAA server group named "svrgrp1," and then adds a AAA server to the group, sets the timeout interval to 6 seconds, sets the retry interval to 7 seconds, and configures the SDI version to version 5:

```
ciscoasa
(config)#
aaa-server svrgrp1 protocol sdi
ciscoasa
(config-aaa-server-group)#
exit
ciscoasa
(config)#
aaa-server svrgrp1 host 192.168.3.4
ciscoasa
(config-aaa-server-host)#
timeout 6
ciscoasa
(config-aaa-server-host)#
retry-interval 7
ciscoasa
(config-aaa-server-host)#
sdi-version sdi-5
```

The following example shows how to narrow down the search path to the targeted groups when you use the **aaa-server** *aaa_server_group_tag* command for LDAP search:

```
ciscoasa(config)# aaa-server CISCO_AD_SERVER protocol ldap
ciscoasa(config)# aaa-server CISCO_AD_SERVER host 10.1.1.1
ciscoasa(config-aaa-server-host)# server-port 636
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Cisco Groups,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password *
ciscoasa(config-aaa-server-host)# ldap-login-dn CISCO\username1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
```

Note When the **ldap-group-base-dn** command is specified, all groups must reside under it in the LDAP directory hierarchy and no group can reside outside this path.

The **ldap-group-base-dn** command takes effect only when at least one activated user-identity based policy exists.

The **server-type microsoft** command, which is not the default, must be configured.

The first **aaa-server** *aaa_server_group_tag* **host** command is used for LDAP operations.

Related Commands

Command	Description
aaa-server	Creates and modifies AAA server groups.
clear configure aaa-server	Removes all AAA server configurations.

Command	Description
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

absolute

To define an absolute time when a time range is in effect, use the **absolute** command in time-range configuration mode. To not specify a time for a time range, use the **no** form of this command.

absolute [**end** *time date*] [**start** *time date*]
no absolute

Syntax Description

date	(Optional) Specifies the date in the format, day month year; for example, 1 January 2006. The valid range of years is 1993 through 2035.
end	(Optional) Specifies the end of the time range.
start	(Optional) Specifies the start of the time range.
time	(Optional) Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

Command Default

If no start time and date are specified, the permit or deny statement is in effect immediately and always on. Similarly, the maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated permit or deny statement is in effect indefinitely.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Time-range Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the **access-list extended time-range** command to bind the time range to an ACL.

Examples

The following example activates an ACL at 8:00 a.m. on 1 January 2006:

```
ciscoasa(config-time-range)# absolute
 start 8:00 1 January 2006
Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

Related Commands

Command	Description
access-list extended	Configures a policy for permitting or denying IP traffic through the ASA.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Defines access control to the ASA based on time.

accept-subordinates

To configure the ASA to accept subordinate CA certificates if delivered during phase one IKE exchange when not previously installed on the device, use the **accept-subordinates** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

accept-subordinates
no accept-subordinates

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is on (subordinate certificates are accepted).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

During phase 1 processing, an IKE peer might pass both a subordinate certificate and an identity certificate. The subordinate certificate might not be installed on the ASA. This command lets an administrator support subordinate CA certificates that are not configured as trustpoints on the device without requiring that all subordinate CA certificates of all established trustpoints be acceptable; in other words, this command lets the device authenticate a certificate chain without installing the entire chain locally.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and allows the ASA to accept subordinate certificates for trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# accept-subordinates
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
default enrollment	Returns enrollment parameters to their defaults.

access-group

To bind an extended or Ethertype ACL to a single interface, use the **access-group** command in global configuration mode. To unbind an ACL from the interface, use the **no** form of this command.

access-group *access_list* { **in** | **out** } **interface** *interface_name* [**per-user-override** / **control-plane**]
no access-group *access_list* { **in** | **out** } **interface** *interface_name*

To apply a single set of global extended rules to all interfaces with the single command, use the **access-group global** command in global configuration mode. To remove the global rules from all configured interfaces, use the **no** form of this command.

access-group *access_list* [**global**]
no access-group *access_list* [**global**]

Syntax Description

access_list	The name of an extended ACL. For bridge group member interfaces, you can also specify an Ethertype ACL.
control-plane	(Optional) Specifies whether or not the ACL is for to-the-box traffic. For example, you can use this option to block certain remote IP addresses from initiating a VPN session to the ASA by blocking ISAKMP. Access rules for to-the-box management traffic (defined by such commands as http, ssh, or telnet) have higher precedence than an ACL applied with the control-plane option. Therefore, such permitted management traffic will be allowed to come in even if explicitly denied by the to-the-box ACL. This option is available for the **in** direction only.
global	Applies an ACL to all traffic on all interfaces.
in	Applies the ACL in the inbound direction at the specified interface.
interface *interface_name*	Name of the network interface. In routed mode, you can apply an extended ACL to both a Bridge Virtual Interface (BVI) and its member interfaces. In transparent mode, you can apply an extended ACL to the member interfaces only. In both modes, you can apply Ethertype ACLs to member interfaces only.
out	Applies the ACL in the outbound direction at the specified interface.
per-user-override	(Optional) Allows downloadable user ACLs to override the ACL applied to the interface. This option is available for the **in** direction only.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	This command was modified to support global policies.
9.7(1)	This command was modified to allow applying extended access groups to a BVI, and Ethertype ACLs to bridge group member interfaces, in routed mode.

Usage Guidelines

Interface-specific access-group rules have higher priority that global rules, so at the time of packet classification, interface-specific rules are processed before global rules.

In routed mode, if you apply access groups to both a BVI and its member interfaces, the precedence depends on direction. Inbound, the member interface access group is checked first, then the BVI access group, and finally the global group. Outbound, the BVI access group is checked first, then the member interface access group.

Usage Guidelines for Interface-specific Rules

The **access-group** command binds an extended ACL to an interface. You must use the **access-list extended** command first to create the ACL.

You can apply the ACL to traffic inbound to an interface or outbound from an interface. If you enter the **permit** option in an **access-list** command statement, the ASA continues to process the packet. If you enter the **deny** option in an **access-list** command statement, the ASA discards the packet and generates syslog message 106023 (or 106100 for ACEs that use non-default logging).

For inbound ACLs, the **per-user-override** option allows downloaded ACLs to override the ACL applied to the interface. If the **per-user-override** option is not present, the ASA preserves the existing filtering behavior. When **per-user-override** is present, the ASA allows the **permit** or **deny** status from the per-user access-list (if one is downloaded) associated to a user to override the permit or deny status from the **access-group** command associated ACL. Additionally, the following rules are observed:

- At the time a packet arrives, if there is no per-user ACL associated with the packet, the interface ACL will be applied.
- The per-user ACL is governed by the timeout value specified by the **uauth** option of the **timeout** command but it can be overridden by the AAA per-user session timeout value.
- Existing ACL log behavior will be the same. For example, if user traffic is denied because of a per-user ACL, syslog message 109025 will be logged. If user traffic is permitted, no syslog message is generated. The log option in the per-user access-list will have no effect.

By default, VPN remote access traffic is not matched against interface ACLs. However, if you use the **no sysopt connection permit-vpn** command to turn off this bypass, the behavior depends on whether there is a **vpn-filter** applied in the group policy and whether you set the **per-user-override** option:

- No **per-user-override**, no **vpn-filter**—Traffic is matched against the interface ACL.
- No **per-user-override**, **vpn-filter**—Traffic is matched first against the interface ACL, then against the VPN filter.
- **per-user-override**, **vpn-filter**—Traffic is matched against the VPN filter only.



Note If all of the functional entries (the permit and deny statements) are removed from an ACL that is referenced by one or more **access-group** commands, the **access-group** commands are automatically removed from the configuration. The **access-group** command cannot reference empty ACLs or ACLs that contain only a remark.

Usage Guidelines for Global Rules

The **access-group global** command applies a single set of global rules on all traffic, no matter which interface the traffic arrives at the ASA.

All global rules apply only to traffic in the ingress (inbound) direction. Global rules are not applied to egress (outbound) traffic. If global rules are configured in conjunction with inbound interface access rules, then the interface access rule, which is specific, is processed before the global access rule, which is general.

Examples

The following example shows how to use the **access-group global** command to apply an ACL to all configured interfaces:

```
ciscoasa(config)# access-list acl-1 extended permit ip host 10.1.2.2 host 10.2.2.2
ciscoasa(config)# access-list acl-2 extended deny ip any any
ciscoasa(config)# access-group acl-1 in interface outside
ciscoasa(config)# access-group acl-2 global
```

The preceding rule passes traffic from 10.1.2.2 to 10.2.2.2 on the output interface and drops traffic from 10.1.1.10 to 10.2.2.20 on the output interface due to the global deny rule. This access-group configuration adds the following rules in the classification table (output from the **show asp table classify** command):

```
in  id=0xb1f90068, priority=13, domain=permit, deny=false
        hits=0, user_data=0xaece1ac0, cs_id=0x0, flags=0x0, protocol=0
        src ip=10.1.2.2, mask=255.255.255.255, port=0
        dst ip=10.2.2.2, mask=255.255.255.255, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a250, priority=12, domain=permit, deny=true
        hits=0, user_data=0xaece1b40, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
in  id=0xb1f90100, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a3f8, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
```

The following example allows global access to an HTTP server (with the IP address 10.2.2.2) in the DMZ from anywhere:

```
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

The preceding rule permits the HTTP connection from outside host 10.1.2.2 to host 10.2.2.2, and it permits the HTTP connection from the inside host 192.168.0.0 to host 10.2.2.2.

The following example shows how a global policy and an interface policy can be used together. The example allows access to a server (with the IP address 10.2.2.2) from any inside host, but it denies access to the server from any other host. The interface policy takes precedence.

```
ciscoasa(config)# access-list inside_acl permit tcp any host 10.2.2.2 eq 23
ciscoasa(config)# access-list global_acl deny ip any host 10.2.2.2
ciscoasa(config)# access-group inside_acl in interface inside
ciscoasa(config)# access-group global_acl global
```

The preceding rule denies the SSH connection from outside host 10.1.2.2 to host 10.2.2.2, and it permits the SSH connection from the inside host 192.168.0.0 to host 10.2.2..2.

The following example shows how NAT and the global access control policy work together. The example permits one HTTP connection from outside host 10.1.2.2 to host 10.2.2.2, permits another HTTP connection from inside host 192.168.0.0 to host 10.2.2.2, and denies (by implicit rule), one HTTP connection from outside host 10.255.255.255 to host 172.31.255.255.

```
ciscoasa(config)# object network dmz-server host 10.1.1.2
ciscoasa(config)# nat (any, any) static 10.2.2.2
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

The following example shows how NAT and the global access control policy work together. The example permits one HTTP connection from host 10.1.1.1 to host 192.168.0.0, permits another HTTP connection from host 209.165.200.225 to host 172.16.0.0, and denies one HTTP connection from host 10.1.1.1 to host 172.16.0.0.

```
ciscoasa(config)# object network 10.1.1.1 host 10.1.1.1
ciscoasa(config)# object network 172.16.0.0 host 172.16.0.0
ciscoasa(config)# object network 192.168.0.0 host 192.168.0.0
ciscoasa(config)# nat (inside, any) source static
10.1.1.1 10.1.1.1
 destination static
            192.168.0.0 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip object
10.1.1.1
 object
172.16.0.0
ciscoasa(config)# access-list global_acl permit ip host 209.165.200.225 object
172.16.0.0
ciscoasa(config)# access-list global_acl deny ip any
172.16.0.0
ciscoasa(config)# access-group global_acl global
```

Related Commands

Command	Description
access-list extended	Creates an extended ACL.

Command	Description
clear configure access-group	Removes access groups from all the interfaces.
show running-config access-group	Displays the current ACL bound to the interfaces.

access-list alert-interval

To specify the time interval between deny flow maximum messages, use the **access-list alert-interval** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list alert-interval *secs*
no access-list alert-interval

Syntax Description

secs	Time interval between deny flow maximum message generation; valid values are from 1 to 3600 seconds. The default value is 300 seconds.

Command Default

The default is 300 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you configure the **log** option for an ACL deny statement, and a traffic flow matches the ACL statement, the appliance caches the flow information. To prevent cache overload, there is a maximum number of cached deny flows that will be kept for the statistics shown in syslog message 106100. If the maximum is reached before issuing 106100 and resetting the cache, syslog message 106101 is issued to indicate that the deny flow maximum was exceeded.

The **access-list alert-interval** command sets the time interval for generating syslog message 106101. When the deny flow maximum is reached, another syslog message 106101 is generated if at least *secs* seconds have passed since the last syslog message 106101 was generated.

See the **access-list deny-flow-max** command for information about the deny flow maximum message generation.

Examples

The following example shows how to specify the time interval between deny flow maximum messages:

```
ciscoasa(config)# access-list alert-interval 30
```

Related Commands

Command	Description
access-list deny-flow-max	Specifies the maximum number of concurrent deny flows that can be created.
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.

access-list deny-flow-max

To specify the maximum number of concurrent deny flows that can be cached for calculating statistics for message 106100, use the **access-list deny-flow-max** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list deny-flow-max *number*
no access-list deny-flow-max *number*

Syntax Description

number	The maximum number of deny flows that should be cached to calculate statistics for syslog message 106100, between 1 and 4096. The default is 4096.

Command Default

The default is 4096.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Syslog message 106101 is generated when the ASA has reached the maximum number of cached deny flows.

Examples

The following example shows how to specify the maximum number of concurrent deny flows that can be cached:

```
ciscoasa(config)
# access-list deny-flow-max 256
```

Related Commands

Command	Description
access-list alert-interval	Sets the time between issuing message 106101.
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.

Command	Description
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access list configuration.

access-list ethertype

To configure an ACL that controls traffic based on its EtherType, use the **access-list ethertype** command in global configuration mode. To remove the ACL, use the **no** form of this command.

access-list *id* **ethertype** { **deny** | **permit** } { **any** | **bpdu** | **dsap** { *hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx** } | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number* }
no access-list *id* **ethertype** { **deny** | **permit** } { **any** | **bpdu** | **dsap** { *hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx** } | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number* }

Syntax Description

any	Permits or denies all traffic.
bpdu	Permits or denies bridge protocol data units. Starting with 9.6(2), this keyword no longer provides the intended result. Instead, write rules for **dsap 0x42**. In 9.9(1) and 9.6+ maintenance releases with the requisite support, **bpdu** and **dsap 0x42** are converted to **dsap bpdu** rules.
deny	Denies traffic.
dsap {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**}	The IEEE 802.2 Logical Link Control packet's Destination Service Access Point address. Include the address you want to permit or deny in hexadecimal, from 0x01 to 0xff. You can also use these keywords for common values: • **bpdu** for 0x42, bridge protocol data units. • **ipx** for 0xe0, Internet Packet Exchange (IPX) 802.2 LLC. • **isis** for 0xfe, Intermediate System to Intermediate System (IS-IS). • **raw-ipx** for 0xff, raw IPX 802.3 format.
hex_number	Permits or denies traffic with a particular EtherType, specified as a 16-bit hexadecimal number greater than or equal to 0x600.
id	Specifies the name or number of an ACL.
eii-ipx	Permits or denies Ethernet II IPX format, EtherType 0x8137.
ipx	Permits or denies IPX. In 9.9(1) and 9.6+ maintenance releases with the requisite support, **ipx** is a shortcut for configuring three separate rules, for **dsap ipx**, **dsap raw-ipx**, and **eii-ipx**.
isis	Permits or denies Intermediate System to Intermediate System (IS-IS). In 9.9(1) and 9.6+ maintenance releases with the requisite support, **isis** is converted to **dsap isis** rules.
mpls-multicast	Permits or denies MPLS multicast.

mpls-unicast	Permits or denies MPLS unicast.
permit	Permits traffic.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(5), 9.1(2)	The **isis** keyword was added.
9.6(2)	The **dsap** *hex_address* keyword was added. The **bpdu** keyword no longer matches the intended traffic; use **dsap 0x42** instead.
9.7(1)	You can now configure Ethertype ACLs for bridge group member interfaces in routed mode.
9.9(1)	The following changes were made: • Keywords for common protocols were added to the **dsap** keyword: **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}. • The **bpdu** keyword is automatically converted to **dsap bpdu**. • The **isis** keyword is automatically converted to **dsap isis**. • The **eii-ipx** keyword was added. • The **ipx** keyword is automatically converted to 3 rules for **dsap ipx**, **dsap raw-ipx**, and **eii-ipx**.

Usage Guidelines

An EtherType ACL is made up of one or more Access Control Entries (ACEs) that specify an EtherType. An EtherType rule controls any EtherType identified by a 16-bit hexadecimal number, as well as selected traffic types.

Note For EtherType ACLs, the implicit deny at the end of the ACL does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the ACL does not now block any IP traffic that you previously allowed with an extended ACL (or implicitly allowed from a high security interface to a low security interface). However, if you explicitly deny all traffic with an EtherType ACE, then IP and ARP traffic is denied; only physical protocol traffic, such as auto-negotiation, is still allowed.

Supported EtherTypes and Other Traffic

An EtherType rule controls the following:

- EtherType identified by a 16-bit hexadecimal number, including common types IPX and MPLS unicast or multicast.
- Ethernet V2 frames.
- BPDUs, which are permitted by default. BPDUs are SNAP-encapsulated, and the ASA is designed to specifically handle BPDUs.
- Trunk port (Cisco proprietary) BPDUs. Trunk BPDUs have VLAN information inside the payload, so the ASA modifies the payload with the outgoing VLAN if you allow BPDUs.
- Intermediate System to Intermediate System (IS-IS).
- The IEEE 802.2 Logical Link Control packet. You can control access based on the Destination Service Access Point address.

The following types of traffic are not supported:

- 802.3-formatted frames—These frames are not handled by the rule because they use a length field as opposed to a type field.

Access Rules for Returning Traffic

Because EtherTypes are connectionless, you need to apply the rule to both the inbound and outbound interfaces if you want traffic to pass in both directions.

Allowing MPLS

If you allow MPLS, ensure that Label Distribution Protocol and Tag Distribution Protocol TCP connections are established through the ASA by configuring both MPLS routers connected to the ASA to use the IP address on the ASA interface as the router-id for LDP or TDP sessions. (LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.)

On Cisco IOS routers, enter the appropriate command for your protocol, LDP or TDP. The interface is the interface connected to the ASA.

```
ciscoasa(config)# mpls ldp router-id interface force
```

Or

```
ciscoasa(config)# tag-switching tdp router-id interface force
```

Examples

The following example shows how to add an EtherType ACL:

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu
ciscoasa(config)# access-list ETHER ethertype permit dsap 0x42
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

In 9.9(1) and 9.6+ maintenance releases with the requisite support, the previous example would be done as follows:

```
ciscoasa(config)# access-list ETHER ethertype permit ipx

INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu

INFO: ethertype bpdu is saved to config as ethertype dsap bpdu
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast

ciscoasa(config)# show access-list ETHER

access-list ETHER; 5 elements
access-list ETHER ethertype permit eii-ipx (hitcount=0)
access-list ETHER ethertype permit dsap ipx(hitcount=0)
access-list ETHER ethertype permit dsap raw-ipx(hitcount=0)
access-list ETHER ethertype permit dsap bpdu(hitcount=0)
access-list ETHER ethertype permit mpls-unicast (hitcount=0)
ciscoasa(config)# access-group ETHER in interface inside
```

Related Commands

Command	Description
access-group	Binds the ACL to an interface.
clear access-group	Clears ACL counters.
clear configure access-list	Clears an ACL from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list extended

To add an Access Control Entry (ACE) to an extended ACL, use the **access-list extended** command in global configuration mode. To remove an ACE, use the **no** form of this command.

For any type of traffic, no ports:
access-list *access_list_name* [**line** *line_number*] **extended** { **deny** | **permit** } *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]
no access-list *access_list_name* [**line** *line_number*] **extended** { **deny** | **permit** } *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

For port-based traffic:
access-list *access_list_name* [**line** *line_number*] **extended** { **deny** | **permit** } { **tcp** | **udp** | **sctp** } [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]
no access-list [**line** *line_number*] **extended** { **deny** | **permit** } { **tcp** | **udp** | **sctp** } [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**

For ICMP traffic, with ICMP type:
access-list [**line** *line_number*] **extended** { **deny** | **permit** } { **icmp** | **icmp6** } [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] **log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**
no access-list [**line** *line_number*] **extended** { **deny** | **permit** } { **icmp** | **icmp6** } [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] **log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**

Syntax Description

access_list_name	Specifies the ACL ID, as a string or integer up to 241 characters in length. The ID is case-sensitive. **Tip** Use all capital letters to see the ACL ID better in your configuration.
deny	Denies a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword prevents the packet from passing through the ASA. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword exempts the traffic from inspection. Some features do not allow deny ACEs to be used. See the command documentation for each feature that uses an ACL for more information.

dest_address_argument	Specifies the IP address or FQDN to which the packet is being sent. Available arguments include: • **host** *ip_address*—Specifies an IPv4 host address. • *ip_address mask* —Specifies an IPv4 network address and subnet mask. When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255). • *ipv6-address*/*prefix-length* —Specifies an IPv6 host or network address and prefix. • **any**, **any4**, and **any6**—**any** specifies both IPv4 and IPv6 traffic; **any4** specifies IPv4 traffic only; and **any6** specifies IPv6 traffic only. • **interface** *interface_name* —Specifies the name of an ASA interface. Use the interface name rather than IP address to match traffic based on which interface is the source or destination of the traffic. You must specify the interface keyword instead of specifying the actual IP address in the ACL when the traffic source is a device interface. For example, you can use this option to block certain remote IP addresses from initiating a VPN session to the ASA by blocking ISAKMP. Any traffic originated from or destined to the ASA, itself, requires that you use the **access-group** command with the **control-plane** keyword. • **object** *nw_obj_id* —Specifies a network object created using the **object network** command. • **object-group** *nw_grp_id* —Specifies a network object group created using the **object-group network** command. • **object-group-network-service** *name*—Specifies the name of a network-service object.
icmp_argument	(Optional) Specifies the ICMP type and code. • *icmp_type* [*icmp_code*]—Specifies the ICMP type by name or number, and the optional ICMP code for that type. If you do not specify the code, then all codes are used. • **object-group** *icmp_grp_id* —Specifies an object group for ICMP/ICMP6 created using the **object-group service** or (deprecated) **object-group icmp** command.
inactive	(Optional) Disables an ACE. To reenable it, enter the entire ACE without the **inactive** keyword. This feature lets you keep a record of an inactive ACE in your configuration to make reenabling easier.
line *line-num*	(Optional) Specifies the line number at which to insert the ACE. If you do not specify a line number, the ACE is added to the end of the ACL. The line number is not saved in the configuration; it only specifies where to insert the ACE.

log [[*level*] [**interval** *secs*] | **disable** | **default**]	(Optional) Sets logging options when an ACE matches a packet for network access (an ACL applied with the **access-group** command). If you enter the **log** keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). If you do not enter the **log** keyword, then the default system log message 106023 is generated for denied packets. Log options are: • *level* —A severity level between 0 and 7. The default is 6 (informational). If you change this level for an active ACE, the new level applies to new connections; existing connections continue to be logged at the previous level. • **interval** *secs* —The time interval in seconds between syslog messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow from the cache used to collect drop statistics. • **disable**—Disables all ACE logging. • **default**—Enables logging to message 106023. This setting is the same as not including the **log** option.
permit	Permits a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword lets the packet pass through the ASA. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword applies inspection to the packet.

port_argument	(Optional; **tcp**, **udp**, **sctp** only.) Specifies the source or destination port. If you do not specify ports, all ports are matched. Note that you can also specify ports in a service object that you specify for the *protocol_argument* instead of using this argument. If you use network-service objects that specify the protocol and ports, you should not specify ports in this argument. Available arguments include: • *operator port* —The port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include: • **lt**—less than • **gt**—greater than • **eq**—equal to • **neq**—not equal to • **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example: `range 100 200` DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP. • **object-group** *service_grp_id* —Specifies a service object group created using the **object-group service** {**tcp** | **udp** | **tcp-udp**} command. Note that these object types are no longer recommended. You cannot specify the recommended generic service objects, where the protocol and port are defined within the object, as the port argument. You specify these objects as part of the protocol argument
protocol_argument	Specifies the IP protocol. If you use network-service objects that specify the protocol and ports, you should specify **ip** in this argument.Available arguments include: • *name* or *number* —Specifies the protocol name or number. For example, UDP is 17, TCP is 6, and EGP is 47. Specify **ip** to apply to all protocols. See the CLI help for the available options. • **object-group** *protocol_grp_id* —Specifies a protocol object group created using the **object-group protocol** command. • **object** *service_obj_id* —Specifies a service object created using the **object service** command. A TCP, UDP, SCTP, or ICMP service object can include a protocol and a source and/or destination port or ICMP type and code, which are used when matching traffic to the ACE; you do not have to configure the port/type separately in the ACE. • **object-group** *service_grp_id*— Specifies a service object group created using the **object-group service** command.

sctp	Sets the protocol to SCTP.
security_group_argument	For use with the TrustSec feature, specifies the security group for which to match traffic in addition to the source or destination address. Available arguments include: • **object-group-security** *security_obj_grp_id* —Specifies a security object group created using the **object-group security** command. • **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag* }—Specifies a security group name or tag.
source_address_argument	Specifies the IP address or FQDN from which the packet is being sent. The available arguments are the same as those described for *dest_address_argument* .
tcp	Sets the protocol to TCP.
time-range *time_range_name*	(Optional) Specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active. See the **time-range** command for information about defining a time range.
udp	Sets the protocol to UDP.
user_argument	For use with the identity firewall feature, specifies the user or group for which to match traffic in addition to the source address. Available arguments include: • **object-group-user** *user_obj_grp_id* —Specifies a user object group created using the **object-group user** command. • **user** {[*domain_nickname*\\]*name* | **any** | **none**}—Specifies a username. Specify **any** to match all users with user credentials, or **none** to match addresses that are not mapped to usernames. These options are especially useful for combining **access-group** and **aaa authentication match** policies. • **user-group** [*domain_nickname*\\\]*user_group_name* —Specifies a user group name. Note the double \\ separating the domain and group name.

Command Default

- Default logging for deny ACEs generates system log message 106023 for denied packets only.
- When the **log** keyword is specified, the default level for system log message 106100 is 6 (informational), and the default interval is 300 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	When using NAT or PAT, mapped addresses and ports are no longer required in an ACL for several features. You should now always use the real, untranslated addresses and ports for these features. Using the real address and port means that if the NAT configuration changes, you do not need to change the ACLs. See the "Features That Use Real IP Addresses" section for more information.
8.4(2)	You can now use identity firewall users and groups for the source and destination, in addition to the source or destination IP address. Support for **user**, **user-group**, and **object-group-user** were added for the source and destination.
9.0(1)	You can now use TrustSec security groups for the source and destination, in addition to the source or destination IP address. Support for **security-group** and **object-group-security** were added for the source or destination.
9.0(1)	Support for IPv6 was added. The **any** keyword was changed to represent IPv4 and IPv6 traffic. The **any4** and **any6** keywords were added to represent IPv4-only and IPv6-only traffic, respectively. You can specify a mix of IPv4 and IPv6 addresses for the source and destination. If you use NAT to translate between IPv4 and IPv6, the actual packet will not include a mix of IPv4 and IPv6 addresses; however, for many features, the ACL always uses the real IP addresses and does not consider the NAT mapped addresses. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs. See the release notes for more information about migration. For information about ACL migration, see the 9.0 release notes.
9.0(1)	Support for the ICMP code was added. When you specify **icmp** as the protocol, you can enter *icmp_type* [*icmp_code*].
9.5(2)	The **sctp** keyword was added.
9.17(1)	The **object-group-network-service** keyword was added.

Usage Guidelines

An ACL is made up of one or more ACEs with the same ACL ID. ACLs are used to control network access or to specify traffic for many features to act upon. Each ACE that you enter for a given ACL name is appended to the end of the ACL, unless you specify the line number in the ACE. To remove the entire ACL, use the **clear configure access-list** command.

Order of ACEs

The order of ACEs is important. When the ASA decides whether to forward or drop a packet, the ASA tests the packet with each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an ACL that explicitly permits all traffic, no further statements are ever checked.

Features That Use Real IP Addresses

The following commands and features use real IP addresses in the ACLs:

- **access-group** command
- Modular Policy Framework **match access-list** command
- Botnet Traffic Filter **dynamic-filter enable classify-list** command
- AAA **aaa ... match** commands
- WCCP **wccp redirect-list group-list** command

Features That Use Mapped IP Addresses

The following features use ACLs, but these ACLs use the mapped values as seen on an interface:

- IPsec ACLs
- **capture** command ACLs
- Per-user ACLs
- Routing protocol ACLs
- All other feature ACLs

Features That Do Not Support Identity Firewall, FQDN, and TrustSec ACLs

The following features use ACLs, but cannot accept an ACL with identity firewall (specifying user or group names), FQDN (fully-qualified domain names), or TrustSec values:

- **route-map** command
- VPN **crypto map** command
- VPN **group-policy** command, except for **vpn-filter**
- WCCP
- DAP

Examples

The following ACL allows all hosts (on the interface to which you apply the ACL) to go through the ASA:

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

The following sample ACL prevents hosts on 192.168.1.0/24 from accessing the 209.165.201.0/27 network. All other addresses are permitted.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp
192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.224
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

If you want to restrict access to only some hosts, then enter a limited **permit ACE**. By default, all other traffic is denied unless explicitly permitted.

```
ciscoasa(config)# access-list ACL_IN extended permit ip
192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.224
```

The following ACL restricts all hosts (on the interface to which you apply the ACL) from accessing a website at address 209.165.201.29. All other traffic is allowed.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

The following ACL that uses object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp
object-group denied object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

To temporarily disable an ACL that permits traffic from one group of network objects (A) to another group of network objects (B):

```
ciscoasa(config)# access-list 104 permit ip host object-group A object-group B inactive
```

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the **access-list extended** command to bind the time range to an ACL. The following example binds an ACL named "Sales" to a time range named "New_York_Minute":

```
ciscoasa(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

See the **time-range** command for more information about how to define a time range.

The following ACL allows any ICMP traffic:

```
ciscoasa(config)# access-list abc extended permit icmp any any
```

The following ACL allows any ICMP traffic for the object group "obj_icmp_1":

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

The following ACL permits ICMP traffic with ICMP type 3 and ICMP code 4 from source host 10.0.0.0 to destination host 10.1.1.1. All other type of ICMP traffic is not be permitted.

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3 4
```

The following ACL permits ICMP traffic with ICMP type 3 and any ICMP code from source host 10.0.0.0 to destination host 10.1.1.1. All other type of ICMP traffic is not be permitted.

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3
```

Related Commands

Command	Description
access-group	Binds the ACL to an interface.
clear access-group	Clears an ACL counter.

Command	Description
clear configure access-list	Clears an ACL from the running configuration.
show access-list	Displays ACEs by number.
show running-config access-list	Displays the current running access list configuration.

access-list remark

To specify the text of a remark to add before or after an extended, EtherType, or standard access control entry, use the **access-list remark** command in global configuration mode. To delete the remark, use the **no** form of this command.

access-list *id* [**line** *line-num*] **remark** *text*
no access-list *id* [**line** *line-num*] **remark** *text*

Syntax Description

id	Name of the ACL.
line *line-num*	(Optional) The line number at which to insert the remark.
remark text	Text of the remark

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The remark text must contain at least one non-space character; an empty remark is not allowed. The remark text can be up to 100 characters long, including spaces and punctuation.

You cannot use the **access-group** command on an ACL that includes a remark only.

Examples

The following example shows how to specify the text of a remark to the end of an ACL.

```
ciscoasa(config)#
access-list MY_ACL remark checklist
```

Related Commands

Command	Description
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.

Command	Description
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access list configuration.

access-list rename

To rename an ACL, use the **access-list rename** command in global configuration mode.

access-list *id* **rename** *new_acl_id*

Syntax Description

id	Name of an existing ACL.
rename *new_acl_id*	Specifies the new ACL ID, as a string or integer up to 241 characters long. The ID is case-sensitive.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

If the ACL is renamed to the same name, the ASA will silently ignore the command.

Examples

The following example shows how to rename an ACL from TEST to OUTSIDE:

```
ciscoasa(config)#
access-list TEST rename OUTSIDE
```

Related Commands

Command	Description
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list standard

To add an Access Control Entry (ACE) to a standard ACL, use the **access-list standard** command in global configuration mode. To remove an ACE, use the **no** form of this command.

access-list *id* **standard** { **deny** | **permit** } { **any4** | **host** *ip_address* | *ip_address subnet_mask* }
no access-list *id* **standard** { **deny** | **permit** } { **any4** | **host** *ip_address* | *ip_address subnet_mask* }

Syntax Description

any4	Matches any IPv4 address.
deny	Denies or exempts a packet if the conditions are matched
host *ip_address*	Specifies an IPv4 host address (that is, the subnet mask is 255.255.255.255).
id	Name or number of an ACL.
ip_address subnet_mask	Specifies an IPv4 network address and subnet mask.
permit	Permits or includes a packet if the conditions are matched.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

A standard ACL is composed of all ACEs with the same ACL ID or name. Standard ACLs are used for a limited number of features, such as route maps or VPN filters. A standard ACL uses IPv4 addresses only, and defines destination addresses only.

Examples

The following example shows how to add an rule to a standard ACL:

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

Related Commands

Command	Description
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access list configuration.

access-list webtype

To add an Access Control Entry (ACE) to a webtype ACL, which filters clientless SSL VPN connections, use the **access-list webtype** command in global configuration mode. To remove the ACE, use the **no** form of this command.

access-list *id* **webtype** { **deny** | **permit** } **url** { *url_string* | **any** } [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] } [**time_range** *name*] [**inactive**]
no access-list *id* **webtype** { **deny** | **permit** } **url** { *url_string* | **any** } [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] } [**time_range** *name*] [**inactive**]
access-list *id* **webtype** { **deny** | **permit** } **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] } [**time_range** *name*] [**inactive**]
no access-list *id* **webtype** { **deny** | **permit** } **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] } [**time_range** *name*] [**inactive**]

Syntax Description

deny	Denies access if the conditions are matched.
dest_address_argument	Specifies the IP address to which the packet is being sent. Destination address options are: • **host** *ip_address* —Specifies an IPv4 host address. • *dest_ip_address mask* —Specifies an IPv4 network address and subnet mask, such as 10.100.10.0 255.255.255.0. • *ipv6-address/prefix-length* —Specifies an IPv6 host or network address and prefix. • **any**, **any4**, and **any6**—**any** specifies both IPv4 and IPv6 traffic; **any4** specifies IPv4 traffic only; and **any6** specifies IPv6 traffic only.
id	Specifies a name or number of an ACL.
inactive	(Optional) Disables an ACE. To reenable it, enter the entire ACE without the **inactive** keyword. This feature lets you keep a record of an inactive ACE in your configuration to make reenabling easier.
log [[*level*] [**interval** *secs*] | **disable** | **default**]	(Optional) Sets logging options when an ACE matches a packet. If you enter the **log** keyword without any arguments, you enable VPN filter system log message 106102 at the default level (6) and for the default interval (300 seconds). If you do not enter the **log** keyword, then the default VPN filter system log message 106103 is generated. Log options are: • *level* —A severity level between 0 and 7. The default is 6 (informational). • **interval** *secs* —The time interval in seconds between syslog messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow from the cache used to collect drop statistics. • **disable**—Disables all ACE logging. • **default**—Enables logging to message 106103. This setting is the same as not including the **log** option.

operator port	(Optional) If you specify **tcp**, the destination port. If you do not specify ports, all ports are matched. The *operator* can be one of the following: • **lt**—less than • **gt**—greater than • **eq**—equal to • **neq**—not equal to • **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example: `range 100 200` The *port* can be the integer or name of a TCP port.
permit	Permits access if the conditions are matched.
time_range *name*	(Optional) Specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active. See the **time-range** command for information about defining a time range.
url {*url_string* | **any**}	Specifies the URL to match. Use **url any** to match all URL-based traffic. Otherwise, enter a URL string, which can include wildcards. For tips on URL strings, see the usages guidelines.

Command Default

The defaults are as follows:

- ACL logging generates syslog message 106103 for denied packets.
- When the **log** optional keyword is specified, the default level for syslog message 106102 is 6 (informational).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **access-list webtype** command is used to configure clientless SSL VPN filtering.

Following are some tips and limitations on specifying URLs:

Select **any** to match all URLs.

- 'Permit url any' will allow all the URLs that have the format protocol://server-ip/path and will block traffic that does not match this pattern, such as port-forwarding. There should be an ACE to allow connections to the required port (port 1494 in the case of Citrix) so that an implicit deny does not occur.
- Smart tunnel and ica plug-ins are not affected by an ACL with 'permit url any' because they match smart-tunnel:// and ica:// types only.
- You can use these protocols: cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel://, and smtp://. You can also use wildcards in the protocol; for example, htt* matches http and https, and an asterisk * matches all protocols. For example, *://*.example.com matches any type URL-based traffic to the example.com network.
- If you specify a smart-tunnel:// URL, you can include the server name only. The URL cannot contain a path. For example, smart-tunnel://www.example.com is acceptable, but smart-tunnel://www.example.com/index.html is not.
- An asterisk * matches none or any number of characters. To match any http URL, enter http://*/*.
- A question mark ? matches any one character exactly.
- Square brackets [] are range operators, matching any character in the range. For example, to match both http://www.cisco.com:80/ and http://www.cisco.com:81/, enter **http://www.cisco.com:8[01]/**.

Examples

The following example shows how to deny access to a specific company URL:

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

The following example shows how to deny access to a specific web page:

```
ciscoasa(config)# access-list acl_file webtype deny url https://www.example.com/dir/file.html
```

The following example shows how to deny HTTP access to any URL on a specific server through port 8080:

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

Related Commands

Command	Description
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the access list configuration running on the ASA.

accounting-mode

To indicate whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode), use the **accounting-mode** command in aaa-server configuration mode. To remove the accounting mode specification, use the **no** form of this command.

accounting-mode { **simultaneous** | **single** }

Syntax Description

simultaneous	Sends accounting messages to all servers in the group.
single	Sends accounting messages to a single server.

Command Default

The default value is single mode.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **single** keyword to send accounting messages to a single server. Use the **simultaneous** keyword to send accounting messages to all servers in the server group.

This command is meaningful only when the server group is used for accounting (RADIUS or TACACS+).

Examples

The following example shows the use of the **accounting-mode** command to send accounting messages to all servers in the group:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa
(config-aaa-server-group)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa accounting	Enables or disables accounting services.
aaa-server protocol	Enters AAA server group configuration mode, so you can configure AAA server parameters that are group-specific and common to all hosts in the group.
clear configure aaa-server	Removes all AAA server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

accounting-port

To specify the port number used for RADIUS accounting for this host, use the **accounting-port** command in aaa-server host configuration mode. To remove the authentication port specification, use the **no** form of this command.

accounting-port *port*
no accounting-port

Syntax Description

port	A port number for RADIUS accounting; the range of valid values is 1- 65535.

Command Default

By default, the device listens for RADIUS on port 1646 for accounting (in compliance with RFC 2058). If the port is not specified, the RADIUS accounting default port number (1646) is used.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to send accounting records. If your RADIUS accounting server uses a port other than 1646, you must configure the ASA for the appropriate port before starting the RADIUS service with the **aaa-server** command.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures accounting port 2222.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
```

```
accountinq-port 2222
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa(config)#
```

Related Commands

Command	Description
aaa accounting	Keeps a record of which network services a user has accessed.
aaa-server host	Enters aaa server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

accounting-server-group

To specify the AAA server group for sending accounting records, use the **accounting-server-group** command in various modes. To remove accounting servers from the configuration, use the **no** form of this command.

accounting-server-group *group_tag*
no accounting-server-group [*group_tag*]

Syntax Description

group_tag	Identifies the previously configured accounting server or group of servers. Use the **aaa-server** command to configure accounting servers.

Command Default

No accounting servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration (deprecated)	• Yes	—	• Yes	—	—
pop3s configuration (deprecated)	• Yes	—	• Yes	—	—
Smtps configuration (deprecated)	• Yes	—	• Yes	—	—
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command is available in tunnel-group general-attributes configuration mode, instead of webvpn configuration mode.
9.5(2)	This command was deprecated for the following modes: imap4s, pop3s, and smtps.
9.8(1)	This command is no longer available for IPSec LAN-to-LAN (ipsec-l2l) tunnel groups; in fact, it was never supported for IPSec LAN-to-LAN.

Usage Guidelines

The ASA uses accounting to keep track of the network resources that users access. If you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes configuration mode.

Examples

The following example entered in tunnel-group-general attributes configuration mode, configures an accounting server group named “aaa-server123” for a remote-access tunnel group “xyz”:

```
ciscoasa(config)# tunnel-group xyz type remote-access
ciscoasa(config)# tunnel-group xyz general-attributes
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server	Configures authentication, authorization, and accounting servers.

acl-netmask-convert

To specify how the ASA treats netmasks received in a downloadable ACL from a RADIUS server that is accessed by using the **aaa-server host** command, use the acl-netmask-convert command in aaa-server host configuration mode. To remove the specified behavior for the ASA, use the **no** form of this command.

acl-netmask-convert { **auto-detect** | **standard** | **wildcard** }
no acl-netmask-convert

Syntax Description

auto-detect	Specifies that the ASA should attempt to determine the type of netmask expression used. If the ASA detects a wildcard netmask expression, it converts it to a standard netmask expression. See "Usage Guidelines" for more information about this keyword.
standard	Specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.
wildcard	Specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions and converts them all to standard netmask expressions when the ACLs are downloaded.

Command Default

By default, no conversion from wildcard netmask expressions is performed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server-host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(4)	This command was added.

Usage Guidelines

Use the **acl-netmask-convert** command with the wildcard or auto-detect keywords when a RADIUS server provides downloadable ACLs that contain netmasks in wildcard format. The ASA expects downloadable ACLs to contain standard netmask expressions whereas Cisco VPN 3000 series concentrators expect downloadable ACLs to contain wildcard netmask expressions, which are the reverse of a standard netmas expression. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match.The **acl-netmask-convert** command helps minimize the effects of these differences upon how you configure downloadable ACLs on your RADIUS servers.

The **auto-detect** keyword is helpful when you are uncertain how the RADIUS server is configured; however, wildcard netmask expressions with "holes" in them cannot be unambiguously detected and converted. For

example, the wildcard netmask 0.0.255.0 permits anything in the third octet and can be used validly on Cisco VPN 3000 series concentrators, but the ASA may not detect this expression as a wildcard netmask.

Examples

The following example configures a RADIUS AAA server named "srvgrp1" on host "192.168.3.4", enables conversion of downloadable ACL netmasks, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa
(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the aaa-server command, or ASDM user authentication.
aaa-server host	Enters aaa-server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

action

To either apply access policies to a session or terminate the session, use the **action** command in dynamic-access-policy-record configuration mode. To reset the session to apply an access policy to a session, use the **no** form of the command.

action { **continue** | **terminate** }
no action { **continue** | **terminate** }

Syntax Description

continue	Applies the access policies to the session.
terminate	Terminates the connection.

Command Default

The default value is continue.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dynamic-access-policy-record configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **continue** keyword to apply the access policies to the session in all of the selected DAP records. Use the **terminate** keyword to terminate the connection in any of the selected DAP records.

Examples

The following example shows how to terminate a session for the DAP policy Finance:

```
ciscoasa (config)#
config-dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
 action terminate
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.

Command	Description
show running-config dynamic-access-policy-record	Displays the running configuration for all DAP records, or for the named DAP record.

action cli command

To configure actions on an event manager applet, use the **action cli command** command in event manager applet configuration mode. To remove the configured action, enter the **no action** *n* command.

action *n* **cli command "** *command* **"**
no action *n*

Syntax Description

"*command* "	Specifies the name of the command. The value of the *command* option must be in quotes; otherwise, an error occurs if the command consists of more than one word. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled. Use the **noconfirm** option if the command has it available.
n	Specifies an action ID. Valid IDs range from 0 - 42947295.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to configure actions on an event manager applet.

Examples

The following example shows how to configure actions on an event manager applet:

```
hostname (config-applet)#
action 1 cli command "show version"
```

Related Commands

Command	Description
description	Describes an applet.
event manager run	Runs an event manager applet.

Command	Description
show event manager	Shows statistical information for each configured event manager applet.
debug event manager	Manages debugging traces for the event manager.

action-uri

To specify a web server URI to receive a username and password for single sign-on (SSO) authentication, use the **action-uri** command in aaa-server-host configuration mode. To reset the URI parameter value, use the **no** form of the command.

action-uri *string*
no action-uri

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string The URI for an authentication program. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for the complete URI is 2048 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server-host configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

This is an SSO with HTTP Forms command. A URI or Uniform Resource Identifier is a compact string of characters that identifies a point of content on the Internet, whether it be a page of text, a video or sound clip, a still or animated image, or a software program. The most common form of URI is the web page address, which is a particular form or subset of URI called a URL.

The WebVPN server of the ASA can use a POST request to submit an SSO authentication request to an authenticating web server. To accomplish this, configure the ASA to pass a username and a password to an action URI on an authenticating web server using an HTTP POST request. The **action-uri** command specifies the location and name of the authentication program on the web server to which the ASA sends the POST request.

You can discover the action URI on the authenticating web server by connecting to the web server login page directly with a browser. The URL of the login web page displayed in your browser is the action URI for the authenticating web server.

For ease of entry, you can enter URIs on multiple, sequential lines. The ASA then concatenates the lines into the URI as you enter them. While the maximum characters per action-uri line is 255 characters, you can enter fewer characters on each line.

Note Any question mark in the string must be preceded by a CTRL-v escape sequence.

Examples

The following example specifies the URI on www.example.com:



```
ciscoasa(config)# aaa-server testgrp1 host www.example.com
ciscoasa(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
ciscoasa(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
ciscoasa(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
ciscoasa(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
ciscoasa(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
ciscoasa(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
ciscoasa(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
ciscoasa(config-aaa-server-host)# action-uri %2Fauth.example.com
ciscoasa(config-aaa-server-host)#
```

Note You must include the hostname and protocol in the action URI. In the preceding example, these are included in http://www.example.com at the start of the URI.

Related Commands

Command	Description
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the SSO server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

activate-tunnel-group-script

This command is used internally to reload an ASDM generated script file when username-from-certificate is configured in tunnel-group sub-mode.



Note Do not use this command in the ASA CLI.

activation-key

To enter a license activation key on the ASA, use the **activation-key** command in privileged EXEC mode.

activation-key [**noconfirm** *activation_key*] **activate** | **deactivate** }

Syntax Description

activate	Activates a time-based activation key. **activate** is the default value. The last time-based key that you activate for a given feature is the active one.
activation_key	Applies an activation key to the ASA. The *activation_key* is a five-element hexadecimal string with one space between each element. The leading 0x specifier is optional; all values are assumed to be hexadecimal. You can install one permanent key, and multiple time-based keys. If you enter a new permanent key, it overwrites the already installed one.
deactivate	Deactivates a time-based activation key. The activation key is still installed on the ASA when you deactivate it, and you can activate it later using the **activate** keyword. If you enter a key for the first time, and specify **deactivate**, then the key is installed on the ASA in an inactive state.
noconfirm	(Optional) Enters an activation key without prompting you for confirmation.

Command Default

By default, your ASA ships with a license already installed. This license might be the Base License, to which you want to add more licenses, or it might already have all of your licenses installed, depending on what you ordered and what your vendor installed for you. See the **show activation-key** command to determine which licenses you have installed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	

Command History

Release	Modification
7.0(5)	Increased the following limits: • ASA5510 Base license connections from 32000 to 5000; VLANs from 0 to 10. • ASA5510 Security Plus license connections from 64000 to 130000; VLANs from 10 to 25. • ASA5520 connections from 130000 to 280000; VLANs from 25 to 100. • ASA5540 connections from 280000 to 400000; VLANs from 100 to 200.

Release	Modification
7.1(1)	SSL VPN licenses were added.
7.2(1)	A 5000-user SSL VPN license was added for the ASA 5550 and above.
7.2(2)	• The maximum number of VLANs for the Security Plus license on the ASA 5505 ASA was increased from 5 (3 fully functional; 1 failover; one restricted to a backup interface) to 20 fully functional interfaces. In addition, the number of trunk ports was increased from 1 to 8. • VLAN limits were increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), and the ASA 5550 (from 200 to 250).
7.2(3)	The ASA 5510 supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** command to change the speed on the interface and use the **show interface** command to see what speed is currently configured for each interface.
8.0(2)	• The Advanced Endpoint Assessment license was added. • VPN load balancing is supported on the ASA 5510 Security Plus license.
8.0(3)	The Secure Client for Mobile license was added.
8.0(4)/8.1(2)	Support for time-based licenses was added.
8.1(2)	The number of VLANs supported on the ASA 5580 increased from 100 to 250.
8.0(4)	The UC Proxy sessions license was added.
8.2(1)	• The Botnet Traffic Filter license was added. • The AnyConnect Essentials License was added. By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command. • Shared licenses for SSL VPN were added.
8.2(2)	The Mobility Proxy no longer requires the UC Proxy license.
8.3(1)	• Failover licenses no longer need to be identical on each unit. The license used for both units is the combined license from the primary and secondary units. • Time-based licenses are stackable. • The IME license was added. • You can install multiple time-based licenses, and have one license per feature active at a time. • You can activate or deactivate time-based licenses using **activate** or **deactivate** keywords.

Release	Modification

8.4(1)	• For the ASA 5550 and ASA 5585-X with SSP-10, the maximum number of contexts was increased from 50 to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was increased from 50 to 250.
	• For the ASA 5580 and 5585-X, the maximum number of VLANs was increased from 250 to 1024.
	• We increased the firewall connection limits:
	  • ASA 5580-20—1,000 K to 2,000 K.
	  • ASA 5580-40—2,000 K to 4,000 K.
	  • ASA 5585-X with SSP-10: 750 K to 1,000 K
	  • ASA 5585-X with SSP-20: 1,000 K to 2,000 K
	  • ASA 5585-X with SSP-40: 2,000 K to 4,000 K
	  • ASA 5585-X with SSP-60: 2,000 K to 10,000 K
	• For the ASA 5580, the AnyConnect VPN session limit was increased from 5,000 to 10,000.
	• For the ASA 5580, the other VPN session limit was increased from 5,000 to 10,000.
	• IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses.
	• Site-to-site sessions were added to the Other VPN license (formerly IPsec VPN).
	• For models available with No Payload Encryption (for example, the ASA 5585-X), the ASA software disables Unified Communications and VPN features, making the ASA available for export to certain countries.

Usage Guidelines

Obtaining an Activation Key

To obtain an activation key, you need a Product Authorization Key, which you can purchase from your Cisco account representative. You need to purchase a separate Product Activation Key for each feature license. For example, if you have the Base License, you can purchase separate keys for Advanced Endpoint Assessment and for additional SSL VPN sessions.

After obtaining the Product Authorization Keys, register them on Cisco.com at one of the following URLs.

- If you are a registered user of Cisco.com, go to the following website:

http://www.cisco.com/go/license

- If you are not a registered user of Cisco.com, go to the following website:

http://www.cisco.com/go/license/public

Context Mode Guidelines

- In multiple context mode, apply the activation key in the system execution space.
- Shared licenses are not supported in multiple context mode.

Failover Guidelines

- Shared licenses are not supported in Active/Active mode.
- Failover units do not require the same license on each unit.

Older versions of ASA software required that the licenses match on each unit. Starting with Version 8.3(1), you no longer need to install identical licenses. Typically, you buy a license only for the primary unit; for Active/Standby failover, the secondary unit inherits the primary license when it becomes active. If you have licenses on both units, they combine into a single running failover cluster license.

- For the ASA 5505 and 5510, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license.

Upgrade and Downgrade Guidelines

Your activation key remains compatible if you upgrade to the latest version from any previous version. However, you might have issues if you want to maintain downgrade capability:

- Downgrading to Version 8.1 or earlier—After you upgrade, if you activate additional feature licenses that were added *before 8.2* , then the activation key continues to be compatible with earlier versions if you downgrade. However if you activate feature licenses that were added in *8.2 or later* , then the activation key is not backwards compatible. If you have an incompatible license key, then see the following guidelines:
  - If you previously entered an activation key in an earlier version, then the ASA uses that key (without any of the new licenses you activated in Version 8.2 or later).
  - If you have a new system and do not have an earlier activation key, then you need to request a new activation key compatible with the earlier version.
- Downgrading to Version 8.2 or earlier—Version 8.3 added more robust time-based key usage as well as failover license changes:
  - If you have more than one time-based activation key active, when you downgrade, only the most recently activated time-based key can be active. Any other keys are made inactive.
  - If you have mismatched licenses on a failover pair, then downgrading will disable failover. Even if the keys are matching, the license used will no longer be a combined license.

Additional Guidelines and Limitations

- The activation key is not stored in your configuration file; it is stored as a hidden file in flash memory.
- The activation key is tied to the serial number of the device. Feature licenses cannot be transferred between devices (except in the case of a hardware failure). If you have to replace your device due to a hardware failure, contact the Cisco Licensing Team to have your existing license transferred to the new serial number. The Cisco Licensing Team will ask for the Product Authorization Key reference number and existing serial number.
- Once purchased, you cannot return a license for a refund or for an upgraded license.
- Although you can activate all license types, some features are incompatible with each other; for example, multiple context mode and VPN. In the case of the AnyConnect Essentials license, the license is incompatible with the following licenses: full SSL VPN license, shared SSL VPN license, and Advanced Endpoint Assessment license. By default, the AnyConnect Essentials license is used instead of the above

licenses, but you can disable the AnyConnect Essentials license in the configuration to restore use of the other licenses using the **no anyconnect-essentials** command.

- Some permanent licenses require you to reload the ASA after you activate them. <xref> lists the licenses that require reloading.

Table 2: Permanent License Reloading Requirements

Model	License Action Requiring Reload
ASA 5505 and ASA 5510	Changing between the Base and Security Plus license.
All models	Changing the Encryption license.
All models	Downgrading any permanent license (for example, going from 10 contexts to 2 contexts).

Examples

The following example shows how to change the activation key on the ASA:

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

The following is sample output from the **activation-key** command that shows output for failover when the new activation key is different than the old activation key:

```
ciscoasa# activation-key 0xyadayada 0xyadayada 0xyadayada 0xyadayada 0xyadayada
Validating activation key. This may take a few minutes...
The following features available in the running permanent activation key are NOT available
 in the new activation key:
Failover is different.
   running permanent activation key: Restricted (R)
   new activation key: Unrestricted (UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with updating flash activation key? [y
]
Flash permanent activation key was updated with the requested key.
```

The following is sample output from a license file:

```
Serial Number Entered: 123456789ja
Number of Virtual Firewalls Selected: 10
Formula One device: ASA 5520
Failover                        : Enabled
VPN-DES                         : Enabled
VPN-3DES-AES                    : Enabled
Security Contexts               : 10
GTP/GPRS                        : Disabled
SSL VPN Peers                   : Default
Total VPN Peers                 : 750
Advanced Endpoint Assessment    : Disabled
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Disabled
Shared License                  : Disabled
UC Phone Proxy Sessions         : Default
Total UC Proxy Sessions         : Default
AnyConnect Essentials           : Disabled
Botnet Traffic Filter           : Disabled
Intercompany Media Engine       : Enabled
```

```
-----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ASA SOFTWARE RELEASE 8.2+ ONLY.
Platform = asa
123456789JA: yadayda1 yadayda1 yadayda1 yadayda1 yadayda1
-----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ALL ASA SOFTWARE RELEASES, BUT EXCLUDES ANY
8.2+ FEATURES FOR BACKWARDS COMPATIBILITY.
Platform = asa
123456789JA: yadayda2 yadayda2 yadayda2 yadayda2 yadayda2
```

Related Commands

Command	Description
anyconnect-essentials	Enables or disables the Anyconnect Essentials license.
show activation-key	Shows the activation key.
show version	Shows the software version and activation key.

activex-relay

To incorporate applications that need ActiveX over the clientless portal, use the **activex-relay** command in group-policy webvpn configuration mode or username webvpn configuration mode. To inherit the **activex-relay** command from the default group policy, use the **no** form of this command.

activex-relay { **enable** | **disable** }
no activex-relay

Syntax Description

enable	Enables ActiveX on WebVPN sessions.
disable	Disables ActiveX on WebVPN sessions.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **activex-relay enable** command to let users launch ActiveX from the WebVPN browser for any HTML content that has the object tags (such as images, audio, videos, JAVA applets, ActiveX, PDF, or flash). These applications use the WebVPN session to download and upload ActiveX controls. The ActiveX relay remains in force until the WebVPN session closes. If you plan to use something like Microsoft OWA 2007, you should disable ActiveX.

Note Because they have the same functionality, the **activex-relay enable** command generates smart tunnel logs even if smart tunnel is disabled.

The following example enables ActiveX controls on WebVPN sessions associated with a given group policy:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# activex-relay enable
```

The following example disables ActiveX controls on WebVPN sessions associated with a given username:

```
ciscoasa(config-username-policy)# webvpn
ciscoasa(config-username-webvpn)# activex-relay disable
```



ad - aq

- ad-agent-mode, on page 153
- address (dynamic-filter blacklist, whitelist), on page 155
- address (media-termination) (Deprecated), on page 158
- address-family ipv4, on page 160
- address-family ipv6, on page 162
- address-pool, on page 163
- address-pools, on page 165
- admin-context, on page 167
- advertise passive-only, on page 169
- aggregate-address, on page 173
- alarm contact description, on page 175
- alarm contact severity, on page 177
- alarm contact trigger, on page 179
- alarm facility input-alarm, on page 181
- alarm facility power-supply rps, on page 183
- alarm facility temperature (actions), on page 185
- alarm facility temperature (high and low thresholds), on page 187
- allocate-interface, on page 189
- allocate-ips, on page 192
- allowed-eid, on page 194
- allow-ssc-mgmt, on page 196
- allow-tls, on page 198
- always-on-vpn, on page 200
- anti-replay, on page 201
- anyconnect ask, on page 203
- anyconnect-custom (Version 9.0 through 9.2), on page 205
- anyconnect-custom (Version 9.3 and later), on page 207
- anyconnect-custom-attr (Version 9.0 through 9.2), on page 209
- anyconnect-custom-attr (Version 9.3 and later), on page 211
- anyconnect-custom-data, on page 213
- anyconnect df-bit-ignore, on page 215
- anyconnect dpd-interval, on page 216
- anyconnect dtls compression, on page 218

- anyconnect enable, on page 219
- anyconnect-essentials, on page 221
- anyconnect external-browser-pkg, on page 223
- anyconnect firewall-rule, on page 225
- anyconnect image, on page 227
- anyconnect keep-installer, on page 230
- anyconnect modules, on page 232
- anyconnect mtu, on page 234
- anyconnect profiles (group-policy attributes webvpn, username attributes webvpn), on page 236
- anyconnect profiles (webvpn), on page 238
- anyconnect ssl compression, on page 240
- anyconnect ssl df-bit-ignore, on page 242
- anyconnect ssl dtls enable, on page 244
- anyconnect ssl keepalive, on page 246
- anyconnect ssl rekey, on page 248
- apcf(Deprecated), on page 250
- app-agent heartbeat, on page 252
- app-id, on page 254
- appl-acl, on page 255
- application-access, on page 257
- application-access hide-details, on page 259

ad-agent-mode

To enables the AD Agent mode so that you can configure the Active Directory Agent for the Cisco Identify Firewall instance, use the **ad-agent-mode** command in global configuration mode.

ad-agent-mode

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

To configure the Active Directory Agent for the Identity Firewall, you must enter the **ad-agent-mode** command, which is a submode of the **aaa-server** command. Entering the **ad-agent-mode** command enters the aaa server group configuration mode.

Periodically or on-demand, the AD Agent monitors the Active Directory server security event log file via WMI for user login and logoff events. The AD Agent maintains a cache of user ID and IP address mappings. and notifies the ASA of changes.

Configure the primary and secondary AD Agents for the AD Agent Server Group. When the ASA detects that the primary AD Agent is not responding and a secondary agent is specified, the ASA switches to the secondary AD Agent. The Active Directory server for the AD agent uses RADIUS as the communication protocol; therefore, you should specify a key attribute for the shared secret between the ASA and AD Agent.

Examples

The following example shows how to enable **ad-agent-mode** while configuring the Active Directory Agent for the Identity Firewall:

```
ciscoasa(config)# aaa-server adagent protocol radius
ciscoasa(config)# ad-agent-mode
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
ciscoasa(config-aaa-server-host)# key mysecret
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

Related Commands

Command	Description
aaa-server	Creates a AAA server group and configures AAA server parameters that are group-specific and common to all group hosts.
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

address (dynamic-filter blacklist, whitelist)

To add an IP address to the Botnet Traffic Filter blacklist or whitelist, use the **address** command in dynamic-filter blacklist or whitelist configuration mode. To remove the address, use the **no** form of this command.

address *ip_address mask*
no address *ip_address mask*

Syntax Description

ip_address	Adds an IP address to the blacklist.
mask	Defines the subnet mask for the IP address. The *mask* can be for a single host or for a subnet.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dynamic-filter blacklist or whitelist configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The static database lets you augment the dynamic database with domain names or IP addresses that you want to whitelist or blacklist. After you enter the dynamic-filter whitelist or blacklist configuration mode, you can manually enter domain names or IP addresses (host or subnet) that you want to tag as good names in a whitelist or bad names in a blacklist using the **address** and **name** commands.

You can enter this command multiple times for multiple entries. You can add up to 1000 blacklist and 1000 whitelist entries.

Examples

The following example creates entries for the blacklist and whitelist:

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
```

```
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

Related Commands

Command	Description
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.

Command	Description
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

address (media-termination) (Deprecated)

To specify the address for a media termination instance to use for media connections to the Phone Proxy feature, use the **address** command in the media-termination configuration mode. To remove the address from the media termination configuration, use the **no** form of this command.

address *ip_address* [**interface** *intf_name*]
no address *ip_address* [**interface** *intf_name*]

Syntax Description

interface *intf_name*	Specifies the name of the interface for which the media termination address is used. Only one media-termination address can be configured per interface.
ip_address	Specifies the IP address to use for the media termination instance.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Media-termination configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** and **uc-ime** commands.

Usage Guidelines

The ASA must have IP addresses for media termination that meet the following criteria:

- For the media termination instance, you can configure a global media-termination address for all interfaces or configure a media-termination address for different interfaces. However, you cannot use a global media-termination address and media-termination addresses configured for each interface at the same time.
- If you configure a media termination address for multiple interfaces, you must configure an address on each interface that the ASA uses when communicating with IP phones.
- The IP addresses are publicly routable addresses that are unused IP addresses within the address range on that interface.

Examples

The following example shows the use of the media-termination address command to specify the IP address to use for media connections:

```
ciscoasa(config)# media-termination mediaterm1
ciscoasa(config-media-termination)# address 192.0.2.25 interface inside
ciscoasa(config-media-termination)# address 10.10.0.25 interface outside
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
media-termination	Configures the media termination instance to apply to a Phone Proxy instance.

address-family ipv4

To enter address family to configure a routing session using standard IP Version 4 (IPv4) address prefixes, use the address-family ipv4 command in router configuration mode. To exit address family configuration mode and remove the IPv4 address family configuration from the running configuration, use the no form of this command.

address-family ipv4
no address-family ipv4

Command Default

IPv4 address prefixes are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router mode configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The address-family ipv4 command places the context router in address family configuration mode, from which you can configure routing sessions that use standard IPv4 address prefixes. To leave address family configuration mode and return to router configuration mode, type exit.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the neighbor remote-as command unless you enter the no bgp default ipv4-unicast command before configuring the neighbor remote-as command.

Examples

The following example places the router in address family configuration mode for the IPv4 address family:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)#
```

Related Commands

Command	Description
bgp default ipv4-unicast	Sets the IP version 4 (IPv4) unicast address family as default for BGP peering session.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

address-family ipv6

To enter address family to configure a routing session such as BGP that use using standard IP Version 6 (IPv6) address prefixes, use the address-family ipv6 command in router configuration mode. To exit address family configuration mode and remove the IPv6 address family configuration from the running configuration, use the no form of this command.

address-family ipv6 [**unicast**]
no address-family ipv6

Syntax Description

unicast	(Optional) Specifies IPv6 unicast address prefixes.

Command Default

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router mode configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

The address-family ipv6 command places the context router in address family configuration mode, from which you can configure routing sessions that use standard IPv6 address prefixes. To leave address family configuration mode and return to router configuration mode, type exit.

Examples

The following example places the router in address family configuration mode for the IPv4 address family:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af)#
```

Related Commands

Command	Description
neighbor ipv6-address activate	Enables exchange of information with a BGP neighbor.

address-pool

To specify a list of address pools for allocating addresses to remote clients, use the **address-pool** command in tunnel-group general-attributes configuration mode. To eliminate address pools, use the **no** form of this command.

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]
no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

Syntax Description

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
interface name	(Optional) Specifies the interface to be used for the address pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

The address-pools settings in the group-policy **address-pools** command override the local pool settings in the tunnel group **address-pool** command.

The order in which you specify the pools is significant. The ASA allocates addresses from these pools in the order in which the pools appear in this command.

Examples

The following example entered in config-tunnel-general configuration mode, specifies a list of address pools for allocating addresses to remote clients for an IPsec remote-access tunnel group test:

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN remote-access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

address-pools

To specify a list of address pools for allocating addresses to remote clients, use the **address-pools** command in group-policy attributes configuration mode. To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command.

address-pools value *address_pool1* [*...address_pool6*]
no address-pools value *address_pool1* [*...address_pool6*]
address-pools none
no address-pools none

Syntax Description

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
none	Specifies that no address pools are configured and disables inheritance from other sources of group policy.
value	Specifies a list of up to 6 address pools from which to assign addresses.

Command Default

By default, the address pool attribute allows inheritance.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The address pools settings in this command override the local pool settings in the group. You can specify a list of up to six local address pools to use for local address allocation.

The order in which you specify the pools is significant. The ASA allocates addresses from these pools in the order in which the pools appear in this command.

The command **address-pools none** disables this attribute from being inherited from other sources of policy, such as the DefaultGrpPolicy. The command **no address pools none** removes the **address-pools none** command from the configuration, restoring the default value, which is to allow inheritance.

Examples

The following example entered in config-general configuration mode, configures pool_1 and pool_20 as lists of address pools to use for allocating addresses to remote clients for GroupPolicy1:

```
ciscoasa(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
ciscoasa(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# address-pools value pool_1 pool_20
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN group policies.
clear configure group-policy	Clears all configured group policies.
show running-config group-policy	Shows the configuration for all group policies or for a particular group policy.

admin-context

To set the admin context for the system configuration, use the **admin-context** command in global configuration mode.

admin-context *name*

Syntax Description

name Sets the name as a string up to 32 characters long. If you have not defined any contexts yet, then first specify the admin context name with this command. Then, the first context you add using the **context** command must be the specified admin context name.

This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen.

"System" or "Null" (in upper or lowercase letters) are reserved names, and cannot be used.

Command Default

For a new ASA in multiple context mode, the admin context is called "admin."

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can set any context to be the admin context, as long as the context configuration resides on the internal Flash memory.

You cannot remove the current admin context, unless you remove all contexts using the **clear configure context** command.

The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the ASA software or allowing remote management for an administrator), it uses one of the contexts that is designated as the admin context.

Examples

The following example sets the admin context to be "administrator":

```
ciscoasa(config)# admin-context administrator
```

Related Commands

Command	Description
clear configure context	Removes all contexts from the system configuration.
context	Configures a context in the system configuration and enters context configuration mode.
show admin-context	Shows the current admin context name.

advertise passive-only

To configure IS-IS to advertise only prefixes that belong to passive interfaces, use the **advertise passive-only** command in router isis configuration mode. To remove the restriction, use the **no** form of this command.

advertise passive-only
no advertise passive-only

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command is an IS-IS mechanism to exclude IP prefixes of connected networks from link-state packet (LSP) advertisements, thereby reducing IS-IS convergence time.

Configuring this command per IS-IS instance is a scalable solution to reduce IS-IS convergence time because fewer prefixes will be advertised in the router nonpseudonode LSP.

This command relies on the fact that when enabling IS-IS on a loopback interface, you usually configure the loopback as passive (to prevent sending unnecessary hello packets out through it because there is no chance of finding a neighbor behind it). Thus, if you want to advertise only the loopback and if it has already been configured as passive, configuring the **advertise passive-only** command per IS-IS instance would prevent the overpopulation of the routing tables.

An alternative to this command is the **no isis advertise-prefix** command. The **no isis advertise-prefix** command is a small-scale solution because it is configured per interface.

Examples

The following example uses the **advertise passive-only** command, which affects the IS-IS instance, and thereby prevents advertising the IP network of Ethernet interface 0. Only the IP address of loopback interface 0 is advertised.

```
!
!
!
interface Gi0/0
```

```
 ip address 192.168.20.1 255.255.255.0
router isis
!.
int gi0/1
  ip add 171.1.1.1 255.255.255.0
   router isis
!.
router isis
 passive-interface outside
 net 47.0004.004d.0001.0001.0c11.1111.00
 advertise-passive-only
 log-adjacency-changes
!
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface

Command	Description
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.

Command	Description
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the aggregate-address command in address family configuration mode. To disable this function, use the no form of this command.

aggregate-address *address mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]
no aggregate-address *address mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]

Syntax Description

address	Aggregate address.
mask	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map map-name	(Optional) Specifies the name of the route map used to select the routes to be suppressed.
advertise-map map-name	(Optional) Specifies the name of the route map used to select the routes to create AS_SET origin communities.
attribute-map map-name	(Optional) Specifies the name of the route map used to set the attribute of the aggregate route.

Command Default

The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the as-set keyword is specified

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Context configuration, Address family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified, to be supported in address-family ipv6 sub-mode.

Usage Guidelines

You can implement aggregate routing in BGP and Multiprotocol BGP (mBGP) either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature.

Using the aggregate-address command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix that matches the aggregate must exist in the Routing Information Base (RIB).) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the as-set keyword.)

Using the as-set keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the aggregate-address command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reach ability information for the summarized routes changes.

Using the summary-only keyword not only creates the aggregate route (for example, 192.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the neighbor distribute-list command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the suppress-map keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the match clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the advertise-map keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the aggregate-address command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists match clauses are supported.

Using the attribute-map keyword allows attributes of the aggregate route to be changed. This form of the aggregate-address command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

Examples

The following example creates an aggregate route and suppresses advertisements of more specific routes to all neighbors.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

Related Commands

Command	Description
address-family ipv4	Enters the address family configuration mode to configure a routing session using standard IP Version 4.

alarm contact description

To enter a description for the alarm inputs in the ISA 3000, use the **alarm contact description** command in global configuration mode. To set the default description to the corresponding contact number, use the no form of this command.

alarm contact { **1** | **2** } **description** *string*
no alarm contact { **1** | **2** } **description**

Syntax Description

1 | 2	Specifies the alarm contact for which the description is configured. Enter 1 or 2.
string	Specifies the description. This may be up to 80 alphanumeric characters long, and will be included in syslog messages.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Examples

The following example specifies the description for the alarm contact 1:

```
ciscoasa(config)# alarm contact 1 description Door Open
```

Related Commands

Command	Description
alarm contact severity	Specifies the severity of an alarm which will in turn affect the LED state in the ISA 3000.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.

Command	Description
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

alarm contact severity

To specify the severity of an alarm in the ISA 3000, use the **alarm contact severity** command in global configuration mode. To revert to the default severity, use the no form of this command.

alarm contact { **1** | **2** | **all** } **severity** { **major** | **minor** | **none** }
no alarm contact { **1** | **2** | **all** } **severity**

Syntax Description

{**1** | **2** | **all**}	Specifies the alarm contact for which you are setting the severity. Enter 1, 2, or all.
severity {**major** | **minor** | **none**}	The severity of the alarm triggered by this alarm contact. Besides labeling the alarm with this severity, the severity controls the behavior of the LED associated with the contact. • **major**—The LED blinks red. • **minor**—The LED is solid red. This is the default. • **none**—The LED is off.

Command Default

By default, the severity is minor.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Examples

The following example specifies the severity for the alarm contact 1:

```
ciscoasa(config)# alarm contact 1 severity major
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.

Command	Description
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

alarm contact trigger

To specify a trigger for one or all alarm inputs in the ISA 3000, use the **alarm contact trigger** command in global configuration mode. To revert to the default trigger, use the **no** form of this command.

alarm contact { **1** | **2** | **all** } **trigger** { **open** | **closed** }
alarm contact { **1** | **2** | **all** } **trigger**

Syntax Description

{**1** | **2** | **all**}	Specifies the alarm contact for which you are setting the trigger. Enter 1, 2, or all.
trigger {**open** | **closed**}	The trigger determines the electrical condition that signals an alert. • **open**—The normal condition for the contact is closed, that is, the electrical current is running through the contact. An alert is triggered if the contact becomes open, that is, the electrical current stops flowing. • **closed**—The normal condition for the contact is open, that is, the electrical current does not run through the contact. An alert is triggered if the contact becomes closed, that is, the electrical current starts running through the contact. This is the default.

Command Default

By default, the closed state is the trigger.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Examples

The following example sets the trigger for the alarm contact 1:

```
ciscoasa(config)# alarm contact 1 trigger open
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.

Command	Description
alarm contact severity	Specifies the severity of alarms.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

alarm facility input-alarm

To specify the logging and notification options for alarm inputs in the ISA 3000, use the **alarm facility input-alarm** command in global configuration mode. To remove the logging and notification options, use the **no** form of this command.

alarm facility input-alarm { **1** | **2** } { **notifies** | **relay** | **syslog** }
no alarm facility input-alarm { **1** | **2** } { **notifies** | **relay** | **syslog** }

Syntax Description

{**1** | **2**}	Specifies the alarm contact, 1 or 2.
notifies	Enables the transmission of SNMP traps when an alarm is triggered.
relay	Enables the hardware output relay when an alarm is triggered, which activates the attached external alarm.
syslog	Enables the transmission of syslog messages when an alarm is triggered and when the alarm condition ends.

Command Default

Syslog is enabled by default, the other options are disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Examples

The following examples specify the logging and notification options for alarm input 1:

```
ciscoasa(config)# alarm facility input-alarm 1 notifies
ciscoasa(config)# alarm facility input-alarm 1 relay
ciscoasa(config)# alarm facility input-alarm 1 syslog
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

alarm facility power-supply rps

To configure power supply alarms in the ISA 3000, use the **alarm facility power-supply rps** command in global configuration mode. To disable the power supply alarm, relay, SNMP traps and syslog, use the **alarm facility power-supply rps disable** command or the **no** version.

alarm facility power-supply rps { **disable** | **notifies** | **relay** | **syslog** }
no alarm facility power-supply rps { **disable** | **notifies** | **relay** | **syslog** }

Syntax Description

disable	Disables the power supply alarm, relay, SNMP traps and syslog.
notifies	Enables the transmission of SNMP traps when an alarm is triggered.
relay	Enables the hardware output relay when an alarm is triggered, which activates the attached external alarm.
syslog	Enables the transmission of syslog messages when an alarm is triggered and when the alarm condition ends.

Command Default

By default, **syslog** is enabled, **relay** and **notifies** are disabled. The alarm is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

The ISA 3000 has two power supplies. By default, the system operates in single-power mode. However, you can configure the system to operate in dual mode, where the second power supply automatically provides power if the primary power supply fails. When you enable dual-mode, the power supply alarm is automatically enabled to send syslog alerts, but you can disable the alert altogether, or also enable SNMP traps or the alarm hardware relay.

The **alarm facility power-supply rps disable** command disables the power supply alarm, relay, traps and syslog. Using the **no alarm facility power-supply rps disable** command enables only the power supply alarm. You must enable the relay, SNMP traps, and syslog separately.

You must also configure the **power-supply dual** command to enable dual mode. The alarm is automatically enabled in dual mode.

Examples

The following example enables dual power supply mode and configures all alert options.

```
ciscoasa(config)# power-supply dual
ciscoasa(config)# alarm facility power-supply rps relay
ciscoasa(config)# alarm facility power-supply rps syslog
ciscoasa(config)# alarm facility power-supply rps notifies
```

The following example disables the dual power supply alarm:

```
ciscoasa(config)# alarm facility power-supply rps disable
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

alarm facility temperature (actions)

To configure the temperature alarms in the ISA 3000, use the **alarm facility temperature** command in global configuration mode. To disable the temperature alarms, use the **no** form of the command.

alarm facility temperature { **primary** | **secondary** } { **notifies** | **relay** | **syslog** }
no alarm facility temperature { **primary** | **secondary** } { **notifies** | **relay** | **syslog** }

Syntax Description

primary	Configures the primary temperature alarm.
secondary	Configures the secondary temperature alarm.
notifies	Enables the transmission of SNMP traps when an alarm is triggered.
relay	Enables the hardware output relay when an alarm is triggered, which activates the attached external alarm.
syslog	Enables the transmission of syslog messages when an alarm is triggered and when the alarm condition ends.

Command Default

The primary temperature alarm is enabled for all alarm actions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

You can configure alarms based on the temperature of the CPU card in the device.

You can set a primary and secondary temperature range using the **alarm facility temperature** command with the **high** and **low** keywords. If the temperature drops below the low threshold, or exceeds the high threshold, the alarm is triggered.

The primary temperature alarm is enabled by default for all alarm actions: output relay, syslog, and SNMP. The default settings for the primary temperature range is -40°C to 92°C.

The secondary temperature alarm is disabled by default. You can set the secondary temperature within the range -35°C to 85°C.

Because the secondary temperature range is more restrictive than the primary range, if you set either the secondary low or high temperature, that setting disables the corresponding primary setting, even if you configure non-default values for the primary setting. You cannot enable two separate high and two separate low temperature alarms.

Thus, in practice, you should configure the primary only, or the secondary only, setting for high and low.

Examples

The following example sets the high and low temperatures for the secondary alarm and enables all alert actions.

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

alarm facility temperature (high and low thresholds)

To configure the high and low temperature threshold values in the ISA 3000, use the **alarm facility temperature** {**low** | **high**} command in global configuration mode. To remove the threshold values, or to revert the primary value to the default, use the **no** form of the command.

alarm facility temperature { **primary** | **secondary** } { **high** | **low** } *threshold*
no alarm facility temperature { **primary** | **secondary** } { **high** | **low** } *threshold*

Syntax Description

primary	Configures the primary temperature alarm.
secondary	Configures the secondary temperature alarm.
high *threshold*	Configures the high threshold in Celsius. The maximum for primary is 92. The maximum for secondary is 85.
low *threshold*	Configures the low threshold in Celsius. The minimum for primary is -40. The minimum for secondary is -35.

Command Default

The default primary high temperature is 92°C, the low is –40°C.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

You can configure alarms based on the temperature of the CPU card in the device.

You can set a primary and secondary temperature range using the **alarm facility temperature** command with the **high** and **low** keywords. If the temperature drops below the low threshold, or exceeds the high threshold, the alarm is triggered.

The primary temperature alarm is enabled by default for all alarm actions: output relay, syslog, and SNMP. The default settings for the primary temperature range is -40°C to 92°C.

The secondary temperature alarm is disabled by default. You can set the secondary temperature within the range -35°C to 85°C.

Because the secondary temperature range is more restrictive than the primary range, if you set either the secondary low or high temperature, that setting disables the corresponding primary setting, even if you

configure non-default values for the primary setting. You cannot enable two separate high and two separate low temperature alarms.

Thus, in practice, you should configure the primary only, or the secondary only, setting for high and low.

Examples

The following example sets the high and low temperatures for the secondary alarm and enables all alert actions.

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

allocate-interface

To allocate interfaces to a security context, use the **allocate-interface** command in context configuration mode. To remove an interface from a context, use the **no** form of this command.

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]
no allocate-interface *physical_interface*
allocate-interface *physical_interface* **.** *subinterface* [**-** *physical interface* **.** *subinterface*] [*map_name* [**-** *map_name*]] [**visible** | **invisible**]
no allocate-interface *physical_interface* **.** *subinterface* [**-** *physical interface* **.** *subinterface*]

Syntax Description

invisible	(Default) Allows context users to only see the mapped name (if configured) in the **show interface** command.

map_name	(Optional) Sets a mapped name.
	The *map_name* is an alphanumeric alias for the interface that can be used within the context instead of the interface ID. If you do not specify a mapped name, the interface ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces are being used by the context.
	A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names:
	`int0`
	`inta`
	`int_0`
	For subinterfaces, you can specify a range of mapped names.
	See the "Usage Guidelines" section for more information about ranges.

physical_interface	Sets the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values. Do not include a space between the interface type and the port number.
subinterface	Sets the subinterface number. You can identify a range of subinterfaces.
visible	(Optional) Allows context users to see physical interface properties in the **show interface** command even if you set a mapped name.

Command Default

The interface ID is invisible in the **show interface** command output by default if you set a mapped name.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Contxt configuration	• Yes	• Yes	—	—	

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can enter this command multiple times to specify different ranges. To change the mapped name or visible setting, reenter the command for a given interface ID, and set the new values; you do not need to enter the **no allocate-interface** command and start over. If you remove the **allocate-interface** command, the ASA removes any interface-related configuration in the context.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA , you can use the dedicated management interface, Management 0/0, (either the physical interface or a subinterface) as a third interface for management traffic.

Note The management interface for transparent mode does not flood a packet out the interface when that packet is not in the MAC address table.

You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.

If you specify a range of subinterfaces, you can specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range:

```
int0-int10
```

If you enter **gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5**, for example, the command fails.

- The numeric portion of the mapped name must include the same quantity of numbers as the subinterface range. For example, both ranges include 100 interfaces:

```
gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
```

If you enter **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15**, for example, the command fails.

Examples

The following example shows gigabitethernet0/1.100, gigabitethernet0/1.200, and gigabitethernet0/2.300 through gigabitethernet0/1.305 assigned to the context. The mapped names are int1 through int8.

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.
show interface	Displays the runtime status and statistics of interfaces.
vlan	Assigns a VLAN ID to a subinterface.

allocate-ips

To allocate an IPS virtual sensor to a security context if you have the AIP SSM installed, use the **allocate-ips** command in context configuration mode. To remove a virtual sensor from a context, use the **no** form of this command.

allocate-ips *sensor_name* [*mapped_name*] [**default**]
no allocate-ips *sensor_name* [*mapped_name*] [**default**]

Syntax Description

default	(Optional) Sets one sensor per context as the default sensor; if the context configuration does not specify a sensor name, the context uses this default sensor. You can only configure one default sensor per context. If you want to change the default sensor, enter the **no allocate-ips** command to remove the current default sensor before you allocate a new default sensor. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor on the AIP SSM.
mapped_name	(Optional) Sets a mapped name as an alias for the sensor name that can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called “sensor1” and “sensor2,” then you can map the “highsec” and “lowsec” senors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.
sensor_name	Sets the sensor name configured on the AIP SSM. To view the sensors that are configured on the AIP SSM, enter **allocate-ips ?**. All available sensors are listed. You can also enter the **show ips** command. In the system execution space, the **show ips** command lists all available sensors; if you enter it in the context, it shows the sensors you already assigned to the context. If you specify a sensor name that does not yet exist on the AIP SSM, you get an error, but the **allocate-ips** command is entered as-is. Until you create a sensor of that name on the AIP SSM, the context assumes the sensor is down.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Context configuration	• Yes	• Yes	—	—	

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

You can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the AIP SSM using the **ips** command, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the AIP SSM is used. You can assign the same sensor to multiple contexts.

Note You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

Examples

The following example assigns sensor1 and sensor2 to context A, and sensor1 and sensor3 to context B. Both contexts map the sensor names to "ips1" and "ips2." In context A, sensor1 is set as the default sensor, but in context B, no default is set so the default that is configured on the AIP SSM is used.

```
ciscoasa(config-ctx)# context
 A
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1 default
ciscoasa(config-ctx)# allocate-ips sensor2 ips2
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold
ciscoasa(config-ctx)# context
 sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1
ciscoasa(config-ctx)# allocate-ips sensor3 ips2
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
ips	Diverts traffic to the AIP SSM for inspection.
show context	Shows a list of contexts (system execution space) or information about the current context.
show ips	Shows the virtual sensors configured on the AIP SSM.

allowed-eid

To configure a LISP inspection map to limit inspected EIDs based on IP address, use the **allowed-eid** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect lisp** command. To allow all EIDs, use the **no** form of this command.

allowed-eid access-list *eid_acl_name*
no allowed-eid access-list *eid_acl_name*

Syntax Description

access-list *eid_acl_name*	Specifies an extended ACL where only the destination IP address is matched to the EID embedded address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	We introduced this command.

Usage Guidelines

Configure a LISP inspection map to limit inspected EIDs based on IP address.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.

3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.
4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following example limits EIDs to those on the 10.10.10.0/24 network:

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

allow-ssc-mgmt

To set an interface on the ASA 5505 to be the SSC management interface, use the **allow-ssc-mgmt** command in interface configuration mode. To unassign an interface, use the **no** form of this command.

allow-ssc-mgmt
no allow-ssc-mgmt

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled in the factory default configuration for VLAN 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

An SSC does not have any external interfaces. You can configure a VLAN as a management VLAN to allow access to an internal management IP address over the backplane. By default, VLAN 1 is enabled for the SSC management address. You can only assign one VLAN as the SSC management VLAN.

Do not configure NAT for the management address if you intend to access it using ASDM. For initial setup with ASDM, you need to access the real address. After initial setup (where you set the password in the SSC), you can configure NAT and supply ASDM with the translated address when you want to access the SSC.

Examples

The following example disables management access on VLAN 1, and enables it for VLAN 2:

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# no allow-ssc-mgmt
ciscoasa(config-if)# interface vlan 2
ciscoasa(config-if)# allow-ssc-mgmt
```

Related Commands

Command	Description
interface	Configures an interface.
ip address	Sets the management IP address for a bridge group.

Command	Description
nameif	Sets the interface name.
security-level	Sets the interface security level.
hw-module module ip	Configures the management IP address for the SSC.
hw-module module allow-ip	Sets the hosts that are allowed to access the management IP address.

allow-tls

To configure ESMTP inspection to allow or prohibit TLS sessions, use the **allow-tls** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

allow-tls [**action log**]
no allow-tls

Syntax Description

action log	Whether to log encrypted connections.

Command Default

The **allow-tls** command is the default for ESMTP inspection.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(3)	This command was added.
9.4(1)	The default was changed to **allow-tls** from **no allow-tls.** However, this default applies to new or reimaged systems. If you upgrade a system that includes **no allow-tls**, the command is not changed.

Usage Guidelines

ESMTP inspection cannot inspect encrypted connections. If you want to enforce inspection of all ESMTP sessions, use the **no allow-tls** command. By disallowing TLS, the STARTTLS indicator is removed from connection requests, forcing the client and server to negotiate clear text connections.

If you want to allow the client and server to negotiate encrypted connections, include the **allow-tls** command in the parameters section of an ESMTP inspection policy map, and connect the map to the ESMTP inspection service policy. You can also edit the _default_esmtp_map, which is applied when you do not apply your own map.

Examples

The following example shows how to allow encrypted ESMTP sessions, which bypasses ESMTP inspection:

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# allow-tls
```

Related Commands

Command	Description
policy-map type inspect esmtp	Configures an ESMTP policy map for inspection.

always-on-vpn

To configure the behavior of the Secure Client Always-On-VPN functionality, use the **always-on-vpn** command in group policy configuration mode.

always-on-vpn [**profile-setting | disable**]

Syntax Description

disable	Switches off the Always-On-VPN functionality.
profile-setting	Uses the **always-on-vpn** setting configured in the Secure Client profile.

Command Default

Always-On-VPN functionality is switched on by default.

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

To enable Always-On-VPN functionality for Secure Client users, configure an Secure Client profile in the profile editor. Then configure the group-policy attributes for the appropriate policy.

Examples

The following example enables always-on functionality for the configured group-policy:

```
ciscoasa(config)# group-policy <group policy> attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# always-on-vpn profile-setting
```

Related Commands

Command	Description
webvpn	Configures group policy for WebVPN.

anti-replay

To enable anti-replay for GTP-U message sequence numbers, use the **anti-replay** command in GTP inspection policy map parameters configuration mode. Use the **no** form of this command disable anti-replay.

anti-replay [*window_size*]
no anti-replay [*window_size*]

Syntax Description

window_size	The size of the sliding window in number of messages. The window size can be 128, 256, 512, or 1024. If you do not enter a value, you get the default, 512.

Command Default

By default, anti-replay is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

You can enable anti-replay by specifying a sliding window for GTP-U messages.

The size of the sliding window is in number of messages and can be 128, 256, 512, or 1024. As valid messages appear, the window moves to the new sequence numbers. Sequence numbers are in the range 0-65535, wrapping when they reach the maximum, and they are unique per PDP context. Messages are considered valid if their sequence numbers are within the window.

Anti-replay helps prevent session hijacking or DoS attacks, which can occur when a hacker captures GTP data packets and replays them.

Examples

The following example enables anti-replay with a window size of 512.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# anti-replay 512
```

Related Commands

Commands	Description
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.
show service-policy inspect gtp	Displays the GTP configuration and statistics.

anyconnect ask

To enable the ASA to prompt remote SSL VPN client users to download the client, use the **anyconnect ask** command in group policy webvpn or username webvpn configuration modes. To remove the command from the configuration, use the **no** form of the command.

anyconnect ask { **none** | **enable** [**default** { **webvpn** | **anyconnect** } **timeout** *value*] }
no anyconnect ask none [**default** { **webvpn** | **anyconnect** }]

Syntax Description

default anyconnect timeout *value*	Prompts the remote user to download the client or goes to the portal page for clientless connections, and waits the duration of *value* before taking the default action—downloading the client.
default webvpn timeout *value*	Prompts the remote user to download the client or goes to the portal page for clientless connections, and waits the duration of *value* before taking the default action—displaying the WebVPN portal page.
enable	Prompts the remote user to download the client or goes to the portal page for clientless connections and waits indefinitely for user response.
none	Immediately performs the default action.

Command Default

The default for this command is anyconnect **ask none default webvpn**. The ASA immediately displays the portal page for clientless connections.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.4(1)	The anyconnect ask command replaced the svc ask command.

Usage Guidelines

<xref> shows the prompt displayed to remote users when either the **default** anyconnect **timeout** *value* command *or* **default webvpn timeout** *value* command *is configured:*

Examples

The following example configures the ASA to prompt the remote user to download the client or go to the portal page and to wait *10 seconds for user response* before downloading the client:

```
ciscoasa(config-group-webvpn)# anyconnect ask enable default svc timeout 10
```

Related Commands

Command	Description
show webvpn anyconnect	Displays information about installed SSL VPN clients.
anyconnect	Enables or requires the SSL VPN client for a specific group or user.
anyconnect image	Specifies a client package file that the ASA expands in cache memory for downloading to remote PCs.

anyconnect-custom (Version 9.0 through 9.2)

To set or update the value of a custom attribute, use the **anyconnect-custom** command in anyconnect-custom-attr configuration mode. To remove the value of a custom attribute, use the **no** form of this command.

anyconnect-custom *attr-name* **value** *attr-value*
anyconnect-custom *attr-name* **none**
no anyconnect-custom *attr-name*

Syntax Description

attr-name	The name of the attribute in the current group policy, as defined by the **anyconnnect-custom-attr** command.
none	Immediately performs the default action.
value *attr-value*	A string containing the attribute value. The value is associated with the attribute name and passed to the client during connection setup. The maximum length is 450 characters.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
anyconnect-custom-attr configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command sets the value of a custom attribute in a group policy. The *AnyConnect Administrator's Guide* lists which values are valid for the custom attributes that apply to that release. Custom attributes are created with the **anyconnect-custom-attr** command.

Multiple instances of this command are supported to build a multiline value for an attribute. All data associated with a given attribute name is delivered to the client in the order that it is entered in the CLI. Individual lines of a multiline value can not be removed.

The **no** form of this command does not allow the **value** or **none** keywords.

If the data associated with an attribute name is entered in multiple CLI lines, it will be sent to the endpoint as a single concatenated string delimited by the newline character (\n).

Examples

The following example configures a custom attribute for an AnyConnect Deferred Update:

```
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed true
```

Related Commands

Command	Description
show run webvpn	Displays configuration information about WebVPN, including **anyconnect** commands.
show run group-policy	Displays configuration information about current group policies.
anyconnect-custom-attr	Creates custom attributes.

anyconnect-custom (Version 9.3 and later)

To set or update the value of a custom attribute, use the **anyconnect-custom** command in group-policy or dynamic-access-policy-record configuration mode. To remove a custom attribute, use the **no** form of this command.

anyconnect-custom *attr-type* **value** *attr-name*
anyconnect-custom *attr-type* **none**
no anyconnect-custom *attr-type*

Syntax Description

attr-type	The type of custom attribute as defined by the **anyconnnect-custom-attr** command.
none	This custom attribute is explicitly omitted from the policy.
value *attr-name*	The name of the custom attribute value as defined by the **anyconnect-custom-data** command. The custom attribute type and named value is passed to the client during connection setup.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
group-policy or dynamic-access-policy-record	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.3(1)	This command has been redefined.

Usage Guidelines

This command sets the value of a custom attribute in a group policy or DAP.

The *AnyConnect Administrator's Guide* lists which values are valid for the custom attributes that apply to that release. Custom attributes are created with the **anyconnect-custom-attr** and **anyconnect-custom-data** commands.

The **no** form of this command does not allow the **none** keyword.

Examples

The following example configures a custom attribute for AnyConnect Deferred Update:

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
ciscoasa(config-webvpn)# exit
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed def-allowed
```

Related Commands

Command	Description
show run webvpn	Displays configuration information about WebVPN, including **anyconnect** commands.
show run group-policy	Displays configuration information about current group policies.
show running-config dynamic-access-policy-record	Display custom attributes used in DAP policies.
anyconnect-custom-attr	Creates custom attribute types used by this command.
anyconnect-custom-data	Creates custom attribute named values used by this command.

anyconnect-custom-attr (Version 9.0 through 9.2)

To create custom attributes, use the **anyconnect-custom-attr** command in Anyconnect-custom-attr configuration mode. To remove custom attributes, use the **no** form of this command.

[**no**] **anyconnect-custom-attr** *attr-name* [**description** *description*]

Syntax Description

attr-name	The name of the attribute. This name is referenced in the group policy syntax and in the aggregate auth protocol messages. The maximum length is 32 characters.
description *description*	A free form description of attribute usage. This text appears in the command help when the custom attribute is referenced from the group-policy attribute configuration mode. The maximum length is 128 characters.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Anyconnect-custom-attr configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command creates custom attributes to support special Secure Client features. After creating custom attributes for a particular feature, you add them to group policies, so that feature can be applied to VPN clients. This command guarantees that all of the defined attribute names are unique.

Some versions of Secure Client use custom attributes to configure features. The release notes and *AnyConnect Administrator's Guide* for each version list any features that require custom attributes.

If you try to remove the definition of attribute that is being used in a group policy, an error message will be displayed, and the action will fail. If a user attempts to add an attribute that already exists as a custom attribute, any changes to the description will be incorporated, but the command will otherwise be ignored.

Multiple instances of this command are supported to build a multiline value for an attribute. All data associated with a given attribute name is delivered to the client in the order that it is entered in the CLI. Individual lines of a multiline value can not be removed.

Examples

The following example configures a custom attribute for AnyConnect Deferred Update:

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description Indicates
 if the deferred update feature is enabled or not
```

Related Commands

Command	Description
show run webvpn	Displays configuration information about WebVPN, including **anyconnect** commands.
show run group-policy	Displays configuration information about current group policies.
anyconnect-custom	Associates custom attribute types and named values with a group policy or dynamic access policy.

anyconnect-custom-attr (Version 9.3 and later)

To create custom attribute types, use the **anyconnect-custom-attr** command in config-webvpn configuration mode. To remove custom attributes, use the **no** form of this command.

[**no**] **anyconnect-custom-attr** *attr-type* [**description** *description*]

Syntax Description

attr-type	The type of the attribute. This type is referenced in the group policy syntax, and DAP-policy syntax, as well as the aggregate auth protocol messages. The maximum length is 32 characters.
description *description*	A free form description of attribute usage. This text appears in the command help when the custom attribute is referenced from the group-policy attribute configuration mode. The maximum length is characters.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
config-webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.3(1)	This command has been redefined.

Usage Guidelines

This command creates custom attributes to support special Secure Client features. After creating custom attributes for a particular feature, you define values for them and then add them to group policies so that the related feature can be applied to VPN clients. This command guarantees that all of the defined attribute names are unique.

Some versions of Secure Client use custom attributes to configure features. The release notes and *AnyConnect Administrator's Guide* for each version list any features that require custom attributes.

If you try to remove the definition of an attribute that is being used in a group policy, an error message will be displayed, and the action will fail. If a user attempts to add an attribute that already exists as a custom attribute, any changes to the description will be incorporated, but the command will otherwise be ignored.

Examples

The following example configures a custom attribute for AnyConnect Deferred Update:'

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description Indicates
 if the deferred update feature is enabled or not
```

ciscoasa(config)# **anyconnect-custom-data DeferredUpdateAllowed def-allowed true**

Related Commands

Command	Description
show run webvpn	Displays configuration information about WebVPN, including **anyconnect** commands.
show run group-policy	Displays configuration information about current group policies.
show running-config dynamic-access-policy-record	Display custom attributes used in DAP policies.
anyconnect-custom	Sets values of custom attributes for policy use.
anyconnect-custom-data	Creates custom attribute named values.

anyconnect-custom-data

To create custom attribute named values, use the **anyconnect-custom-data** command in global configuration mode. To remove custom attributes, use the **no** form of this command.

anyconnect-custom-data *attr-type attr-name attr-value*
no anyconnect-custom-data *attr-type attr-name*

Syntax Description

attr-type	The type of the attribute previously defined using **anyconnect-custom-attr**.
attr-name	The name of the attribute with the specified value. It can be referenced in group-policy and dynamic-access-policy-record config mode.
attr-value	A string containing the attribute value. Maximum length of 420 characters.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command defines custom attribute named values to support special Secure Client features. After creating custom attributes for a particular feature, you define values for them and then add them to DAP or group policies so that the related feature can be applied to VPN clients.

Some versions of Secure Client use custom attributes to configure features. The release notes and *AnyConnect Administrator's Guide* for each version list any features that require custom attributes.

If you try to remove the named value of an attribute that is being used in a group policy, an error message will be displayed, and the action will fail.

Multiple instances of this command are supported to build a multiline value for an attribute. All data associated with a given attribute name is delivered to the client in the order that it is entered in the CLI. Individual lines of a multiline value can not be removed.

Examples

The following example configures a custom attribute for AnyConnect Deferred Update:

```
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

Related Commands

Command	Description
show run webvpn	Displays configuration information about WebVPN, including **anyconnect** commands.
show run group-policy	Displays configuration information about current group policies.
show running-config dynamic-access-policy-record	Display custom attributes used in DAP policies.
show run anyconnect-custom-data	Display all defined custom attribute named values.
anyconnect-custom	Associate custom attribute types and values with a group policy or DAP.
anyconnect-custom-attr	Creates custom attributes.

anyconnect df-bit-ignore

To ignore the DF bit in packets that need fragmentation, use the **anyconnect-df-bit-ignore** command in group policy webvpn configuration mode. To acknowledge the DF bits that need fragmentation, use the **no** form of the command.

anyconnect df-bit-ignore { **enable** | **none** }
no anyconnect df-bit-ignore { **enable** | **none** }

Syntax Description

enable	Enables DF-bit ignore for Secure Client.
none	Disables DF-bit for Secure Client.

Command Default

By default, this option is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(2)	The **svc df-bit-ignore** command was added.
8.4(3)	The anyconnect df-bit-ignore command replaced the svc df-bit-ignore command.

Examples

```
vmb-5520(config-group-webvpn)# anyconnect routing-filtering-ignore ?
config-group-webvpn mode commands/options:
  enable  Enable Routing/Filtering for AnyConnect Client
  none    Disable Routing/Filtering for AnyConnect Client
```

anyconnect dpd-interval

To enable Dead Peer Detection (DPD) on the ASA and to set the frequency that either the remote client or the ASA performs DPD over SSL VPN connections, use the anyconnect **dpd-interval** command in group policy webvpn or username webvpn configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

anyconnect dpd-interval { [**gateway** { *seconds* | **none** }] | [**client** { *seconds* | **none** }] }
no anyconnect dpd-interval { [**gateway** { *seconds* | **none** }] | [**client** { *seconds* | **none** }] }

Syntax Description

client none	Disables the DPD that the client performs.
client seconds	Specifies the frequency, from 30 to 3600 seconds, for which the client performs DPD.
gateway none	Disables DPD testing that the ASA performs.
gateway seconds	Specifies the frequency, from 30 to 3600 seconds, for which the ASA performs DPD. A value of 300 is recommended.

Command Default

The default is DPD is enabled and set to 30 seconds for both the ASA (gateway) and the client.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
8.0(3)	The default setting changed from disabled to 30 seconds for both the ASA (gateway) and the client.
8.4(1)	The anyconnect dpd-interval command replaced the svc dpd-interval command.

Usage Guidelines

The gateway refers to the ASA. You enable DPD and specify the interval with which the ASA waits for any packets from the client. If no packets are received within that interval, the ASA performs the DPD test with three attempts at the same interval. If it doesn't receive a response from the client, the ASA tears down the TLS/DTLS tunnel.

The DPD process on the ASA gets triggered only when the ASA has a packet to send out toward the client over the TLS/DTLS tunnel.

Examples

The following example shows how to configure the DPD frequency performed by the ASA (gateway) to 3000 seconds, and the DPD frequency performed by the client to 1000 seconds, for the existing group policy *sales* :

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect dpd-interval gateway 3000
ciscoasa(config-group-webvpn)# anyconnect dpd-interval client 1000
```

anyconnect dtls compression

To enable compression on low bandwidth links for a specific group or user, use the Secure Client **dtls compression** command in group policy webvpn or username webvpn configuration mode. To delete the configuration from the group, use the **no** form of the command.

anyconnect dtls compression { **lzs** | **none** }
no anyconnect dtls compression { **lzs** | **none** }

Syntax Description

lzs	Enables a stateless compression algorithm.
none	Disables compression.

Command Default

The default is to not enable Secure Client compression.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Examples

The following examples shows the sequence to disable compression:

```
asa# config terminal
asa(config)# group-policy DfltGrpPolicy attributes
asa(config-group-policy)# webvpn
asa(config-group-webvpn)# anyconnect ssl compression none
asa(config-group-webvpn)# anyconnect dtls compression none
```

anyconnect enable

To enable the ASA to download an Secure Client to remote computers or to connect to the ASA using the Secure Client with SSL or IKEv2, use the anyconnect enable command in webvpn configuration mode. To remove the command from the configuration, use the **no** form of the command.

anyconnect enable
no anyconnect enable

Command Default

The default for this command is disabled. The ASA does not download the client.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added as svc enable.
8.4(1)	The anyconnect enable command replaced the svc enable command.

Usage Guidelines

Entering the no anyconnect enable command does not terminate active sessions.

The **anyconnect enable** command must be issued after configuring the Secure Client images with the **anyconnect image xyz** command. To use an Secure Client or Secure Client weblaunch, **anyconnect enable** is required. If the **anyconnect enable** command is not issued with SSL or IKEv2, Secure Client does not function as expected and times out with an IPsec VPN connection termination error. As a result, the **show webvpn svc** command does not consider the SSL VPN client to be enabled and does not list the installed Secure Client packages.

Examples

In the following example shows how to enable the ASA to download the client:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect enable
```

Related Commands

Command	Description
anyconnect image	Specifies an AnyConnect SSL VPN client package file that the ASA expands in cache memory for downloading to remote PCs.

Command	Description
anyconnect modules	Specifies the names of modules that the AnyConnect SSL VPN Client requires for optional features.
anyconnect profiles	Specifies the name of the file used to store profiles that the ASA downloads to the Cisco AnyConnect SSL VPN client.
show webvpn anyconnect	Displays information about SSL VPN clients installed on the ASA and loaded in cache memory for downloading to remote PCs.
anyconnect localization	Specifies the package file used to store localization files that are downloaded to the Cisco AnyConnect VPN Client.

anyconnect-essentials

To enable AnyConnect Essentials on the ASA, use the **anyconnect-essentials** command in group policy webvpn configuration mode. To disable the use of AnyConnect Essentials and enable the premium Secure Client instead, use the **no** form of the command.

anyconnect-essentials
no anyconnect-essentials

Command Default

AnyConnect Essentials is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Use this command to toggle between using the full AnyConnect SSL VPN client and the AnyConnect Essentials SSL VPN client, assuming that the full Secure Client license is installed. AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the ASA, that provides the premium Secure Client capability, with the following exceptions:

- No CSD (including HostScan/Vault/Cache Cleaner)
- No clientless SSL VPN

The AnyConnect Essentials client provides remote end users running Microsoft Windows Vista, Windows Mobile, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client.

You enable or disable the AnyConnect Essentials license by using the **anyconnect-essentials** command, which is meaningful only after you have installed the AnyConnect Essentials license on the ASA. Without this license, this command returns the following error message:

```
ERROR: Command requires AnyConnect Essentials license
```

Note This command only enables or disables the use of AnyConnect Essentials. The AnyConnect Essentials *license* itself is not affected by the setting of the **anyconnect-essentials** command.

When the AnyConnect Essentials license is enabled, Secure Client use Essentials mode, and Clientless SSL VPN access is disabled. When the AnyConnect Essentials license is disabled, Secure Client use the full AnyConnect SSL VPN Client license.



Note This command is not supported on the ASA Virtual or devices. See the licensing documentation for more information.

If you have active clientless SSL VPN connections, and you enable the AnyConnect Essentials license, then all connections are logged off and will need to be reestablished.

Examples

In the following example, the user enters webvpn configuration mode and enables the AnyConnect Essentials VPN client:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect-essentials
```

anyconnect external-browser-pkg

To configure the path for the Secure Client external browser package, use the **anyconnect external-browser-pkg** command in the webvpn configuration mode. Use the **no** form of the command to remove the external browser path.

anyconnect external-browser-pkg { *package path* }

no anyconnect external-browser-pkg { *package path* }

Syntax Description

{*packagepath*}	Configures the external browser package path on the device for single sing-on authentication.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Web VPN configuration	• Yes	• —	• Yes	• —	• —

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

By default, Secure Client uses it's embedded browser for SAML single sign-on authentication. You can configure the operating system's default browser (platform's native browser) for SAML authentication. Choosing the operating system's default browser requires an external browser package for Secure Client to use the default OS browser for single sign-on authentication.

The **anyconnect external-browser-pkg** command allows you to configure an external browser path for Secure Client single sign-on authentication.

The following example shows how to use the **anyconnect external-browser-pkg** command to configure a path for the external bowser for Secure Client single sign-on authentication.

```
ciscoasa
#
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-webvpn)# anyconnect external-browser-pkg disk0:
```

Related Commands

Command	Description
external-browser	Configures the Secure Client external browser for single sign-on authentication.

Command	Description
tunnel-group	Creates a VPN connection profile or accesses the database of VPN connection profiles.
show webvpnanyconnect external-browser-pkg	Displays information about the specified single sing-on package file.

anyconnect firewall-rule

To establish a public or provide ACL firewall, use the **anyconnect firewall-rule** command in either group policy webvpn or username webvpn configuration mode.

anyconnect firewall-rule client interface { **public** | **private** } *ACL*

Syntax Description

ACL	Specifies the access control list
client interface	Specify client interface
private	Configure private interface rule
public	Configure public interface rule

Command Default

No default behavior or values .

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This svc firewall-rule command was added.
8.4(1)	The anyconnect firewall-rule command replaced the svc firewall-rule command.
9.0(1)	The ACL in the command can now be a Unified Access Control rule that can specify both IPv4 and IPv6 addresses.

Usage Guidelines

To function as expected, this command requires a release of the AsyncOS for Web version 7.0 that provides AnyConnect Secure Mobility licensing support for the Secure Client. It also requires an Secure Client release that supports Secure Client, ASA 8.3, and ASDM 6.3.

The following notes clarify how the Secure Client uses the firewall:

- The source IP is not used for firewall rules. The client ignores the source IP information in the firewall rules sent from the ASA. The client determines the source IP depending on whether the rules are public or private. Public rules are applied to all interfaces on the client. Private rules are applied to the virtual adapter.
- The ASA supports many protocols for ACL rules. However, the AnyConnect firewall feature supports only TCP, UDP, ICMP, and IP. If the client receives a rule with a different protocol, it treats it as an invalid firewall rule, and then disables split tunneling and uses full tunneling for security reasons.

Be aware of the following differences in behavior for each operating system:

- For Windows computers, deny rules take precedence over allow rules in Windows Firewall. If the ASA pushes down an allow rule to the Secure Client, but the user has created a custom deny rule, the Secure Client rule is not enforced.
- On Windows Vista, when a firewall rule is created, Vista takes the port number range as a comma-separated string (for example, from 1-300 or 5000-5300). The maximum number of ports allowed is 300. If you specify a number greater than 300 ports, the firewall rule is applied only to the first 300 ports.
- Windows users whose firewall service must be started by the Secure Client (not started automatically by the system) may experience a noticeable increase in the time it takes to establish a VPN connection.
- On Mac computers, the Secure Client applies rules sequentially in the same order that the ASA applies them. Global rules should always be last.
- For third-party firewalls, traffic is passed only if both the Secure Client firewall and the third-party firewall allow that traffic type. If the third-party firewall blocks a specify traffic type that the Secure Client allows, the client blocks the traffic.

For more information about the Secure Client firewall including ACL rule examples for local printing and tethered device support, see the AnyConnect Administrator's Guide.

Examples

The following example enables the ACL AnyConnect_Client_Local_Print as a public firewall:

```
ciscoasa(config)# group-policy example_group attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect firewall-rule client-interface public value
AnyConnect_Client_Local_Print
```

Related Commands

Command	Description
show webvpn anyconnect	Displays information about installed SSL VPN clients.
anyconnect	Enables or requires the SSL VPN client for a specific group or user.
anyconnect image	Specifies a client package file that the ASA expands in cache memory for downloading to remote PCs.

anyconnect image

To install or upgrade the Secure Client distribution package and add it to the running configuration, use the anyconnect image command in webvpn configuration mode. To remove the Secure Client distribution package from the running configuration, use the **no** form of the command.

anyconnect image *path* **order** [**regex** *expression*]
no anyconnect image *path* **order** [**regex** *expression*]

Syntax Description

order	With multiple client package files, specifies the order of the package files, from 1 to 65535. The ASA downloads portions of each client in the order you specify to the remote PC until it achieves a match with the operating system.
path	Specifies the path and filename of the Secure Client package, up to 255 characters.
regex *expression*	Specifies a string that the ASA uses to match against the user-agent string passed by the browser.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added as svc image.
8.0(1)	The **regex** *keyword was* added.
8.4(1)	The Secure Client image command replaced the svc image command.

Usage Guidelines

Numbering the package files establishes the order in which the ASA downloads portions of them to the remote PC until it achieves a match with the operating system. It downloads the package file with the lowest number first. Therefore, you should assign the lowest number to the package file that matches the most commonly-encountered operating system used on remote PCs.

The default order is 1. If you do not specify the *order* argument, each time that you enter the **svc image** command, you overwrite the image that was previously considered number 1.

You can enter the **anyconnect image** command for each client package file in any order. For example, you can specify the package file to be downloaded second (*order* 2) before entering the **anyconnect image** command specifying the package file to be downloaded first (*order* 1).

For mobile users, you can decrease the connection time of the mobile device by using the **regex keyword.** When the browser connects to the ASA, it includes the user-agent string in the HTTP header. When the ASA receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

Note When using the standalone client, the **regex** command is ignored. It is used only for the web browser as a performance enhancement, and the regex string is not matched against any user or agent provided by the standalone client.

The ASA expands both Secure Client and Cisco Secure Desktop (CSD) package files in cache memory. For the ASA to successfully expand the package files, there must be enough cache memory to store the images and files of the package file.

If the ASA detects there is not enough cache memory to expand a package, it displays an error message to the console. The following example shows an error message reported after an attempt to install a package file with the **svc image** command:

```
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0520-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

If this occurs when you attempt to install a package file, examine the amount of cache memory remaining and the size of any previously installed packages with the **dir cache:/** command in global configuration mode.

Note If your ASA has only the default internal flash memory size or the default DRAM size (for cache memory) you could have problems storing and loading multiple Secure Client packages on the ASA. Even if there is enough space in flash memory to hold the package files, the ASA could run out of cache memory when it unzips and loads the client images. For more information about the ASA memory requirements when deploying Secure Client, and possibly upgrading the ASA memory, see the latest release notes for the ASA 5500 series.

Examples

The following example loads Secure Client package files for Windows, MAC, and Linux in that order:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect image
 disk0:/anyconnect-win-3.0.0527-k9.pkg 1
ciscoasa(config-webvpn)# anyconnect image
 disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2
ciscoasa(config-webvpn)# anyconnect image
 disk0:/anyconnect-linux-3.0.0414-k9.pkg 3
ciscoasa(config-webvpn)
```

The following is sample output from the show webvpn Secure Client command, which displays the Secure Client packages loaded and their order:

```
ciscoasa(config-webvpn)# show webvpn anyconnect
1. disk0:/anyconnect-win-3.0.0527-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,0,0527
  Hostscan Version 3.0.0527
  Tue 10/19/2010 16:16:56.25
2. disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2 dyn-regex=/Intel Mac OS X/
  CISCO STC Darwin_i386
  3.0.0414
  Wed Oct 20 20:39:53 MDT 2010
3. disk0:/anyconnect-linux-3.0.0414-k9.pkg 3 dyn-regex=/Linux i[1-9]86/
  CISCO STC Linux
  3.0.0414
  Wed Oct 20 20:42:02 MDT 2010
3 AnyConnect Client(s) installed
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
anyconnect modules	Specifies the names of modules that the AnyConnect SSL VPN Client requires for optional features.
anyconnect profiles	Specifies the name of the file used to store profiles that the ASA downloads to the Cisco AnyConnect SSL VPN client.
show webvpn anyconnect	Displays information about SSL VPN clients installed on the ASA and loaded in cache memory for downloading to remote PCs.
anyconnect localization	Specifies the package file used to store localization files that are downloaded to the Cisco AnyConnect VPN Client.

anyconnect keep-installer

Note This command does not apply to versions of Secure Client after 2.5, but is still available for backward compatibility. Configuring the **anyconnect keep-installer** command does not affect Secure Client 3.0 or later.

To enable the permanent installation of an SSL VPN client on a remote PC, use the anyconnect keep-installer command in group-policy webvpn or username webvpn configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

anyconnect keep-installer { **installed** | **none** }
no anyconnect keep-installer { **installed** | **none** }

Syntax Description

installed	Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections.
none	Specifies that the client uninstalls from the remote computer after the active connection terminates.

Command Default

The default is permanent installation of the client is enabled. The client remains on the remote computer at the end of the session.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	The svc keep-installer command was added.
8.4(1)	The anyconnect keep-installer command replaced the svc keep-installer command.

Examples

In the following example, the user enters group policy webvpn configuration mode and configures the group policy to remove the client at the end of the session:

```
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)# anyconnect keep-installer none
ciscoasa(config-group-webvpn)#
```

Related Commands

Command	Description
show webvpn anyconnect	Displays information about Secure Client installed on the ASA and loaded in cache memory for downloading to remote PCs.
anyconnect	Enables or requires the SSL VPN client for a specific group or user.
anyconnect enable	Enables the ASA to download Secure Client files to remote PCs.
anyconnect image	Specifies an Secure Client package file that the ASA expands in cache memory for downloading to remote PCs.

anyconnect modules

To specify the names of modules that the AnyConnect SSL VPN Client requires for optional features, use the **anyconnect modules** command in group policy webvpn or username webvpn configuration mode. To remove the command from the configuration, use the **no** form of the command.

anyconnect modules { **none** | **value** *string* }
no anyconnect modules { **none** | **value** *string* }

Syntax Description

string	*The name of the optional module, up to 256 characters. Separate multiple strings with commas.*

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	The svc modules command was added.
8.4(1)	The anyconnect modules command replaced the svc modules command.

Usage Guidelines

To minimize download time, the client only requests downloads (from the ASA) of modules that it needs for each feature that it supports. The **anyconnect modules** command enables the ASA to download these modules.

The following table shows the string values that represent AnyConnect Modules.

String representing AnyConnect Module	AnyConnect Module Name
dart	AnyConnect DART (Diagnostics and Reporting Tool)
nam	AnyConnect Network Access Manager
vpngina	AnyConnect SBL (Start Before Logon)

String representing AnyConnect Module	AnyConnect Module Name
websecurity	AnyConnect Web Security Module
telemetry	AnyConnect Telemetry Module
posture	AnyConnect Posture Module
none	If you choose **none**, the ASA downloads the essential files with no optional modules. Existing modules are removed from the group policy.

Examples

In the following example, the user enters group-policy attributes mode for the group policy *PostureModuleGroup*, enters webvpn configuration mode for the group policy, and specifies the string *posture* and *telemetry* so that the AnyConnect Posture Module and AnyConnect Telemetry Module will be downloaded to the endpoint when it connects to the ASA.

```
ciscoasa> en

Password:
ciscoasa# config t
ciscoasa(config)# group-policy PostureModuleGroup attributes

ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect modules value posture,telemetry

ciscoasa(config-group-webvpn)# write mem

Building configuration...
Cryptochecksum: 40975338 b918425d 083b391f 9e5a5c69
22055 bytes copied in 3.440 secs (7351 bytes/sec)
[OK]
ciscoasa(config-group-webvpn)#
```

To remove a module from a group policy, resend the command specifying only the module values you want to keep. For example, this command removes the telemetry module:

```
ciscoasa(config-group-webvpn)# anyconnect modules value posture
```

Related Commands

Command	Description
show webvpn anyconnect	Displays information about Secure Client packages that are loaded in cache memory on the ASA and available for download.
anyconnect enable	Enables an Secure Client for a specific group or user.
anyconnect image	Specifies an Secure Client package file that the ASA expands in cache memory for downloading to remote PCs.

anyconnect mtu

To adjust the MTU size for VPN connections established by the Cisco AnyConnect VPN Client, use the **anyconnect mtu** command in group policy webvpn or username webvpn configuration mode. To remove the command from the configuration, use the **no** form of the command.

anyconnect mtu *size*
no anyconnect mtu *size*

Syntax Description

size	The MTU size in bytes, from 576 to 1406 bytes.

Command Default

The default size is 1406 bytes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	Th svc mtu command was added.
8.4(1)	The anyconnect mtu command replaced the svc mtu command.

Usage Guidelines

This command affects only the Secure Client. The VPN Client is not capable of adjusting to different MTU sizes.

The default for this command in the default group policy is **no svc mtu**. The MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

Examples

The following example configures the MTU size to 500 bytes for the group policy >*telecommuters*
:

```
ciscoasa(config)# group-policy telecommuters attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect mtu 500
```

Related Commands

Command	Description
anyconnect keep-installer	Disables the automatic uninstalling feature of the client. After the initial download, the client remains on the remote PC after the connection terminates.
anyconnect ssl dtls	Enables DTLS for CVCs establishing SSL VPN connections.
show run webvpn	Displays configuration information about WebVPN, including **anyconnect** commands.

anyconnect profiles (group-policy attributes webvpn, username attributes webvpn)

To specify a CVC profiles package downloaded to Cisco AnyConnect VPN Client (CVC) users, use the **anyconnect profiles** command in webvpn or configuration mode. You can access the webvpn configuration mode by first entering the group-policy attributes command or the username attributes. To remove the command from the configuration and cause the value it to be inherited, use the **no** form of the command.

anyconnect profiles { **value** *profile* | **none** } [**type** *type*]
no anyconnect profiles { **value** *profile* | **none** } [**type** *type*]

Syntax Description

value *profile*	*The name of the profile.*
none	The ASA does not download profiles.
type *type*	(Optional.) The profile type. The default is **user**. Specify one of the following: • **user**—AnyConnect VPN Profile. • **vpn-mgmt**—AnyConnect Management VPN Profile. • **umbrella**—Umbrella Roaming Security Profile • **ampenabler**—AMP Enabler Service Profile • **websecurity**—Web Security Service Profile • **nam**—NAM Service Module • **iseposture**—ISE Posture Profile • **nvm**—Network Visibility Service Profile

Command Default

The default is none. The ASA does not download profiles.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	The svc profiles command was added.

Release	Modification
8.3(1)	The optional type **value** was added.
8.4(1)	The anyconnect profiles command replaced the svc profiles command.

Usage Guidelines

This command, entered in group policy webvpn or username attributes webvpn configuration mode, enables the ASA to download profiles to CVC users on a group policy or username basis. To download a CVC profile to all CVC users, use this command from webvpn configuration mode.

A CVC profile is a group of configuration parameters that the CVC uses to configure the connection entries that appear in the CVC user interface, including the names and addresses of host computers. You can create and save profiles using the CVC user interface. You can also edit this file with a text editor and set advanced parameters that are not available through the user interface.

The CVC installation contains one profile template (cvcprofile.xml) that you can edit and use as a basis for creating other profile files. For more information about editing CVC profiles, see the *Cisco AnyConnect VPN Client Administrator Guide.*

Examples

In the following example, the user enters the **anyconnect profiles value** command, which displays the available profiles:

```
ciscoasa(config-group-webvpn)# anyconnect profiles value ?
config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

Then the user configures the group policy to use the CVC profile sales:

```
ciscoasa(config-group-webvpn)# anyconnect profiles sales
```

Related Commands

Command	Description
show webvpn anyconnect	Displays information about installed Secure Client.
anyconnect	Enables or requires an SSL VPN client for a specific group or user.
anyconnect image	Specifies an Secure Client package file that the ASA expands in cache memory for downloading to remote PCs.

anyconnect profiles (webvpn)

To specify a file as a profiles package that the ASA loads in cache memory and makes available to group policies and username attributes of Cisco AnyConnect VPN Client (CVC) users, use the **anyconnect profiles** command in webvpn configuration mode. To remove the command from the configuration and cause the ASA to unload the package file from cache memory, use the **no** form of the command.

anyconnect profiles { *profile path* }
no anyconnect profiles { *profile path* }

Syntax Description

path	The path and filename of the profile file in flash memory of the ASA.
profile	*The name of the profile to create in cache memory.*

Command Default

The default is none. The ASA does not load a profiles package in cache memory.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	Th svc profiles command was added.
8.4(1)	The anyconnect profiles command replaced the svc profiles command.

Usage Guidelines

A CVC profile is a group of configuration parameters that the CVC uses to configure the connection entries that appear in the CVC user interface, including the names and addresses of host computers. You can create and save profiles using the CVC user interface.

You can also edit this file with a text editor and set advanced parameters that are not available through the user interface. The CVC installation contains one profile template (cvcprofile.xml) that you can edit and use as a basis for creating other profile files. For more information about editing CVC profiles, see the *Cisco AnyConnect VPN Client Administrator Guide.*

After you create a new CVC profile and upload it to flash memory, identify the XML file to the ASA as a profile using the **anyconnect profiles** command in webvpn configuration mode. After you enter this command, files are loaded into cache memory on the ASA. Then you can specify the profile for a group or user with the **anyconnect profiles** command from group policy webvpn configuation or username attributes configuration mode.

Examples

In the following example, the user previously created two new profile files (sales_hosts.xml and engineering_hosts.xml) from the cvcprofile.xml file provided in the CVC installation and uploaded them to flash memory on the ASA.

Then the user identifies these files to the ASA as CVC profiles, specifying the names >*sales* and >*engineering* :

```
ciscoasa(config-webvpn)# anyconnect profiles sales disk0:sales_hosts.xml
ciscoasa(config-webvpn)# anyconnect profiles engineering disk0:engineering_hosts.xml
```

Entering the **dir cache:stc/profiles** command shows the profiles that have been loaded into cache memory:

```
ciscoasa(config-webvpn)# dir cache:stc/profiles
Directory of cache:stc/profiles/
0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg
2428928 bytes total (18219008 bytes free)
ciscoasa(config-webvpn)#
```

These profiles are available to the **svc profiles** command in group policy webvpn configuration or username attributes configurate modes:

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect profiles value ?
config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

Related Commands

Command	Description
show webvpn anyconnect	Displays information about installed Secure Client.
anyconnect	Enables or requires the SSL VPN client for a specific group or user.
anyconnect image	Specifies an Secure Client package file that the ASA expands in cache memory for downloading to remote PCs.

anyconnect ssl compression

To enable compression of http data over an SSL VPN connection for a specific group or user, use the anyconnect **ssl compression** command in group policy webvpn or username webvpn configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

anyconnect ssl compression { **deflate** | **lzs** | **none** }
no anyconnect ssl compression { **deflate** | **lzs** | **none** }

Syntax Description

deflate	Enables a deflate compression algorithm.
lzs	Enables a stateless compression algorithm.
none	Disables compression.

Command Default

By default, compression is set to none (disabled).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	The **anyconnect compression** command was added.

Usage Guidelines

For SSL VPN connections, the **compression** command configured from webvpn configuration mode overrides the anyconnect **ssl compression** command configured in group policy and username webvpn mode.

Examples

In the following example, SVC compression is disabled for the group policy sales:

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl compression none
```

Related Commands

Command	Description
anyconnect	Enables or requires the SSL VPN client for a specific group or user.
anyconnect keepalive	Specifies the frequency at which a client on a remote computer sends keepalive messages to the ASA over an SSL VPN connection.
anyconnect keep-installer	Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections.
anyconnect rekey	Enables the client to perform a rekey on an SSL VPN connection.
compression	Enables compression for all SSL, WebVPN, and IPsec VPN connections.
show webvpn anyconnect	Displays information about installed SSL VPN clients.

anyconnect ssl df-bit-ignore

To enable the forced fragmentation of packets on an SSL VPN connection (allowing them to pass through the tunnel) for a specific group or user, use the **anyconnect ssl df-bit-ignore** command in the group policy webvpn or username webvpn configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

anyconnect ssl df-bit-ignore { **enable** | **disable** }
no anyconnect ssl df-bit-ignore

Syntax Description

enable	Enable DF-bit ignore for Secure Client with SSL.
disable	Disable DF-bit for Secure Client with SSL.

Command Default

DF bit ignore is set to *disabled.*

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	The anyconnect ssl df-bit-ignore form of the command replaced svc df-bit-ignore.

Usage Guidelines

This feature allows the force fragmentation of packets that have the DF bit set, allowing them to pass through the tunnel. An example use case is for servers in your network that do not respond correctly to TCP MSS negotiations.

Examples

In the following example, DF bit ignore is enabled for the group policy sales:

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl df-bit-ignore enable
```

Related Commands

Command	Description
anyconnect	Enables or requires the SSL VPN client for a specific group or user.
anyconnect keepalive	Specifies the frequency at which a client on a remote computer sends keepalive messages to the ASA over an SSL VPN connection.
anyconnect keep-installer	Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections.
anyconnect rekey	Enables the client to perform a rekey on an SSL VPN connection.

anyconnect ssl dtls enable

To enable Datagram Transport Layer Security (DTLS) connections on an interface for specific groups or users establishing SSL VPN connections with the Cisco AnyConnect VPN Client, use the **anyconnect ssl dtls enable** command in group policy webvpn or username attributes webvpn configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

anyconnect ssl dtls enable *interface*
no anyconnect ssl dtls enable *interface*

Syntax Description

interface	*The name of the interface.*

Command Default

The default is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	The svc dtls command was added.
8.4(1)	The anyconnect ssl dtls command replaced the svc dtls command.

Usage Guidelines

Enabling DTLS allows the Secure Client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, Secure Client users establishing SSL VPN connections connect with an SSL tunnel only.

This command enables DTLS for specific groups or users. To enable DTLS for all Secure Client users, use the **anyconnect ssl dtls enable** command in webvpn configuration mode.

Examples

The following example enters group policy webvpn configuration mode for the group policy *sales* and enables DTLS:

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl dtls enable
```

Related Commands

Command	Description
dtls port	Specifies a UDP port for DTLS.
anyconnect dtls	Enables DTLS for groups or users establishing SSL VPN connections.
vpn-tunnel-protocol	Specifies VPN protocols that the ASA allows for remote access, including SSL.

anyconnect ssl keepalive

To configure the frequency of keepalive messages which a remote client sends to the ASA over SSL VPN connections, use the **anyconnect ssl keepalive** command in group policy webvpn or username webvpn configuration modes. Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited.

anyconnect ssl keepalive { **none** | *seconds* }
no anyconnect ssl keepalive { **none** | *seconds* }

Syntax Description

none	Disables keepalive messages.
seconds	Enables keepalive messages and specifies the frequency of the messages, from 15 to 600 seconds.

Command Default

The default is 20 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	The svc keepalive command was added.
8.0(3)	The default setting changed from disabled to 20 seconds.
8.4(1)	The anyconnect ssl keepalive command replaced the svc keepalive command.

Usage Guidelines

Both the Cisco SSL VPN Client (SVC) and the Cisco AnyConnect VPN Client can send keepalive messages when they establish SSL VPN connections to the ASA.

You can adjust the frequency of keepalive messages (specified in *seconds)* to ensure that an SSL VPN connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

Adjusting the frequency also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

Note Keepalives are enabled by default. If you disable keepalives, in the event of a failover event, SSL VPN client sessions are not carried over to the standby device.

Examples

In the following example, the user configures the ASA to enable the client to send keepalive messages, with a frequency of 300 seconds (5 minutes), for the existing group policy named >*sales* :

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl keepalive 300
```

Related Commands

Command	Description
anyconnect	Enables or requires an SSL VPN client for a specific group or user.
anyconnect dpd-interval	Enables Dead Peer Detection (DPD) on the ASA, and sets the frequency in which either the client or the ASA performs DPD.
anyconnect keep-installer	Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections.
anyconnect ssl rekey	Enables the client to perform a rekey on a session.

anyconnect ssl rekey

To enable a remote client to perform a rekey on an SSL VPN connection, use the anyconnect ssl rekey command in group-policy webvpn or username webvpn configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

anyconnect ssl rekey { **method** { **ssl** | **new-tunnel** } | **time** *minutes* | **none** }
no anyconnect ssl rekey { **method** { **ssl** | **new-tunnel** } | **time** *minutes* | **none** }

Syntax Description

method ssl	Specifies that the client establishes a new tunnel during rekey.
method new-tunnel	Specifies that the client establishes a new tunnel during rekey.
method none	Disables rekey.
time *minutes*	Specifies the number of minutes from the start of the session until the rekey takes place, from 4 to 10080 (1 week).

Command Default

The default is none (disabled).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	The svc rekey command was added.
8.0(2)	The behavior of the **svc rekey method ssl** command changed to that of the **svc rekey method new-tunnel** command to prevent the possibility of a “man in the middle” attack.
8.4(1)	The anyconnect ssl rekey command replaced the svc rekey command.

Usage Guidelines

The Cisco Secure Client can perform a rekey on an SSL VPN connection to the ASA. Configuring the rekey method as **ssl** or **new-tunnel** specifies that the client establishes a new tunnel during rekey instead of the SSL renegotiation taking place during the rekey.

Examples

In the following example, the user specifies that remote clients belonging to the group policy *sales* renegotiate with SSL during rekey and rekey occurs 30 minutes after the session begins:

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anycoanynnect ssl rekey method ssl
ciscoasa(config-group-webvpn)# anyconnect ssl rekey time 30
```

Related Commands

Command	Description
anyconnect enable	Enables or requires the Secure Client for a specific group or user.
anyconnect dpd-interval	Enables Dead Peer Detection (DPD) on the ASA, and sets the frequency that either the Secure Client or the ASA performs DPD.
anyconnect keepalive	Specifies the frequency at which an Secure Client on a remote computer sends keepalive messages to the ASA.
anyconnect keep-installer	Enables the permanent installation of an Secure Client onto a remote computer.

apcf(Deprecated)

To enable an Application Profile Customization Framework profile, use the **apcf** command in webvpn configuration mode. To disable a particular APCF script, use the **no** form of the command. To disable all APCF scripts, use the **no** form of the command without arguments.

apcf URL / **filename.ext**
no apcf [**URL** / **filename.ext**]

Syntax Description

filename.extension	Specifies the name of the APCF customization script. These scripts are always in XML format. The extension might be .xml, .txt, .doc or one of many others
URL	Specifies the location of the APCF profile to load and use on the ASA. Use one of the following URLs: http://, https://, tftp://, ftp://; flash:/, disk#:/' The URL might include a server, port, and path. If you provide only the filename, the default URL is flash:/. You can use the **copy** command to copy an APCF profile to flash memory.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

The **apcf** command enables the ASA to handle non-standard web applications and web resources so that they render correctly over a WebVPN connection. An APCF profile contains a script that specifies when (pre, post), where (header, body, request, response), and which data to transform for a particular application.

You can use multiple APCF profiles on the ASA. When you do, the ASA applies each one of them in the order of oldest to newest.

We recommend that you use the APCF command only with the support of the Cisco TAC.

Examples

The following example shows how to enable an APCF named apcf1, located on flash memory at /apcf:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 apcf
flash:/apcf/apcf1.xml
ciscoasa(config-webvpn)#
```

This example shows how to enable an APCF named apcf2.xml, located on an HTTPS server called myserver, port 1440 with the path /apcf:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 apcf
https://myserver:1440/apcf/apcf2.xml
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
proxy-bypass	Configures minimal content rewriting for a particular application.
rewrite	Determines whether traffic travels through the ASA.
show running config webvpn apcf	Displays the APCF configuration.

app-agent heartbeat

To configure the heartbeat message interval for the app-agent (application agent) running on the ASA to check the health of the chassis, use the **app-agent heartbeat** command in global configuration mode.

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

Syntax Description

interval *ms*	Sets the amount of time between heartbeats, between 100 and 6000 ms, in multiples of 100. The default is 1000 ms.
retry-count *number*	Sets the number of retries, between 1 and 30. The default is 3 retries.

Command Default

For the Firepower 4100/9300, Firepower 1100/2100, and Secure Firewall 1200/3100/4200 device models, the default timer is 6000, 60000, and 10000 milliseconds respectively, and the default retry count is 10. You cannot use this command to change these values.

For other device models, the default interval value is 1000 milliseconds, and the retry count is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.6(2)	Command added.
9.9(1)	The minimum interval was changed from 300 to 100 ms.

Usage Guidelines

The ASA checks whether it can communicate over the backplane with the host chassis.

For the Firepower 4100/9300, the minimum combined time (*interval* x *retry-count*) cannot be less than 600 ms. For example, if you set the interval to 100, and the retry count to 3, then the total combined time is 300 ms, which is not supported. For example, you can set the interval to 100, and the retry count to 6 to meet the minimum time (600 ms).

Examples

The following example sets the heartbeat timeout to 10 seconds:

```
ciscoasa(config)# app-agent heartbeat interval 1000 retry-count 10
```

Related Commands

Command	Description
health-check	Sets the cluster health check parameters.

app-id

The **app-id** command specifies the Cisco-defined application ID in a network-service object. Although this command can appear in the **show object network-service** output, you should not configure it yourself.

app-id *number*
no app-id *number*

Syntax Description

number	The number is a unique Cisco-assigned number for a particular application, in the range 1-4294967295.

Command Default

No application ID is assigned to the object.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network-service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was introduced.
9.24(1)	This command is no longer user configurable.

Related Commands

Command	Description
object network-service	Creates a network-service object.
object-group network-service	Creates a network-service object group.

appl-acl

To identify a previously configured webtype ACL to apply to a session, use the **appl-acl** command in dap webvpn configuration mode. To remove the attribute from the configuration, use the **no** form of the command. To remove all web-type ACLs, use the **no** form of the command without arguments.

appl-acl [*identifier*]
no appl-acl [*identifier*]

Syntax Description

identifier	The name of the previously configured webtype ACL. The maximum length is 240 characters.

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

To configure webtype ACLs, use the **access-list webtype** command in global configuration mode.

Use the **appl-acl** command multiple times to apply more than one webtype ACL to the DAP policy.

Examples

The following example shows how to apply the previously configured webtype ACL called newacl to the dynamic access policy:

```
ciscoasa
 (config)#
config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dynamic-access-policy-record)#
 appl-acl newacl
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
access-list_webtype	Creates a web-type ACL.

application-access

To customize the Application Access fields of the WebVPN Home page that is displayed to authenticated WebVPN users, and the Application Access window that is launched when the user selects an application, use the **application-access** command in customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

application-access { **title** | **message** | **window** } { **text** | **style** } *value*
no application-access { **title** | **message** | **window** } { **text** | **style** } *value*

Syntax Description

message	Changes the message displayed under the title of the Application Access field.
style	Changes the style of the Application Access field.
text	Changes the text of the Application Access field.
title	Changes the title of the Application Access field.
value	The actual text to display (a maximum of 256 characters), or Cascading Style Sheet (CSS) parameters (a maximum of 256 characters).
window	Changes the Application Access window.

Command Default

The default title text of the Application Access field is “Application Access”.

The default title style of the Application Access field is:

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text of the Application Access field is “Start Application Client”.

The default message style of the Application Access field is:

background-color:#99CCCC;color:maroon;font-size:smaller.

The default window text of the Application Access window is:

“Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.”.

The default window style of the Application Access window is:

background-color:#99CCCC;color:black;font-weight:bold.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

This command is accessed by using the **webvpn** command or the **tunnel-group webvpn-attributes** command.

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameter. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

The following tips can help you make the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the background color of the Application Access field to the RGB hexadecimal value 66FFFF, a shade of green:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

Related Commands

Command	Description
application-access hide-details	Enables or disables the display of the application details in the Application Access window.
browse-networks	Customizes the Browse Networks field of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application field of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.

application-access hide-details

To hide application details that are displayed in the WebVPN Applications Access window, use the **application-access hide-details** command in customization configuration mode, which is accessed by using the **webvpn** command or the **tunnel-group webvpn-attributes** command. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

application-access hide − details { **enable** | **disable** }
no application-access [**hide - details** { **enable** | **disable** }]

Syntax Description

disable	Does not hide application details in the Application Access window.
enable	Hides application details in the Application Access window.

Command Default

The default is disabled. Application details appear in the Application Access window.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Examples

The following example disables the appearance of the application details:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access hide-details disable
```

Related Commands

Command	Description
application-access	Customizes the Application Access field of the WebVPN Home page.
browse-networks	Customizes the Browse Networks field of the WebVPN Home page.
web-applications	Customizes the Web Application field of the WebVPN Home page.



ar - az

- area, on page 263
- area authentication, on page 265
- area default-cost, on page 267
- area filter-list prefix, on page 269
- area nssa, on page 271
- area-password, on page 273
- area range (ipv6 router ospf), on page 277
- area range (router ospf), on page 279
- area stub, on page 281
- area virtual-link (ipv6 router ospf), on page 283
- area virtual-link (router ospf), on page 285
- arp, on page 288
- arp-inspection, on page 290
- arp permit-nonconnected, on page 292
- arp rate-limit, on page 294
- arp timeout, on page 295
- asdm disconnect, on page 296
- asdm disconnect log_session, on page 298
- asdm history enable, on page 300
- asdm image, on page 301
- asdm location, on page 303
- as-path access-list, on page 304
- asp load-balance per-packet, on page 306
- asp rule-engine compile-offload, on page 308
- asp rule-engine transactional-commit, on page 309
- asr-group, on page 311
- assertion-consumer-url (Deprecated), on page 313
- attribute bind, on page 315
- attribute source-group, on page 316
- attribute source-group host, on page 317
- attribute source-group keepalive, on page 319
- attributes, on page 321
- auth-cookie-name, on page 323

- authenticated-session-username, on page 325
- authentication (bfd-template), on page 327
- authentication, on page 329
- authentication eap-proxy, on page 332
- authentication key, on page 333
- authentication key eigrp, on page 337
- authentication mode, on page 339
- authentication ms-chap-v1, on page 343
- authentication ms-chap-v2, on page 344
- authentication pap, on page 345
- authentication send-only, on page 347
- authentication-attr-from-server, on page 351
- authentication-certificate, on page 353
- authentication-exclude, on page 355
- authentication-port, on page 356
- authentication-server-group (imap4s, pop3s, smtps) (Deprecated), on page 358
- authentication-server-group (tunnel-group general-attributes), on page 360
- authorization-required, on page 362
- authorization-server-group (imap4s, pop3s, smtps) (Deprecated), on page 364
- authorization-server-group (tunnel-group general-attributes), on page 366
- authorize-only, on page 368
- auth-prompt, on page 370
- auto-signon, on page 372
- auto-summary, on page 375
- auto-update device-id, on page 377
- auto-update poll-at, on page 379
- auto-update poll-period, on page 381
- auto-update server, on page 383
- auto-update timeout, on page 385
- avc, on page 386

area

To create an OSPF v2 or OSPFv3 area, use the **area** command in router configuration mode. To remove the area, use the **no** form of this command.

area *area_id*
no area *area_id*

Syntax Description

area_id	The ID of the area being created. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

The area that you create does not have any parameters set. Use the related **area** commands to set the area parameters.

Examples

The following example shows how to create an OSPF area with an area ID of 1:

```
ciscoasa(config-router)# area 1
ciscoasa(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area authentication

To enable authentication for an OSPFv2 area, use the **area authentication** command in router configuration mode. To disable area authentication, use the **no** form of this command.

area *area_id* **authentication** [**message-digest**]
no area *area_id* **authentication** [**message-digest**]

Syntax Description

area_id	The identifier of the area for which authentication is to be enabled. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication for the area specified by the *area_id*.

Command Default

Area authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified OSPFv2 area does not exist, it is created when this command is entered. Entering the **area authentication** command without the **message-digest** keyword enables simple password authentication. Including the **message-digest** keyword enables MD5 authentication.

Examples

The following example shows how to enable MD5 authentication for area 1:

```
ciscoasa(config-router)# area 1 authentication message-digest
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.

Command	Description
show running-config router	Displays the commands in the global router configuration.

area default-cost

To specify a cost for the default summary route sent into a stub or NSSA, use the **area default-cost** command in router configuration mode or IPv6 router configuration mode. To restore the default cost value, use the **no** form of this command.

area *area_id* **default-cost** *cost*
no area *area_id* **default-cost** *cost*

Syntax Description

area_id	The identifier of the stub or NSSA whose default cost is being changed. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
cost	Specifies the cost for the default summary route that is used for a stub or NSSA. Valid values range from 0 to 65535

Command Default

The default value of *cost* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode and OSPFv3 are supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Examples

The following example show how to specify a default cost for summary route sent into a stub or NSSA:

```
ciscoasa(config-router)# area 1 default-cost 5
ciscoasa(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area filter-list prefix

To filter prefixes advertised in Type 3 LSAs between OSPFv2 areas of an ABR, use the **area filter-list prefix** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

area *area_id* **filter-list prefix** *list_name* { **in** | **out** }
no area *area_id* **filter-list prefix** *list_name* { **in** | **out** }

Syntax Description

area_id	Identifies the area for which filtering is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
in	Applies the configured prefix list to prefixes advertised inbound to the specified area.
list_name	Specifies the name of a prefix list.
out	Applies the configured prefix list to prefixes advertised outbound from the specified area.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Only Type 3 LSAs can be filtered. If an ASBR has been configured in the private network, then it sends Type 5 LSAs (describing private networks) that are flooded to the entire AS including the public areas.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
ciscoasa(config-router)# area 1 filter-list prefix-list AREA_1 in
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area nssa

To configure an area as an NSSA, use the **area nssa** command in router configuration mode or IPv6 router configuration mode. To remove the NSSA designation from the area, use the **no** form of this command.

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** { **1** | **2** }] [**metric** *value*]] [**no-summary**]
no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** { **1** | **2** }] [**metric** *value*]] [**no-summary**]

Syntax Description

area_id	Identifies the area being designated as an NSSA. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
default-information-originate	Used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.
metric *metric_value*	(Optional) Specifies the OSPF default metric value. Valid values range from 0 to 16777214.
metric-type {**1** | **2**}	(Optional) the OSPF metric type for default routes. Valid values are the following: • **1**—type 1 • **2**—type 2. The default value is 2.
no-redistribution	(Optional) Used when the router is an NSSA ABR and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area.
no-summary	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Command Default

The defaults are as follows:

- No NSSA area is defined.
- The **metric-type** is 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple content mode and OSPFv3 are supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

If you configure one option for an area, and later specify another option, both options are set. For example, entering the following two command separately results in a single command with both options set in the configuration:

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area area_id nssa default-information-originate
```

Examples

The following example shows how setting two options separately results in a single command in the configuration:

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area 1 nssa default-information-originate
ciscoasa(config-rtr)# exit
ciscoasa(config-rtr)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

Related Commands

Command	Description
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area-password

To configure the IS-IS area authentication password, use the **area-password** command in router isis configuration mode. To disable the password, use the **no** form of this command.

area-password *password* [**authenticate snp** { **validate** | **send-only** }]
no area password [*password*]

Syntax Description

password	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into sequence number PDUS (SNPs).
validate	Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	Causes the system to only insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Command Default

No area password is defined and area password authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

Using the **area-password** command on all routers in an area prevents unauthorized routers from injecting false routing information into the link-state database.

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 1 (station router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an area authentication password and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
ciscoasa(config-router)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.

Command	Description
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.

Command	Description
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

area range (ipv6 router ospf)

To consolidate and summarize OSPFv3 routes at an area boundary, use the **area range** command in ipv6 router ospf configuration mode. To disable this function, use the **no** form of this command.

area *area_id ipv6-prefix-/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]
no area *area_id ipv6-prefix-/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

Syntax Description

advertise	(Optional) Sets the range status to advertise and generates Type 3 summary link-state advertisements (LSAs).
area_id	Specifies the identifier of the area for which routes are to be summarized. You can specify the identifier as either a decimal number or an IPv6 prefix.
cost *cost*	(Optional) Specifies the metric or cost for this summary route, which is used during OSPF SPF calculations to detemine the shortest paths to the destination. Valid values range from 0 to 16777215.
ipv6-prefix	Specifies the IPv6 prefix.
not-advertise	(Optional) Sets the range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
prefix-length	Specifies the IPv6 prefix length.

Command Default

The range status is set to advertise by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each IPv6 prefix and prefix

length. This behavior is called *route summarization* . You can configure multiple **area range** commands for an area. In this way, OSPFv3 can summarize routes for many different sets of IPv6 prefixes and prefix lengths.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for IPv6 prefix 2000:0:0:4::2 with the prefix-length 2001::/64:

```
ciscoasa(config-router)# area 1 range
2000:0:0:4::2/2001::/64

ciscoasa(config-router)#
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode for OSPFv3.
show running-config ipv6 router	Displays the IPv6 commands in the global router configuration.

area range (router ospf)

To consolidate and summarize routes at an area boundary, use the **area range** command in router ospf configuration mode. To disable this function, use the **no** form of this command.

area *area_id* **range** *address mask* **advertise** | **not-advertise**]
no area *area_id* **range** *address mask* **advertise** | **not-advertise**]

Syntax Description

address	IP address of the subnet range.
advertise	(Optional) Sets the address range status to advertise and generates Type 3 summary link-state advertisements (LSAs).
area_id	Identifies the area for which the range is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
mask	IP address subnet mask.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Command Default

The address range status is set to advertise.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization* . You can configure multiple **area range** commands for an area. In this way, OSPF can summarize addresses for many different sets of address ranges.

The **no area** *area_id* **range** *ip_address netmask* **not-advertise** command removes only the **not-advertise** optional keyword.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
ciscoasa(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
ciscoasa(config-router)# area 0 range 192.168.110.0 255.255.255.0
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area stub

To define an area as a stub area, use the **area stub** command in router configuration mode or IPv6 router configuration mode. To remove the stub area, use the **no** form of this command.

area *area_id* **stub** [**no-summary**]
no area *area_id* **stub** [**no-summary**]

Syntax Description

area_id	Identifies the stub area. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
no-summary	Prevents an ABR from sending summary link advertisements into the stub area.

Command Default

The default behaviors are as follows:

- No stub areas are defined.
- Summary link advertisements are sent into the stub area.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

The command is used only on an ABR attached to a stub or NSSA.

There are two stub area router configuration commands: the area stub and area default-cost commands. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost** command only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example configures the specified area as a stub area:

```
ciscoasa(config-rtr)# area 1 stub
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub or NSSA.
area nssa	Defines the area as a not-so-stubby area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area virtual-link (ipv6 router ospf)

To define an OSPFv3 virtual link, use the **area virtual-link** command in ipv6 router ospf configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]
no area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

Syntax Description

area_id	Specifies the area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or valid IPv6 prefix. Valid decimal values range from 0 to 4294967295.
hello-interval *seconds*	(Optional) Specifies the time in seconds between hello packets that the ASA sends on the interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192 seconds.
retransmit-interval *seconds*	(Optional) Specifies the time in seconds between LSA retransmissions for adjacent routers that belong to the interface. The retransmission interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Valid values range from 1 to 8192 seconds.
router_id	Specifies the router ID that is associated with the virtual link neighbor. The router ID appears in the **show ipv6 ospf** or **show ipv6 display** command.
transmit-delay *seconds*	(Optional) Specifies the estimated time in seconds that is required to send a link-state update packet on the interface. The integer value must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. Valid values range from 1 to 8192 seconds.
dead-interval *seconds*	(Optional) Specifies the time in seconds that hello packets are not seen before a neighbor indicates that the router is down. The dead interval in an unsigned integer value. As with the hello interval, this value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192 seconds.
ttl-security hops *hop-count*	(Optional) Configures the time-to-live (TTL) security on a virtual link. Valid values for the hop count range from 1 to 254.



Note Single-digit passwords and passwords starting with a digit followed by a white space are no longer supported.

Command Default

The defaults are as follows:

- *area_id*: No area ID is predefined.

- *router_id*: No router ID is predefined.
- **hello-interval**: 10 seconds.
- **retransmit-interval**: 5 seconds.
- **transmit-delay**: 1 second.
- **dead-interval**: 40 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

In OSPFv3, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic occurs.

The setting of the retransmission interval should be conservative, or unnecessary retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be correctly configured. Use the **show ipv6 ospf** command to obtain the router ID.

Examples

The following example establishes a virtual link in OSPFv3:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello interval 5
```

area virtual-link (router ospf)

To define an OSPF virtual link, use the **area virtual-link** command in router ospf configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0|8]** *key*] | [**message-digest-key** *key_id* **md5[0|8]** *key*]]]]
no area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0|8]** *key*] | [**message-digest-key** *key_id* **md5[0|8]** *key*]]]]

Syntax Description

area_id	Area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
authentication	(Optional) Specifies the authentication type.
key-chain *key-chain-name*	(Optional) Specifies a key chain to use for authentication. The key-name argument can be a maximum of 63 alphanumeric characters.
authentication-key [0 | 8]*key*	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
dead-interval *seconds*	(Optional) Specifies the interval before declaring a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
hello-interval *seconds*	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
md5 [0 | 8] *key*	(Optional) Specifies an alphanumeric key up to 16 bytes.
message-digest	(Optional) Specifies that message digest authentication is used.
message-digest-key *key_id*	(Optional) Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
0	Specifies an unencrypted password will follow.
8	Specifies an encrypted password will follow.
null	(Optional) Specifies that no authentication is used. Overrides password or message digest authentication if configured for the OSPF area.
retransmit-interval *seconds*	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
router_id	The router ID associated with the virtual link neighbor. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.

transmit-delay *seconds*	(Optional) Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535. The default is 5 seconds.

Note Single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported.

Command Default

The defaults are as follows:

- *area_id*: No area ID is predefined.
- *router_id*: No router ID is predefined.
- **hello-interval** *seconds*: 10 seconds.
- **retransmit-interval** *seconds*: 5 seconds.
- **transmit-delay** *seconds*: 1 second.
- **dead-interval** *seconds*: 40 seconds.
- **authentication-key [0 | 8]** *key*: No key is predefined.
- **message-digest-key** *key_id* **md5 [0 | 8]** *key*: No key is predefined.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	We added this command.
9.12(1)	Key chain feature was added to support rotating keys for OSPF authentication.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic ensues.

The setting of the retransmit interval should be conservative, or needless retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

The specified authentication key is used only when authentication is enabled for the backbone with the **area** *area_id* **authentication** command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key [0 | 8]** *key* or **message-digest-key** *key_id* **md5[0 | 8]** *key* are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

If the authentication type is not specified for an interface, the interface uses the authentication type specified for the area. If no authentication type has been specified for the area, the area default is null authentication.



Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be properly configured. Use the **show ospf** command to see the router ID.

Examples

The following example establishes a virtual link with MD5 authentication:

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 8
sa5721bk47
```

The following example establishes a virtual link with rotating keys authentication:

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 authentication key-chain
CHAIN-RTR-OSPFKEY
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
show running-config router	Displays the commands in the global router configuration.

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
show running-config ipv6 router	Displays the IPv6 commands in the global router configuration.

arp

To add a static ARP entry to the ARP table, use the **arp** command in global configuration mode. To remove the static entry, use the **no** form of this command.

arp *interface_name ip_address mac_address* [**alias**]
no arp *interface_name ip_address mac_address*

Syntax Description

alias	(Optional) Enables proxy ARP for this mapping. If the ASA receives an ARP request for the specified IP address, then it responds with the ASA MAC address. When the ASA receives traffic destined for the host belonging to the IP address, the ASA forwards the traffic to the host MAC address that you specify in this command. This keyword is useful if you have devices that do not perform ARP, for example. In transparent firewall mode, this keyword is ignored; the ASA does not perform proxy ARP.
interface_name	The interface attached to the host network.
ip_address	The host IP address.
mac_address	The host MAC address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.

Usage Guidelines

Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

A static ARP entry maps a MAC address to an IP address and identifies the interface through which the host is reached. Static ARP entries do not time out, and might help you solve a networking problem. In transparent firewall mode, the static ARP table is used with ARP inspection (see the **arp-inspection** command).

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the ASA, such as management traffic.

Examples

The following example creates a static ARP entry for 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface:

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Related Commands

Command	Description
arp timeout	Sets the time before the ASA rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp-inspection

To enable ARP inspection for transparent firewall mode, use the **arp-inspection** command in global configuration mode. To disable ARP inspection, use the **no** form of this command.

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]
no arp-inspection *interface_name* **enable**

Syntax Description

enable	Enables ARP inspection.
flood	(Default) Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the ASA drops the packet. **Note** The management-specific interface, if present, never floods packets even if this parameter is set to flood.
interface_name	The bridge group member interface on which you want to enable ARP inspection.
no-flood	(Optional) Specifies that packets that do not exactly match a static ARP entry are dropped.

Command Default

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the ASA. When you enable ARP inspection, the default is to flood non-matching ARP packets.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Gloabl configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	You can now configure this command in routed mode when using Integrated Routing and Bridging.

Usage Guidelines

Configure static ARP entries using the **arp** command before you enable ARP inspection.

ARP inspection checks all ARP packets against static ARP entries (see the **arp** command) and blocks mismatched packets. This feature prevents ARP spoofing.

When you enable ARP inspection, the ASA compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the ASA drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the ASA to either forward the packet out all interfaces (flood), or to drop the packet.

Note The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can then intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, provided the correct MAC address and the associated IP address are in the static ARP table.

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the ASA, such as management traffic.

Examples

The following example enables ARP inspection on the outside interface and sets the ASA to drop any ARP packets that do not match the static ARP entry:

```
ciscoasa(config)# arp outside 209.165.200.225 0009.7cbe.2100
ciscoasa(config)# arp-inspection outside enable no-flood
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp permit-nonconnected

To enable the ARP cache to also include non-directly-connected subnets, use the **arp permit-nonconnected** command in global configuration mode. To disable non-connected subnets, use the **no** form of this command.

arp permit-nonconnected
no arp permit-nonconnected

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(5), 9.0(1)	We added this command.

Usage Guidelines

The ASA ARP cache only contains entries from directly-connected subnets by default. When the **no arp permit-nonconnected** command is there (default behavior), the ASA rejects both incoming ARP requests and ARP responses in case the ARP packet received is in a different subnet than the connected interface.

Note that the first case (default behavior) causes a failure in case PAT is configured on the ASA and the virtual IP address (mapped) for PAT is in a different subnet than the connected interface.

Also, we do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attacks against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.

You may want to use this feature if you use:

- Secondary subnets.
- Proxy ARP on adjacent routes for traffic forwarding.

Examples

The following example enables non-connected subnets:

```
ciscoasa(config)# arp permit non-connected
```

The default behavior can be seen in the output of the **debug arp** command on the ASA as:

For an incoming ARP request:

```
- larp-in: request at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.2.2 0000.0000.0000
having smac 0013.8083.0bb1 dmac ffff.ffff.ffff\narp-in: Arp packet received from 10.10.2.1
 which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

For an incoming ARP response:

The following example enables non-connected subnets:

```
ciscoasa(config)# arp permit non-connected

- arp-in: response at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.1.2 0016.4687.9f43
having smac 0013.8083.0bb1 dmac 0016.4687.9f43\narp-in: Arp packet received from 10.10.2.1
 which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

Related Commands

Command	Description
arp	Adds a static ARP entry.

arp rate-limit

To set the ARP rate limit to control the number of ARP packets per second, use the **arp rate-limit** command in global configuration mode. To restore the default, use the **no** form of this command.

arp rate-limit *seconds*
no arp rate-limit

Syntax Description

seconds	Specifies the number of seconds between 10 and 32768. The default value depends on your ASA model.

Command Default

The default value depends on your ASA model.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

You can customize this value to prevent an ARP storm attack.

Examples

The following example sets the ARP rate to 10000 per second:

```
ciscoasa(config)# arp rate-limit 10000
```

Related Commands

Command	Description
show arp rate-limit	Shows the ARP rate limit.

arp timeout

To set the time before the ASA rebuilds the ARP table, use the **arp timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

arp timeout *seconds*
no arp timeout *seconds*

Syntax Description

seconds	The number of seconds between ARP table rebuilds, from 60 to 4294967.

Command Default

The default value is 14,400 seconds (4 hours).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Gloabl configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.

Usage Guidelines

Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently.

Examples

The following example changes the ARP timeout to 5,000 seconds:

```
ciscoasa(config)# arp timeout 5000
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp timeout	Shows the current configuration of the ARP timeout.

asdm disconnect

To terminate an active ASDM session, use the **asdm disconnect** command in privileged EXEC mode.

asdm disconnect *session*

Syntax Description

session	The session ID of the active ASDM session to be terminated.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm disconnect** command to the **asdm disconnect** command.

Usage Guidelines

Use the **show asdm sessions** command to display a list of active ASDM sessions and their associated session IDs. Use the **asdm disconnect** command to terminate a specific session.

When you terminate an ASDM session, any remaining active ASDM sessions keep their associated session ID. For example, if there are three active ASDM sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM sessions keep the session IDs 0 and 2. The next new ASDM session in this example would be assigned a session ID of 1, and any new sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm sessions** commands display the active ASDM sessions before and after the **asdm disconnect** command is entered.

```
ciscoasa# show asdm sessions
0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm sessions
1 192.168.1.2
```

Related Commands

Command	Description
show asdm sessions	Displays a list of active ASDM sessions and their associated session ID.

asdm disconnect log_session

To terminate an active ASDM logging session, use the **asdm disconnect log_session** command in privileged EXEC mode.

asdm disconnect log_session *session*

Syntax Description

session	The session ID of the active ASDM logging session to be terminated.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **show asdm log_sessions** command to display a list of active ASDM logging sessions and their associated session IDs. Use the **asdm disconnect log_session** command to terminate a specific logging session.

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the ASA. Terminating a log session may have an adverse effect on the active ASDM session. To terminate an unwanted ASDM session, use the **asdm disconnect** command.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

When you terminate an ASDM logging session, any remaining active ASDM logging sessions keep their associated session ID. For example, if there are three active ASDM logging sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM logging sessions keep the session IDs 0 and 2. The next new ASDM logging session in this example would be assigned a session ID of 1, and any new logging sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm log_sessions** commands display the active ASDM sessions before and after the **asdm disconnect log_sessions** command is entered.

```
ciscoasa# show asdm log_sessions
0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm log_sessions
1 192.168.1.2
```

Related Commands

Command	Description
show asdm log_sessions	Displays a list of active ASDM logging sessions and their associated session ID.

asdm history enable

To enable ASDM history tracking, use the **asdm history enable** command in global configuration mode. To disable ASDM history tracking, use the **no** form of this command.

asdm history enable
no asdm history enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm history enable** command to the **asdm history enable** command.

Usage Guidelines

The information obtained by enabling ASDM history tracking is stored in the ASDM history buffer. You can view this information using the **show asdm history** command. The history information is used by ASDM for device monitoring.

Examples

The following example enables ASDM history tracking:

```
ciscoasa(config)# asdm history enable
ciscoasa(config)#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

asdm image

To specify the location of the ASDM software image in flash memory, use the **asdm image** command in global configuration mode. To remove the image location, use the **no** form of this command.

asdm image *url*
no asdm image [*url*]

Syntax Description

url Sets the location of the ASDM image in flash memory. See the following URL syntax:

- **disk0:**/[*path*/]*filename*

For the ASA 5500 series, this URL indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased.

- **disk1:**/[*path*/]*filename*

For the ASA 5500 series, this URL indicates the external Flash memory card.

- **flash:**/[*path*/]*filename*

This URL indicates the internal Flash memory.

Command Default

If you do not include this command in your startup configuration, the ASA uses the first ASDM image it finds at startup. It searches the root directory of internal Flash memory and then external flash memory. The ASA then inserts the **asdm image** command into the running configuration if it discovered an image.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can store more than one ASDM software image in flash memory. If you enter the **asdm image** command to specify a new ASDM software image while there are active ASDM sessions, the new command does not disrupt the active sessions; active ASDM sessions continue to use the ASDM software image they started with. New ASDM sessions use the new software image. If you enter the **no asdm image** command, the command is removed from the configuration. However, you can still access ASDM from the ASA using the last-configured image location.

If you do not include this command in your startup configuration, the ASA uses the first ASDM image it finds at startup. It searches the root directory of internal flash memory and then external flash memory. The ASA then inserts the **asdm image** command into the running configuration if it discovered an image. Be sure to save the running configuration to the startup configuration using the **write memory** command. If you do not save the **asdm image** command to the startup configuration, every time you reboot, the ASA searches for an ASDM image and inserts the **asdm image** command into your running configuration. If you are using Auto Update, the automatic addition of this command at startup causes the configuration on the ASA not to match the configuration on the Auto Update Server. This mismatch causes the ASA to download the configuration from the Auto Update Server. To avoid unnecessary Auto Update activity, save the **asdm image** command to the startup configuration.

Examples

The following example sets the ASDM image to asdm.bin:

```
ciscoasa(config)# asdm image flash:/asdm.bin
ciscoasa(config)#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.
boot	Sets the software image and startup configuration files.

asdm location

Caution Do not manually configure this command. ASDM adds **asdm location** commands to the running configuration and uses them for internal communication. This command is included in the documentation for informational purposes only.

asdm location *ip_addr netmask if_name*
asdm location *ipv6_addr/prefix if_name*

Syntax Description

if_name	The name of the highest security interface. If you have multiple interfaces at the highest security, then an arbitrary interface name is chosen. This interface name is not used, but is a required parameter.
ip_addr	The IP address used internally by ASDM to define the network topology.
ipv6_addr/prefix	The IPv6 address and prefix used internally by ASDM to define the network topology.
netmask	The subnet mask for *ip_addr*.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm location** command to the **asdm location** command.

Usage Guidelines

Do not manually configure or remove this command.

as-path access-list

To configure an autonomous system path filter using a regular expression, use the as-path access-list command in global configuration mode. To delete the autonomous system path filter and remove it from the running configuration file, use the no form of this command.

as-path access-list *acl-name* { **permit** | **deny** } *regexp*
no as-path access-list *acl-name*

Syntax Description

acl-name	Name that specifies the AS-path access-list.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions
regexp	Regular expression that defines the AS-path filter. The autonomous system number is expressed in the range from 1 to 65535. For more details about autonomous system number formats, see the router bgp command. **Note** See the "Regular Expressions" appendix in the Cisco IOS Terminal Services Configuration Guide for information about configuring regular expressions.

Command Default

No autonomous system path filter is created.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	We added this command.

Usage Guidelines

Use the as-path access-list command to configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the permit or deny condition applies. The autonomous system path should not contain the local autonomous system number.

The Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described

in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail.

Examples

In the following example, an autonomous system path access list (number 500) is defined to configure the ASA to not advertise any path through or from autonomous system 65535 to the 10.20.2.2 neighbor:

```
ciscoasa(config)# as-path access-list as-path-acl deny _65535_
ciscoasa(config)# as-path access-list as-path-acl deny ^65535$
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-fmaily ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.1 remote-as 65535
ciscoasa(config-router-af)# neighbor 10.20.2.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 10.20.2.2 filter-list as-path-acl out
```

asp load-balance per-packet

For multi-core ASAs, to change the load balancing behavior to be per packet, use the **asp load-balance per-packet** command in global configuration mode. To restore the default load-balancing mechanism, use the **no** form of this command.

asp load-balance per-packet [**auto**]
no asp load-balance per-packet

Syntax Description

auto	Automatically enables and disables per-packet load-balancing on each interface receive ring according to network conditions.

Command Default

Per-packet load-balancing is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Gloabl configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.1(1)	We added this command.
9.3(1)	The **auto** option was added.
9.8(1)	The **auto** option is now available for the ASA Virtual.

Usage Guidelines

The job of the load balancer is to distribute packets to CPU cores and to maintain packet order. By default, a connection can only be processed by one core at a time. Due to this behavior, the cores will be under-utilized if there are a small number of interfaces/RX rings in use when compared to the number of cores. For example if there are only two Gigabit Ethernet interfaces in use on an ASA, then only two cores will be used. (A Ten Gigabit Ethernet interface has 4 RX rings and a Gigabit Ethernet interface as 1 RX ring.) You may want to optimize the load balancer by enabling per-packet load balancing so you can use more cores.

The default load-balancing behavior optimizes overall system performance when you have many interfaces in use, while the per-packet load balancer optimizes the overall system performance when you have a smaller number of interfaces that are active.

If you enable per-packet load balancing, when one core processes packets from an interface, another core can receive and process the next packet from the same interface. Therefore, it is possible for all cores to process packets from the same interface simultaneously.

Per-packet load balancing will improve performance if:

- The system drops packets
- The **show cpu** command shows CPU usage far less than 100%—The CPU usage is a good indicator of how many cores are being used. For example, on an 8-core system, if two cores are used, **show cpu** shows 25%; four cores: 50%; six cores: 75%.
- There are a small number of interfaces that are in use

Note Typically if there are less than 64 concurrent flows on the ASA, then enabling per-packet load balancing will incur more overhead than its benefit.

The **auto** option enables the ASA to detect whether or not asymmetric traffic has been added. The one-to-one lock between interface receive rings and cores is released if load balancing is needed. Load balancing per packet is only enabled on the heavily-loaded interface receive rings, not on all the interface receive rings. This adaptive load balance mechanism helps avoid the following issues:

- Overruns caused by sporadic traffic spikes on flows
- Overruns caused by bulk flows oversubscribing specific interface receive rings
- Overruns caused by relatively heavily overloaded interface receive rings, in which a single core cannot sustain the load.

The **auto** option is not available for the ASA Virtual in 9.7 and earlier.

Examples

The following example shows how to change the default load-balancing behavior:

```
ciscoasa(config)# asp load-balance per-packet
```

The following example enables the automatic switching on and off of per-packet load balancing:

```
ciscoasa(config)# asp load-balance per-packet auto
```

Related Commands

Command	Description
clear asp load-balance history	Clears and resets the ASP load balancing per packet history statistics.
show asp load-balance	Displays a histogram of the load balancer queue sizes.
show asp load-balance per-packet	Displays current status, high and low watermarks, and the global threshold.
show asp load-balance per-packet history	Displays current status, high and low watermarks, the global threshold, the times of switching ASP load balancing per packet on and off since the last reset, the history of ASP load balancing per packet with time stamps, and the reasons for switching it on and off.

asp rule-engine compile-offload

Use the **asp rule-engine compile-offload** command to enable or disable the compile offload function for the rule engine.

asp rule-engine compile-offload [**threshold** *rule-threshold*]
no asp rule-engine compile-offload [**threshold** *rule-threshold*]

Syntax Description

threshold*rule-threshold*	Rule update threshold count to offload the compilation, 1 – 1000000. Default is 100.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was introduced.

Usage Guidelines

When enabled, tmatch compilation is offloaded to the data path from the control plane if the tmatch object rule update count is greater than the threshold value. This leaves more time for the control plane to perform other tasks. Offloaded compliation is for rule-based policies such as ACLs, NAT, and VPN.

Because there is a fixed overhead to offload the compilation, you can increase the default threshold of 100 to adjust performance. The default threshold should work well in most cases.

Example

The following example increases the threshold to 1000.

```
ciscoasa(config)# asp rule-engine compile-offload threshold 1000
```

Related Commands

Command	Description
show asp rule-engine	Displays the status of the ASP rule engine.

asp rule-engine transactional-commit

Use the **asp rule-engine transactional-commit** command to enable or disable the transactional commit model for the rule engine.

asp rule-engine transactional-commit *option*
no asp rule-engine transactional-commit *option*

Syntax Description

option Enables the transactional commit model for the rule engine for the selected policies. Options include:

- **access-group**—Access rules applied globally or to interfaces.
- **nat**—Network address translation rules.

Command Default

By default, the transactional commit model is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(5)	We added this command.
9.3(1)	We added the **nat** keyword.

Usage Guidelines

By default, when you change a rule-based policy (such as access rules), the changes become effective immediately. However, this immediacy comes at a slight cost in performance. The performance cost is more noticeable for very large rule lists in a high connections-per-second environment, for example, when you change a policy with 25,000 rules while the ASA is handling 18,000 connections per second.

The performance is affected because the rule engine compiles rules to enable faster rule lookup. By default, the system will also search uncompiled rules when evaluating a connection attempt so that new rules can be applied; since the rules are not compiled, the search takes longer.

You can change this behavior so that the rule engine uses a transactional model when implementing rule changes, continuing to use the old rules until the new rules are compiled and ready for use. Using the transactional model, performance should not drop during the rule compilation. The following table clarifies the behavioral difference.

Model	Before Compilation	During Compilation	After Compilation
Default	Match old rules.	Match new rules. (Connections per second rate will decrease.)	Match new rules.
Transactional	Match old rules.	Match old rules. (Connections per second rate will be unaffected.)	Match new rules.

An additional benefit of the transactional model is that, when replacing an ACL on an interface, there is no gap between deleting the old ACL and applying the new one. This reduces the chances that acceptable connections will be dropped during the operation.

Tip If you enable the transactional model for a rule type, there are syslog messages to mark the beginning and the end of the compilation. These messages are numbered 780001 and following.

Examples

The following example enables the transactional commit model for access groups:

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

Related Commands

Command	Description
clear conf asp rule-engine transactional-commit	Clears the transactional commit configurations for the rule engine.
show asp rule-engine	Displays the status of the ASP rule engine.

asr-group

To specify an asymmetrical routing interface group ID, use the **asr-group** command in interface configuration mode. To remove the ID, use the **no** form of this command.

asr-group *group_id*
no asr-group *group_id*

Syntax Description

group_id	The asymmetric routing group ID. Valid values are from 1 to 32.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	—	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When Active/Active failover is enabled, you may encounter situations where load balancing causes the return traffic for outbound connections to be routed through an active context on the peer unit, in which the context for the outbound connection is in the standby group.

The **asr-group** command causes incoming packets to be reclassified with the interface of the same ASR group if a flow with the incoming interface cannot be found. If reclassification finds a flow with another interface, and the associated context is in standby state, then the packet is forwarded to the active unit for processing.

Stateful Failover must be enabled for this command to take effect.

You can view ASR statistics using the **show interface detail** command. These statistics include the number of ASR packets sent, received, and dropped on an interface.

Note No two interfaces in the same context should be configured in the same ASR group.

Examples

The following example assigns the selected interfaces to the asymmetric routing group 1.

Context ctx1 configuration:

```
ciscoasa/ctx1(config)# interface Ethernet2
ciscoasa/ctx1(config-if)# nameif outside
ciscoasa/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
ciscoasa/ctx1(config-if)# asr-group 1
```

Context ctx2 configuration:

```
ciscoasa/ctx2(config)# interface Ethernet3
ciscoasa/ctx2(config-if)# nameif outside
ciscoasa/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
ciscoasa/ctx2(config-if)# asr-group 1
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
show interface	Displays interface statistics.

assertion-consumer-url (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To identify the URL that the security device accesses to contact the assertion consumer service, use the **assertion-consumer-url** command in the webvpn configuration mode for that specific SAML-type SSO server. To remove the URL from the assertion, use the **no** form of this command.

assertion-consumer-url *url*
no assertion-consumer-url [*url*]

Syntax Description

url	Specifies the URL of the assertion consumer service used by the SAML-type SSO server. The URL must start with either http:// or https:// and must be less than 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.5(2)	This command was deprecated, with the introduction of support for SAML 2.0.

Usage Guidelines

Single sign-on (SSO) support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO servers.

If the URL begins with HTTPS, the requirement is to install the root certificate for the assertion consumer service SSL certificate.

Examples

The following example specifies the assertion consumer URL for a SAML-type SSO server:

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
```

```
ciscoasa(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
ciscoasa(config-webvpn-sso-saml#
```

Related Commands

Command	Description
issuer	Specifies the SAML-type SSO server security device name.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a WebVPN SSO server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

attribute bind

To change the IP-to-attribute binding for an attribute-based network object, use the **attribute bind** command in EXEC mode.

attribute bind *agent-name* **binding** *ip-address* **type** *attribute-type* **value** *attribute-value*

Syntax Description

agent-name	Specifies the name of the VM attribute agent monitoring the attribute.
ip-address	Specifies the IP address of the attribute-based network object being managed.
attribute-type	Specifies the string identifying the attribute type to be updated.
attribute-value	Specifies the string identifying the new value to be assigned to the attribute type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Examples

The following example specifies the assertion consumer URL for a SAML-type SSO server:

```
ciscoasa(config)# attribute bind VMAgent binding 10.10.1.19 type custom.location value
global
```

Related Commands

Command	Description
attribute source-group	Configures a VM attribute agent.
object network attribute	Configures an attribute-based network object.
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attribute source-group

To configure a VM attribute agent to communicate with VMware vCenter or a single ESXi host, use the **attribute source-group** command in EXEC mode. To delete an agent, use the **no** form of this command.

attribute source-group *agent-name* **type** *agent-type*
no attribute source-group *agent-name*

Syntax Description

agent-name	Specifies the name of the VM attribute agent name.
agent-type	Specifies the the type of attribute agent. Currently ESXi is the only supported agent type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Examples

The following example shows how to configure a VM attribute agent:

```
ciscoasa(config)# attribute source-group VMAgent type esxi
```

Related Commands

Command	Description
object network attribute	Configures an attribute-based network object.
show attribute source-group	Shows information about configured attribute agents.
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attribute source-group host

To configure VMware vCenter host credentials that allow a VM attribute agent to communicate with vCenter or a single ESXi host, use the **attribute source-group host** command in attribute agent configuration mode. To delete host credentials, use the **no** form of this command.

host *ip-address* **username** *ESXi-username* **password** *ESXi-password*
no host *ip-address*

Syntax Description

ip-address	Specifies the name of the VM attribute agent.
ESXi-username	Specifies the vCenter host username.
ESXi-password	Specifies the vCenter host password.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Attribute agent configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use this command after you configure or modify an attribute agent.

Examples

The following example shows how to configure host credentials for an attribute agent:

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# host 10.122.202.217 user admin password Cisco123
```

Related Commands

Command	Description
attribute source-group	Configures a VM attribute agent.
object network attribute	Configures an attribute-based network object.
show attribute source-group	Shows information about configured attribute agents.

Command	Description
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attribute source-group keepalive

To configure keepalive settings for VMware vCenter communication, use the **attribute source-group keepalive** command in attribute agent configuration mode. To restore the default values, use the **no** form of this command.

keepalive retry-interval *interval* **retry-count** *count*
no keepalive

Syntax Description

interval	Specifies the interval between keepalive messages from the attribute agent to vCenter. Each time a keepalive message receives a response from the source, the agent is considered to be in contact with the source, and the keepalive timer for that agent is restarted. The default is 30 seconds.
count	Specifies the retry count when a keepalive message is not received. Each time the timer expires without receiving a keepalive, the retry count for that agent is incremented. If the retry count reaches the configured threshold value, the agent declares that it has lost contact with the source. The default is 3.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Attribute agent configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use this command after you configure or modify an attribute agent.

Examples

The following example specifies the assertion consumer URL for a SAML-type SSO server:

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# keepalive retry-timer 100 retry-count 5
```

Related Commands

Command	Description
attribute source-group	Configures a VM attribute agent.
object network attribute	Configures an attribute-based network object.

Command	Description
show attribute source-group	Shows information about configured attribute agents.
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attributes

To specify attribute value pairs that the ASA writes to the DAP attribute database, enter the **attributes** command in dap test attributes mode.

attributes *name value*

Syntax Description

name	Specifies a well-known attribute name, or an attribute that incorporates a "label" tag. The label tag corresponds to the endpoint ID that you configure for file, registry, process, antivirus, antispyware, and personal firewall endpoint attributes in the DAP record.
value	The value assigned to the AAA attribute.

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
DAP attributes configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use this command multiple times to enter multiple attribute value pairs.

Normally the ASA retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The ASA writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint selection attributes for a DAP record.

Examples

The following example assumes that ASA selects two DAP records if the authenticated user is a member of the SAP group and has antivirus software installed on the endpoint system. The endpoint ID for the antivirus software endpoint rule is *nav*.

The DAP records have the following policy attributes:

DAP Record 1	DAP Record 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2

DAP Record 1	DAP Record 2
—	url-entry = enable

```
ciscoasa
 #
test dynamic-access-policy attributes
ciscoasa
(config-dap-test-attr)#
attributes aaa.ldap.memberof SAP
ciscoasa
(config-dap-test-attr)#
 attributes endpoint.av.nav.exists true
ciscoasa
(config-dap-test-attr)#
exit
ciscoasa
 #
test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable
ciscoasa
 #
```

Related Commands

Command	Description
display	Displays current attribute lists.
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes.
test dynamic-access-policy execute	Executes the logic that generates the DAP and displays the resulting access policies to the console.

auth-cookie-name

To specify the name of an authentication cookie, use the **auth-cookie-name** command in aaa-server host configuration mode. This is an SSO with HTTP Forms command.

auth-cookie-name

Syntax Description

name	The name of the authentication cookie. The maximum name size is 128 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The WebVPN server of the ASA uses an HTTP POST request to submit a single sign-on (SSO) authentication request to an SSO server. If authentication succeeds, the authenticating web server passes back an authentication cookie to the client browser. The client browser then authenticates to other web servers in the SSO domain by presenting the authentication cookie. The **auth-cookie-name** command configuresthe name of the authentication cookie to be used for SSO by the ASA.

A typical authentication cookie format is Set-Cookie: *cookie name =cookie value* [;*cookie attributes*]. In the following authentication cookie example, SMSESSION is the name that would be configured with the **auth-cookie-name** command:

```
Set-Cookie:
```

Examples

The following example specifies the authentication cookie name of SMSESSION for the authentication cookie received from a web server named example.com:

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# auth-cookie-name SMSESSION
ciscoasa(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies that a username parameter must be submitted as part of the HTTP POST request used for SSO authentication.

authenticated-session-username

To specify which authentication username to associate with the session when double authentication is enabled, use the **authenticated-session-username** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

authenticated-session-username { **primary** | **secondary** }
no authenticated-session-username

Syntax Description

primary	Uses the username from the primary authentication server.
secondary	Uses the username from the secondary authentication server.

Command Default

The default value is **primary**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **authenticated-session-username** command selects the authentication server from which the ASA extracts the username to associate with the session.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies the use of the username from the secondary authentication server for the connection:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authenticated-session-username secondary
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the prefill username feature.

Command	Description
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

authentication (bfd-template)

To configure authentication in a BFD template for single-hop and multi-hop sessions, use the authentication command in BFD configuration mode. To disable authentication in the BFD template for single-hop or multi-hop sessions, use the **no** form of this command.

authentication *authentication-type* [**0|8**] *key-string* **key-id** *id*

Syntax Description

authentication-type	Specifies the authentication type. Valid values are **md5**, **meticulous-md5**, **meticulous-sha-1**, and **sha-1**.
0|8	0 specifies that an UNENCRYPTED password will follow. 8 specifies that an ENCRYPTED password will follow.
key-string	Specifies the authentication string that must be sent and received in the packets using the routing protocol being authenticated. The valid range is 1 to 17 uppercase and lowercase alphanumeric characters, except that the first character CANNOT be a number.
id	Specifies the shared key ID that matches the key string.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
BFD configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to configure authentication in a BFD single-hop and multi-hop templates. We recommend that you configure authentication to enhance security.

Authentication must be configured on each BFD source-destination pair, and authentication parameters must match on both devices.

Examples

The following example configures authentication in a single-hop BFD template.

```
ciscoasa(config)# bfd single-hop sh-template
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

The following example configures authentication in a multi-hop BFD template.

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# authentication shat-1 0 cisco key-id 10
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

authentication

To configure the authentication method for WebVPN and e-mail proxies, use the **authentication** command in various modes. To restore the default method, use the **no** form of this command. The ASA authenticates users to verify their identity.

authentication [{ [**aaa**] [**certificate**] [**multiple certificate**] [**saml**] [**mailhost**] [**piggyback**] }
no authentication [[**aaa**] [**certificate**] [**multiple certificate**] [**saml**] [**mailhost**] [**piggyback**]

Syntax Description

aaa	Provides a username and password that the ASA checks with a previously configured AAA server.
certificate	Provides a certificate during SSL negotiation.
mailhost	Authenticates via the remote mail server for SMTPS only. For IMAP4S and POP3S, mailhost authentication is mandatory and not displayed as a configurable option.
multiple certificate	Provides a multiple certificate option during SSL negotiation.
piggyback	Requires that an HTTPS WebVPN session already exist. Piggyback authentication is available for e-mail proxies only.
saml	SAML authentication method is mutually exclusive.

Command Default

The following table shows the default authentication methods for WebVPN and e-mail proxies:

Protocol	Default Authentication Method
IMAP4S	Mailhost (required)
POP3S	Mailhost (required)
SMTPS	AAA
WebVPN	AAA

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—
Webvpn configuration	• Yes	—	• Yes		
Tunnel group Webvpn configuration	• Yes	—	• Yes		

Command History

Release	Modification
8.0(2)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group webvpn-attributes configuration mode for WebVPN.
8.0(2)	This command was modified to reflect changes to certificate authentication requirements.
9.5(2)	This command was modified to reflect support for SAML 2.0
9.7(1)	The existing authenticatioin attribute is modified to include an option for multiple-certificate authentication.

Usage Guidelines

At least one authentication method is required. For WebVPN, for example, you can specify AAA authentication, certificate authentication, or both. You can enter these commands in either order.

WebVPN certificate authentication requires that HTTPS user certificates be required for the respective interfaces. That is, for this selection to be operational, before you can specify certificate authentication, you must have specified the interface in an **authentication-certificate** command.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group webvpn-attributes configuration mode.

For WebVPN, you can require both AAA and certificate authentication. In this case, users must provide both a certificate and a username and password. For e-mail proxy authentication, you can require more than one authentication method. Specifying the command again overwrites the current configuration.

Examples

The following example shows how to require that WebVPN users provide certificates for authentication:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication certificate
```

Examples

The following example shows how to require that WebVPN users provide certificates for authentication:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication certificate
```

Related Commands

Command	Description
authentication-certificate	Requests a certificate from a WebVPN client establishing a connection.
show running-config	Displays the current tunnel group configuration.
clear configure aaa	Removes or resets the configured AAA values.
show running-config aaa	Displays the AAA configuration.

authentication eap-proxy

For L2TP over IPsec connections, to enable EAP and permit the ASA to proxy the PPP authentication process to an external RADIUS authentication server, use the **authentication eap-proxy** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication eap-proxy
no authentication eap-proxy

Syntax Description

This command has no keywords or arguments.

Command Default

By default, EAP is not a permitted authentication protocol.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ppp-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel group type.

Examples

The following example entered in config-ppp configuration mode, permits EAP for PPP connections for the tunnel group named ppremotegrp:

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication eap
ciscoasa(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication key

To enable authentication for IS-IS, use the **authentication key** command in router isis configuration mode. To disable such authentication, use the **no** form of this command

authentication key [**0** | **8**] *password* [**level-1** | **level-2**]
no authentication key [**0** | **8**] *password* [**level-1** | **level-2**]

Syntax Description

password	Enables authentication and specifies the key.
level-1	(Optional) Enables authentication for Level 1 packets only.
level-2	(Optional) Enables authentication for Level 2 packets only.

Command Default

No key authentication is provided for IS-IS packets at the router level.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If no password is configured with the **key** command, no key authentication is performed.

Key authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the authentication mode command.

Only one authentication key is applied to IS-IS at one time. That is, if you configure a second authentication key command, the first is overridden.

If neither the **level-1** nor **level-2** keyword is configured, the password applies to both levels.

You can specify authentication for an individual IS-IS interface by using the **isis authentication key** command.

Note In IS-IS, the **authentication key-chain** command is used to select live for the globally configured key chain. Due to the absence of the key chain infrastructure in ASA, we supply the key along with the command.

Examples

The following example configures IS-IS to accept and send any key belonging to the key chain named site1:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).

Command	Description
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.

Command	Description
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

authentication key eigrp

To enable authentication of EIGRP packets and specify the authentication key, use the **authentication key eigrp** command in interface configuration mode. To disable EIGRP authentication, use the **no** form of this command.

authentication key eigrp *as-number key* **key-id** *key-id*
no authentication key eigrp *as-number*

Syntax Description

as-number	The autonomous system number of the EIGRP process being authenticated. This must be the same value as configured for the EIGRP routing process.
key	Key to authenticate EIGRP updates. The key can contain up to 16 characters.
key-id *key-id*	Key identification value; valid values range from 1 to 255.

Command Default

EIGRP authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

You must configure both the **authentication mode eigrp** and the **authentication key eigrp** commands on an interface to enable EIGRP message authentication. Use the **show running-config interface** command to view the **authentication** commands configured on an interface.

Examples

The following examples shows EIGRP authentication configured on interface GigabitEthernet0/3:

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# authentication mode eigrp md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

Related Commands

Command	Description
authentication mode eigrp	Specifies the type of authentication used for EIGRP authentication.

authentication mode

To specify the type of authentication used in IS-IS packets for the IS-IS instance, use the **authentication mode** command in router isis configuration mode. To restore clear text authentication, use the **no** form of this command.

authentication mode { **md5** | **text** } [**level-1** | **level-2**]
no authentication mode

Syntax Description

md5	Message Digest 5 (MD5) authentication.
text	Clear text authentication.
level-1	(Optional) Enables the specified authentication for Level 1 packets only.
level-2	(Optional) Enables the specified authentication for Level 2 packets only.

Command Default

No authentication is provided for IS-IS packets at the router level by use of this command, although you can configure clear text (plain text) authentication by other means, such as the **area-password** command or the **domain-password** command.

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Usage Guidelines

If neither the **level-1** nor **level-2** keyword is configured, the mode applies to both levels.

You can specify the type of authentication and the level to which it applies for a single IS-IS interface, rather than per IS-IS instance, by using the **isis authentication mode** command.

If you had clear text authentication configured by using the **area-password** or **domain-password** command, the authentication mode command overrides both of those commands.

If you configure the authentication mode command and subsequently try to configure the **area-password** or **domain-password** command, you will not be allowed to do so. If you truly want to configure clear text authentication using the **area-password** or **domain-password** command, you must use the **no authentication mode** command first.

Examples

The following example configures MD5 authentication for the IS-IS instance on Level 1 packets:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

authentication ms-chap-v1

For L2TP over IPsec connections, to enable Microsoft CHAP, Version 1 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode.To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command. To disable Microsoft CHAP, Version 1, use the **no** form of this command.

authentication ms-chap-v1
no authentication ms-chap-v1

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ppp-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel-group type. This protocol is similar to CHAP, but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

authentication ms-chap-v2

For L2TP over IPsec connections, to enable Microsoft CHAP, Version 2 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication ms-chap-v2
no authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ppp-attributes configurationn	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel-group type.

This protocol is similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than clear text passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel group database or just the specified tunnel group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

authentication pap

For L2TP over IPsec connections, to permit PAP authentication for PPP, use the **authentication pap** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication pap
no authentication pap

Syntax Description

This command has no keywords or arguments.

Command Default

By default, PAP is not a permitted authentication protocol.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ppp-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel group type.

This protocol passes the clear text username and password during authentication and is not secure.

Examples

The following example entered in config-ppp configuration mode, permits PAP for PPP connections for a tunnel group named ppremotegrps:

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication pap
ciscoasa(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.

Command	Description
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication send-only

To specify for the IS-IS instance that authentication is performed only on IS-IS packets being sent (not received), use the **authentication send-only** command in router isis configuration mode. To configure authentication to be performed on packets being sent and received, use the **no** form of this command.

authentication send-only [**level-1** | **level-2**]
no authentication send-only

Syntax Description

level-1	(Optional) Authentication is performed only on Level 1 packets that are being sent (not received).
level-2	(Optional) Authentication is performed only on Level 2 packets that are being sent (not received).

Command Default

If authentication is configured at the router level, it applies to IS-IS packets being sent and received.

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Usage Guidelines

Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. The routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then specify the **no authentication send-only** command to disable the send only feature.

If neither the **level-1** nor **level-2** keyword is configured, the send only feature applies to both levels.

This command can apply to clear text authentication or MD5 authentication. The mode is determined by the **authentication mode** command.

Examples

The following example configures IS-IS Level 1 packets to use clear text authentication on packets being sent (not received):

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication key-chain site1 level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.

Command	Description
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.

Command	Description
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

authentication-attr-from-server

To specify which authentication server authorization attributes to apply to the connection when double authentication is enabled, use the **authentication-attr-from-server** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

authentication-attr-from-server { **primary** | **secondary** }
no authentication-attr-from-server

Syntax Description

primary	Uses the primary authentication server.
secondary	Uses the secondary authentication server.

Command Default

The default value is **primary**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **authentication-attr-from-server** command selects the authentication server from which the ASA extracts the authorization attributes to be applied to the connection.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies that the authorization attributes to be applied to the connection must come from the secondary authentication server:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-attr-from-server secondary
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the prefill username feature.

Command	Description
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

authentication-certificate

To request a certificate from a WebVPN client establishing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

authentication-certificate *interface-name*
no authentication-certificate [*interface-name*]

Syntax Description

interface-name The name of the interface used to establish the connection. Available interfaces names are:

- **inside** Name of interface GigabitEthernet 0/1
- **outside** Name of interface GigabitEthernet 0/0

Command Default

If you omit the **authentication-certificate** command, client certificate authentication is disabled. If you do not specify an interface name with the **authentication-certificate** command, the default interface name is **inside**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

For this command to take effect, WebVPN must already be enabled on the corresponding interface. An interface is configured and named with the **interface**, **IP address**, and **nameif** commands.

This command applies only to WebVPN client connections; however, the ability to specify client certificate authentication for management connections with the **http authentication-certificate** command is available on all platforms, including those that do not support WebVPN.

The ASA validates certificates using the PKI trustpoints. If a certificate does not pass validation, then one of the following actions occurs:

If:	Then:
The local CA embedded in the ASA is not enabled.	The ASA closes the SSL connection.

If:	Then:
The local CA is enabled, and AAA authentication is not enabled.	The ASA redirects the client to the certificate enrollment page for the local CA to obtain a certificate.
Both the local CA and AAA authentication are enabled.	The client is redirected to a AAA authentication page. If configured, the client also is presented with a link to the enrollment page for the local CA.

Examples

The following example configures certificate authentication for WebVPN user connections on the outside interface:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
authentication (tunnel-group webvpn configuration mode)	Specifies that the members of a tunnel group must use a digital certificate for authentication.
http authentication-certificate	Specifies authentication by means of certificate for ASDM management connections to the ASA.
interface	Configures the interface used to establish the connection
show running-config ssl	Displays the current set of configured SSL commands.
ssl trust-point	Configures the SSL certificate trustpoint.

authentication-exclude

To enable end users to browse to configured links without logging in to clientless SSL VPN, enter the **authentication-exclude** command in webvpn configuration mode. Use this command multiple times to permit acccess to multiple sites.

authentication-exclude *url-fnmatch*

Syntax Description

url-fnmatch	Identifies the link to exempt from the requirement to log in to a clientless SSL VPN.

Command Default

Disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

This feature is useful when you require some internal resources to be available for public use via SSL VPN.

You need to distribute information about the links to end users in an SSL VPN-mangled form, for example, by browsing to these resources using SSL VPN and copying the resulting URLs into the information about links that you distribute.

Examples

The following example shows how to exempt two sites from authentication requirements:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 authentication-exclude http://www.example.com/public/*
ciscoasa
(config-webvpn)#
authentication-exclude *example.html
ciscoasa
(config-webvpn)#
ciscoasa
 #
```

authentication-port

To specify the port number used for RADIUS authentication for this host, use the **authentication-port** command in aaa-server configuration host configuration mode. To remove the authentication port specification, use the **no** form of this command.

authentication-port *port*
no authentication-port

Syntax Description

port	A port number, in the range 1-65535, for RADIUS authentication.

Command Default

By default, the device listens for RADIUS on port 1645 (in compliance with RFC 2058). If the port is not specified, the RADIUS authentication default port number 1645 is used.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	Semantic change to the command to support the specification of server ports on a per-host basis for server groups that contain RADIUS servers.

Usage Guidelines

This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to assign authentication functions. If your RADIUS authentication server uses a port other than 1645, you must configure the ASA for the appropriate port before starting the RADIUS service with the **aaa-server** command.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry interval of 7 seconds, and configures authentication port 1650.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
```

```
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication on a server designated by the aaa-server command or by ASDM user authentication.
aaa-server host	Enters aaa-server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

authentication-server-group (imap4s, pop3s, smtps) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify the set of authentication servers to use for e-mail proxies, use the **authentication-server-group** command in various modes. To remove authentication servers from the configuration, use the **no** form of this command.

authentication-server-group *group_tag*
no authentication-server-group

Syntax Description

group_tag	Identifies the previously configured authentication server or group of servers.

Command Default

No authentication servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

The ASA authenticates users to verify their identity.

If you configure AAA authentication, you must configure this attribute as well. Otherwise, authentication always fails.

Use the **aaa-server** command to configure authentication servers.

Examples

The following example shows how to configure an IMAP4S e-mail proxy to use the set of authentication servers named “IMAP4SSVRS”:

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# authentication-server-group IMAP4SSVRS
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.

authentication-server-group (tunnel-group general-attributes)

To specify the AAA server group to use for user authentication for a tunnel group, use the **authentication-server-group** command in tunnel-group general-attributes configuration mode. To return this attribute to the default, use the **no** form of this command.

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]
authentication-server-group [(*interface_name*)] *server_group*

Syntax Description

interface_name	(Optional) Specifies the interface at which the IPsec tunnel terminates.
LOCAL	(Optional) Requires authentication with the local user database if all of the servers in the server group have been deactivated due to communication failures.
server_group	Identifies the previously configured authentication server or group of servers.

Command Default

The default setting for the server-group in this command is **LOCAL**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
8.0(2)	This command was enhanced to allow per-interface authentication for IPsec connections.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Use the **aaa-server** command to configure authentication servers and the **aaa-server-host** command to add servers to a previously configured AAA server group.

Examples

The following example entered in config-general configuration mode, configures an authentication server group named aaa-server456 for an IPsec remote access tunnel group named remotegrp:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
```

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server	Creates a AAA server group and configures AAA server parameters that are group-specific and common to all group hosts.
aaa-server host	Adds servers to a previously configured AAA server group and configures host-specific AAA server parameters.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

authorization-required

To require users to authorize successfully prior to connecting, use the **authorization-required** command in various modes. To remove the attribute from the configuration, use the **no** form of this command.

authorization-required
no authorization-required

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
7.2(1)	Replaced the webvpn configuration mode with the imap4s, pop3s, and smtps configuration modes.
9.5(2)	This command was deprecated for the following modes: imap4s, pop3s, and smtps.

Examples

The following example requires authorization based on the complete DN for users connecting through a remote access tunnel group named remotegrp. The first command configures the tunnel-group type as ipsec_ra (IPsec remote access) for the remote group named remotegrp. The second command enters tunnel-group general-attributes configuration mode for the specified tunnel group, and the last command specifies that authorization is required for the named tunnel group.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-required
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
authorization-dn-attributes	Specifies the primary and secondary subject DN fields to use as the username for authorization.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

authorization-server-group (imap4s, pop3s, smtps) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify the set of authorization servers to use for a tunnel group for all remote access VPNs, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command.

authorization-server-group *group_tag*
no authorization-server-group

Syntax Description

group_tag	Identifies the previously configured authorization server or group of servers. Use the **aaa-server** command to configure authorization servers.

Command Default

No authorization servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
9.5(2)	This command was deprecated.

Usage Guidelines

The ASA uses authorization to verify the level of access to network resources that users are permitted. Use the server configurations for authorization that you used with the **aaa-server** command.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group general-attributes mode.

When VPN authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example shows how to configure POP3S e-mail proxy to use the set of authorization servers named “POP3Spermit”:

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)# authorization-server-group POP3Spermit
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

authorization-server-group (tunnel-group general-attributes)

To specify the set of authorization servers to use for a tunnel group for all remote access VPNs, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command.

authorization-server-group [(*if_name*)] *group_tag*
no authorization-server-group

Syntax Description

group_tag	Identifies the previously configured authorization server or group of servers. Use the **aaa-server** command to configure authorization servers.
(*if_name*)	(Optional) The name of the interface on which the tunnel terminates. You must include the parentheses.

Command Default

No authorization servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.

Usage Guidelines

The ASA uses authorization to verify the level of access to network resources that users are permitted. Use the server configurations for authorization that you used with the aaa-server command.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group general-attributes mode.

When VPN authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example entered in tunnel-general configuration mode, configures an authorization server group named “aaa-server78” for an IPsec remote-access tunnel group named “remotegrp”:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

authorize-only

To enable authorize-only mode for a RADIUS AAA server group, use the **authorize-only** command in aaa-server group configuration mode. To disable authorize-only mode, use the **no** form of this command.

authorize-only
no authorize-only

Syntax Description

This command has no arguments or keywords.

Command Default

Authorize-only mode is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to configure a RADIUS server group in authorize-only mode for ISE Change of Authorization (CoA). If you use authorize-only mode, any RADIUS common password configured for a RADIUS host are ignored.

The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is no longer required to apply access control lists (ACLs) for each VPN session established with the ASA.

When an end user requests a VPN connection, the ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network. An accounting start message is sent to the ISE to register the session. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA. The ISE sends a policy update to the ASA via a CoA "policy push." This identifies a new user ACL that provides increased network access privileges. Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates.

Examples

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE. Include the **authorize-only** command in the server group configuration, because the server group will not be used for authentication.

```
ciscoasa(config)# aaa-server ise protocol radius
```

```
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Related Commands

Command	Description
dynamic-authorization	Enables dynamic authorization for the RADIUS server group.
interim-accounting-update	Enables the generation of RADIUS interim-accounting-update messages.
without-csd	Switches off hostscan processing for connections that are made to a specific tunnel-group.

auth-prompt

To specify or change the AAA challenge text for through-the-ASA user sessions, use the **auth-prompt** command in global configuration mode. To remove the authentication challenge text, use the **no** form of this command.

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*
no auth-prompt prompt [**prompt** | **accept** | **reject**]

Syntax Description

accept	If a user authentication via Telnet is accepted, displays the prompt string.
prompt	The AAA challenge prompt string follows this keyword.
reject	If a user authentication via Telnet is rejected, displays the prompt string.
string	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters, spaces, and punctuation characters are permitted. Entering a question mark or pressing the Enter key ends the string. (The question mark appears in the string.)

Command Default

If you do not specify an authentication prompt:

- FTP users see FTP authentication .
- HTTP users see HTTP Authentication.
- Telnet users see no challenge text.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	Minor semantic changes.

Usage Guidelines

The auth-prompt command lets you specify the AAA challenge text for HTTP, FTP, and Telnet access through the ASA when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users see when logging in.

If user authentication occurs from Telnet, you can use the accept and reject options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the ASA displays the auth-prompt accept text, if specified, to the user; otherwise, it displays the reject text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The accept and reject text do not appear.

Note Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example sets the authentication prompt to the string "Please enter your username and password.":

```
ciscoasa(config)# auth
-prompt prompt Please enter your username and password
```

After this string is added to the configuration, users see the following:

```
Please enter your username and password
User Name:
Password:
```

For Telnet users, you can also provide separate messages to display when the ASA accepts or rejects the authentication attempt; for example:

```
ciscoasa(config)# auth-prompt reject Authentication failed. Try again.
ciscoasa(config)# auth-prompt accept Authentication succeeded.
```

The following example sets the authentication prompt for a successful authentication to the string, "You're OK."

```
ciscoasa(config)# auth-prompt accept You're OK.
```

After successfully authenticating, the user sees the following message:

```
You're OK.
```

Related Commands

Command	Description
clear configure auth-prompt	Removes the previously specified authentication prompt challenge text and reverts to the default value, if any.
show running-config auth-prompt	Displays the current authentication prompt challenge text.

auto-signon

To configure the ASA to automatically pass user login credentials for clientless SSL VPN connections on to internal servers, use the **auto-signon** command in any of three modes: webvpn configuration, webvpn group configuration, or webvpn username configuration mode. To disable auto-signon to a particular server, use the **no** form of this command with the original **ip**, **uri**, and **auth-type** arguments. To disable auto-signon to all servers, use the **no** form of this command without arguments.

auto-signon allow { **ip** *ip-address ip-mask* | **uri** *resource-mask* } **auth-type** { **basic** | **ftp** | **ntlm** | **all** }
no auto-signon [**allow** { **ip** *ip-address ip-mask* | **uri** *resource-mask* } **auth-type** { **basic** | **ftp** | **ntlm** | **all** }]

Syntax Description

all	Specifies both the NTLM and HTTP Basic authentication methods.
allow	Enables authentication to a particular server.
auth-type	Enables selection of an authentication method.
basic	Specifies the HTTP Basic authentication method.
ftp	Ftp and cifs authentication type.
ip	Specifies that an IP address and mask identifies the servers to be authenticated to.
ip-address	In conjunction with *ip-mask* , identifies the IP address range of the servers to be authenticated to.
ip-mask	In conjunction with *ip-address* , identifies the IP address range of the servers to be authenticated to.
ntlm	Specifies the NTLMv1 authentication method.
resource-mask	Identifies the URI mask of the servers to be authenticated to.
uri	Specifies that a URI mask identifies the servers to be authenticated to.

Command Default

By default, this feature is disabled for all servers.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration (global)	• Yes	—	• Yes	—	—

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn group policy configuration	• Yes	—	• Yes	—	—
Webvpn username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
8.0(1)	NTLMv2 support was added. The **ntlm** keyword includes both NTLMv1 and NTLMv2.

Usage Guidelines

The **auto-signon** command is a single sign-on method for clientless SSL VPN users. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, HTTP Basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).

You can use the auto-signon feature in three modes: webvpn configuration group-policy, webvpn configuration, or webvpn username configuration mode. The typical precedence behavior applies, where username supersedes group, and group supersedes global. The mode you choose depends on the desired scope of authentication:

Mode	Scope
Webvpn configuration	All WebVPN users globally
Webvpn group configuration	A subset of WebVPN users defined by a group policy
Webvpn username configuration	An individual WebVPN user

Examples

The following example configures auto-signon for all clientless users, using NTLM authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow ip 10.1.1.0
 255.255.255.0
 auth-type ntlm
```

The following example configures auto-signon for all clientless users, using HTTP Basic authentication, to servers defined by the URI mask https://*.example.com/*:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
The following example configures auto-signon for clientless users ExamplePolicy group policy,
 using either HTTP Basic or NTLM authentication, to servers defined by the URI mask
https://*.example.com/*:
```

```
ciscoasa(config)# group-policy ExamplePolicy attributes

ciscoasa(config-group-policy)# webvpn

ciscoasa(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

The following example configures auto-signon for a user named Anyuser, using HTTP Basic authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# auto-signon allow ip 10.1.1.0
 255.255.255.0
 auth-type basic
```

Related Commands

Command	Description
show running-config webvpn auto-signon	Displays auto-signon assignments of the running configuration.

auto-summary

To enable the automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable route summarization, use the **no** form of this command.

auto-summary
no auto-summary

Syntax Description

This command has no arguments or keywords.

Command Default

Route summarization is enabled for RIP Version 1, RIP Version 2, and EIGRP.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	Support for EIGRP was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

RIP Version 1 always uses automatic summarization. You cannot disable automatic summarization for RIP Version 1.

If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised.

EIGRP summary routes are given an administrative distance value of 5. You cannot configure this value.

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables RIP route summarization:

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
ciscoasa(config-router)# no auto-summary
```

The following example disables automatic EIGRP route summarization:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# no auto-summary
```

Related Commands

Command	Description
clear configure router	Clears all **router** commands and router configuration mode commands from the running configuration.
router eigrp	Enables the EIGRP routing process and enters EIGRP router configuration mode.
router rip	Enables the RIP routing process and enters RIP router configuration mode.
show running-config router	Displays the **router** commands and router configuration mode commands in the running configuration.

auto-update device-id

To configure the ASA device ID for use with an Auto Update Server, use the **auto-update device-id** command in global configuration mode. To remove the device ID, use the **no** form of this command.

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** | [*if_name*] | **mac-address** [*if_name*] | **string** *text*]
no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** | [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

Syntax Description

hardware-serial	Uses the hardware serial number of the ASA to uniquely identify the device.
hostname	Uses the hostname of the ASA to uniquely identify the device.
ipaddress [*if_name*]	Uses the IP address of the ASA to uniquely identify the ASA. By default, the ASA uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the *if_name* option.
mac-address [*if_name*]	Uses the MAC address of the ASA to uniquely identify the ASA. By default, the ASA uses the MAC address of the interface used to communicate with the Auto Update Server. If you want to use a different MAC address, specify the *if_name* option.
string *text*	Specifies the text string to uniquely identify the device to the Auto Update Server.

Command Default

The default ID is the hostname.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example sets the device ID to the serial number:

```
ciscoasa(config)# auto-update device-id hardware-serial
```

Related Commands

auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.

auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-at

To schedule a specific time for the ASA to poll the Auto Update Server, use the **auto-update poll-at** command in global configuration mode. To remove all specified scheduling times for the ASA to poll the Auto Update Server, use the **no** form of this command.

auto-update poll-at *days-of-the-week time* [**randomize** *minutes* [*retry_count* [*retry_period*]]]
no auto-update poll-at *days-of-the-week time* [**randomize** *minutes* [*retry_count* [*retry_period*]]]

Syntax Description

days-of-the-week	Any single day or combination of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday. Other possible values are daily (Monday through Sunday), weekdays (Monday through Friday) and weekend (Saturday and Sunday).
randomize >*minutes*	Specifies the period to randomize the poll time following the specified start time. from from 1 to 1439 minutes.
>*retry_count*	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
>*retry_period*	Specifies how long to wait between connection attempts. The default is 5 minutes. The range is from 1 and 35791 minutes.
>*time*	Specifies the time in the format HH:MM at which to start the poll. For example, 8:00 is 8:00 AM and 20:00 is 8:00 PM.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **auto-update poll-at** command specifies a time at which to poll for updates. If you enable the **randomize** option, the polling occurs at a random time within the range of the first >*time* option and the specified number of minutes. The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

In the following example, the ASA polls the Auto Update Server every Friday and Saturday night at a random time between 10:00 p.m. and 11:00 p.m. If the ASA is unable to contact the server, it tries two more times every 10 minutes.

```
ciscoasa(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
ciscoasa(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the ASA.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-period

To configure how often the ASA checks for updates from an Auto Update Server, use the **auto-update poll-period** command in global configuration mode. To reset the parameters to the defaults, use the **no** form of this command.

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]
no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

Syntax Description

poll_period	Specifies how often, in minutes, to poll an Auto Update Server, between 1 and 35791. The default is 720 minutes (12 hours).
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait, in minutes, between connection attempts, between 1 and 35791. The default is 5 minutes.

Command Default

The default poll period is 720 minutes (12 hours).

The default number of times to try reconnecting to the Auto Update Server if the first attempt fails is 0.

The default period to wait between connection attempts is 5 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

The following example sets the poll period to 360 minutes, the retries to 1, and the retry period to 3 minutes:

```
ciscoasa(config)# auto-update poll-period 360 1 3
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update server

To identify the Auto Update Server, use the **auto-update server** command in global configuration mode. To remove the server, use the **no** form of this command.

auto-update server *url* [**source** *interface*] { **verify-certificate** | **no-verification** }
no auto-update server *url* [**source** *interface*] { **verify-certificate** | **no-verification** }

Syntax Description

no-verification	Does not verify the Auto Update Server certificate.
source *interface*	Specifies which interface to use when sending requests to the Auto Update Server. If you specify the same interface specified by the **management-access** command, the Auto Update requests travel over the same IPsec VPN tunnel used for management access.
url	Specifies the location of the Auto Update Server using the following syntax: **https:**[[*user:password@location* [*:port*]] */pathname*
verify-certificate	For HTTPS, verifies the certificate returned by the Auto Update Server. This setting is the default.

Command Default

9.1 and earlier: Certificate verification is disabled.

9.2(1) and later: The **verify-certificate** option is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The command was modified to add support for multiple servers.
9.2(1)	The Auto Update server certificate verification is now enabled by default. The **no-verification** keyword was added.

Usage Guidelines

The ASA periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

You can configure multiple servers to work with auto-update. When checking for updates, a connection is made to the first server, but if that fails, then the next server is contacted. This process continues until all the

servers have been tried. If all of them fail to connect, then a retry starting with the first server is attempted if the auto-update poll period has been configured to retry the connection.

For auto-update functionality to work correctly, you must use the **boot system configuration** command and ensure that it specifies a valid boot image. In addition, you must use the **asdm image** command with auto-update to update the ASDM software image.

If the interface specified in the **source** *interface* argument is the same interface specified with the **management-access** command, requests to the Auto Update Server are sent over the VPN tunnel.

9.2(1) and later: The Auto Update server certificate verification is now enabled by default; for new configurations, you must explicitly disable certificate verification. If you are upgrading from an earlier release, and you did not enable certificate verification, then certificate verification is not enabled, and you see the following warning:

```
WARNING: The certificate provided by the auto-update servers will not be verified. In order
 to verify this certificate please use the verify-certificate option.
```

The configuration will be migrated to explicitly configure no verification:

auto-update server no-verification

Examples

The following example sets the Auto Update Server URL and specifies the interface as outside:

```
ciscoasa(config)# auto-update server http://10.1.1.1:1741/ source outside verify-certificate
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the ASA.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update timeout

To set a timeout period in which to contact the Auto Update Server, use the **auto-update timeout** command in global configuration mode. To remove the timeout, use the **no** form of this command.

auto-update timeout [*period*]
no auto-update timeout [*period*]

Syntax Description

period Specifies the timeout period in minutes between 1 and 35791. The default is 0, which means there is no timeout. You cannot set the timeout to 0; use the **no** form of the command to reset it to 0.

Command Default

The default timeout is 0, which sets the ASA to never time out.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

A timeout condition is reported with syslog message 201008.

If the Auto Update Server has not been contacted for the timeout period, the ASA stops all traffic going through it. Set a timeout to ensure that the ASA has the most recent image and configuration.

Examples

The following example sets the timeout to 24 hours:

```
ciscoasa(config)# auto-update timeout 1440
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

avc

To enable Application Visibility Control (AVC) and download the Vulnerability Database (VDB), use the **avc** command in global configuration mode. To disable AVC and remove all AVC network-service objects, groups, and other data structures, use the **no** form of the command.

When downloading the VDB manually, the command is for Privileged EXEC mode.

avc
no avc
avc download vdb

Syntax Description

download vdb	Manually download the Vulnerability Database (VDB). Use this command if a VDB automatic download fails.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration Privileged EXEC mode for download	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.24(1)	This command was added.

Usage Guidelines

You must enable Application Visibility and Control (AVC) to download the Vulnerability Database (VDB) and create the network-service objects and groups that you can use in access control rules or other policies that use extended ACLs. If you subsequently disable AVC, all downloaded and extracted files, and the AVC network-service objects and groups, are deleted.

When you view the running configuration, the **avc** command shows the version of the VDB currently installed on the **vdb-version** parameter. A 0 indicates the VDB is not installed. This parameter is not configurable.

VDB Download Guidelines

- You must configure DNS and DNS lookup on an interface through which support.sourcefire.com can be contacted, so that the Vulnerability Database (VDB) can be downloaded. A route to that server must also be available.

- In a high-availability group, the VDB download must be possible over the management interface, because the standby unit cannot pass traffic over data interfaces. The standby unit downloads VDB updates itself.
- In a cluster, each unit downloads the VDB separately.
- In multiple context mode, only one user context downloads the VDB, and shares it with contexts where AVC is enabled.
- VDB download uses HTTPS, so it requires that a trusted CA certificate from third-party Certificate Authority is installed on the device, to ensure a secure connection.
- When downloading a VDB update, after the download is complete, the system clears the existing AVC network-service objects and groups, and other AVC files, and rebuilds them. Your AVC-based policies will stop working until the update is complete.
- The VDB download file is about 70 MB. An extracted VDB requires at least 450 MB of disk space. Ensure there is adequate free space on the device to download and extract the VDB.

.

Example

The following example enables AVC and starts the VDB download. After giving the download time to complete, use the **show avc status** command to verify when the download is complete and the AVC feature is ENABLED and READY to be used.

```
ciscoasa(config)# avc
...
ciscoasa(config)# show avc status
AVC (Application Visibility and Control): ENABLED : READY
VDB (containing app definition) download status: UP-TO-DATE
VDB version: current 397, last 0
VDB last update at 15:29:57 UTC Apr 29 2025; last update attempt at 15:27:36 UTC Apr 29
2025; next update at 15:30:55 UTC May 6 2025.
VDB download link:
https://50.19.123.95/auto-update/auto-dl.cgi/Download/files/Cisco_VDB_Fingerprint_Database-4.5.0-399.sh.REL.tar
```

The following example manually downloads the VDB. This action is necessary only if a VDB download fails.

```
ciscoasa# avc download vdb
```

Related Commands

show avc	Shows the status and associated information about the AVC system.



b

- backup, on page 391
- backup interface, on page 395
- backup-package auto, on page 397
- backup-package location, on page 398
- backup-servers, on page 400
- banner (global), on page 402
- banner (group-policy), on page 405
- base-url, on page 407
- basic-mapping-rule, on page 409
- basic-security, on page 411
- bfd echo, on page 413
- bfd interval, on page 415
- bfd map, on page 417
- bfd slow-timers, on page 419
- bfd-template, on page 421
- bgp aggregate-timer, on page 423
- bgp always-compare-med, on page 425
- bgp asnotation dot, on page 427
- bgp bestpath compare-routerid, on page 430
- bgp bestpath med missing-as-worst, on page 431
- bgp-community new-format, on page 432
- bgp default local-preference, on page 434
- bgp deterministic-med, on page 435
- bgp enforce-first-as, on page 438
- bgp fast-external-fallover, on page 440
- bgp graceful-restart, on page 441
- bgp inject-map, on page 443
- bgp log-neighbor-changes, on page 445
- bgp maxas-limit, on page 447
- bgp nexthop, on page 448
- bgp redistribute-internal, on page 451
- bgp router-id, on page 453
- bgp scan-time, on page 454

- bgp suppress-inactive, on page 456
- bgp transport, on page 458
- blocks, on page 459
- boot, on page 461
- border style, on page 465
- breakout, on page 467
- bridge-group, on page 469
- browse-networks, on page 471

backup

To back up an ASA configuration, certificates, keys, and images, use the **backup** command in privileged EXEC mode.

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

Syntax Description

/noconfirm	Specifies not to prompt for the **location** and **cert-passphrase** parameters. Allows you to bypass warning and error messages to continue the backup.
context *ctx-name*	In multiple context mode from the system execution space, enter the **context** keyword to backup the specified context. Each context must be backed up individually; that is, re-enter the **backup** command for each file.
interface *name*	(Optional) Specifies the interface name through which the backup will be copied. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
location *path*	The backup **location** can be a local disk or a remote URL. If you do not provide a location, the following default names are used: • Single mode—disk0:*hostname* .backup.*timestamp* .tar.gz • Multiple mode—disk0:*hostname* .context-*ctx-name* .backup.*timestamp* .tar.gz
passphrase *value*	During the backup of VPN certificates and preshared keys, a secret key identified by the **cert-passphrase** keyword is required to encode the certificates. You must provide a passphrase to be used for encoding and decoding the certificates in PKCS12 format. The backup only includes RSA key pairs tied to the certificates and excludes any standalone certificates.

Command Default

If you do not provide a location, the following default names are used:

- Single mode—disk0:*hostname* .backup.*timestamp* .tar.gz
- Multiple mode—disk0:*hostname* .context-*ctx-name* .backup.*timestamp* .tar.gz

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added.
9.5(1)	The **interface** *name* argument was added.

Usage Guidelines

See the following guidelines:

- You should have at least 300 MB of disk space available at the backup location before you start a backup.
- If you make any configuration changes during or after a backup, those changes will not be included in the backup. If you change a configuration after making the backup, then perform a restore, this configuration change will be overwritten. As a result, the ASA might behave differently.
- You can start only one backup at a time.
- You can only restore a configuration to the same ASA version as when you performed the original backup. You cannot use the restore tool to migrate a configuration from one ASA version to another. If a configuration migration is required, the ASA automatically upgrades the resident startup configuration when it loads the new ASA OS.
- If you use clustering, you can only back up the startup-configuration, running-configuration, and identity certificates. You must create and restore a backup separately for each unit.
- If you use failover, you must create and restore a backup separately for the active and standby units.
- If you set a master passphrase for the ASA, then you need that master passphrase to restore the backup configuration that you create with this procedure. If you do not know the master passphrase for the ASA, see the CLI configuration guide to learn how to reset it before continuing with the backup.
- If you import PKCS12 data (with the **crypto ca trustpoint** command) and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint. Because of this limitation, if you specify a different name for the trustpoint and its key pair after you have restored an ASDM configuration, the startup configuration will be the same as the original configuration, but the running configuration will include a different key pair name. This means that if you use different names for the key pair and trustpoint, you cannot restore the original configuration. To work around this issue, make sure that you use the same name for the trustpoint and its key pair.
- If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table. Note that if you have a default route through a management-only interface, all **backup** traffic will match that route and never check the data routing table. In this scenario, always specify the interface if you need to back up through a data interface.
- You cannot back up using the CLI and restore using ASDM, or vice versa.
- When backup location command is issued, ensure to use double slash '//' for the directory path. For example,

```
ciscoasa# backup location disk0://sample-backup
```

- Each backup file includes the following content:
  - Running-configuration
  - Startup-configuration

- All security images

Cisco Secure Desktop and Host Scan images

Cisco Secure Desktop and Host Scan settings

AnyConnect (SVC) client images and profiles

AnyConnect (SVC) customizations and transforms

- Identity certificates (includes RSA key pairs tied to identity certificates; excludes standalone keys)
- VPN pre-shared keys
- SSL VPN configurations
- Application Profile Custom Framework (APCF)
- Bookmarks
- Customizations
- Dynamic Access Policy (DAP)
- Plug-ins
- Pre-fill scripts for connection profiles
- Proxy Auto-config
- Translation table
- Web content
- Version information

Examples

The following example shows how to create a backup:

```
ciscoasa# backup location disk0://sample-backup
Backup location [disk0://sample-backup]?
Begin backup...
Backing up [ASA version] ... Done!
Backing up [Running Config] ... Done!
Backing up [Startup Config]  ... Done!
Enter a passphrase to encrypt identity certificates. The default is cisco. You will be
required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] ... Done!
IMPORTANT: This device uses master passphrase encryption. If this backup file is used to
restore to a device with a different master passphrase, you will need to provide the current
 master passphrase during restore.
Backing up [VPN Pre-shared keys] ... Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] ... Done!
Backing up [SSL VPN Configurations: Bookmarks]... Done!
Backing up [SSL VPN Configurations: Customization] ... Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] ... Done!
Backing up [SSL VPN Configurations: Plug-in] ... Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] ... Done!
Backing up [SSL VPN Configurations: Proxy auto-config] ... Done!
Backing up [SSL VPN Configurations: Translation table] ... Done!
Backing up [SSL VPN Configurations: Web Content] ... Done!
```

```
Backing up [Anyconnect(SVC) client images and profiles] ... Done!
Backing up [Anyconnect(SVC) customizations and transforms] ... Done!
Backing up [Cisco Secure Desktop and Host Scan images] ... Done!
Backing up [UC-IME tickets] ... Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

Related Commands

Command	Description
restore	Restores an ASA configuration, keys, certificates, and images from a backup file.

backup interface

For models with a built-in switch, such as the ASA 5505, use the **backup interface** command in interface configuration mode to identify a VLAN interface as a backup interface, for example, to an ISP. To restore normal operation, use the **no** form of this command.

backup interface vlan *number*
backup interface vlan *number*

Syntax Description

vlan *number*	Specifies the VLAN ID of the backup interface.

Command Default

By default, the **backup interface** command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
7.2(2)	The Security Plus license no longer limits the number of VLAN interfaces to 3 for normal traffic, 1 for a backup interface, and 1 for failover; you can now configure up to 20 interfaces without any other limitations. Therefore ,the **backup interface** command is not required to enable more than 3 interfaces.

Usage Guidelines

This command can be entered in the interface configuration mode for a VLAN interface only. This command blocks all through traffic on the identified backup interface unless the default route through the primary interface goes down.

When you configure Easy VPN with the **backup interface** command, if the backup interface becomes the primary, then the ASA moves the VPN rules to the new primary interface. See the **show interface** command to view the state of the backup interface.

Be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. See the **dhcp client route distance** command to override the administrative distance for default routes acquired from a DHCP server. To configure dual ISP support, see the **sla monitor** and **track rtr** commands for more information.

You cannot configure a backup interface when the **management-only** command is already configured on the interface.

Examples

The following example configures four VLAN interfaces. The backup-isp interface only allows through traffic when the primary interface is down. The **route** commands create default routes for the primary and backup interfaces, with the backup route at a lower administrative distance.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# backup interface vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# route outside 0 0 10.1.1.2 1
ciscoasa(config)# route backup-isp 0 0 10.1.2.2 2
```

Related Commands

Command	Description
forward interface	Restricts an interface from initiating traffic to another interface.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
dhcp client route distance	Overrides the administrative distance for default routes acquired from a DHCP server.
sla monitor	Creates an SLA monitoring operation for static route tracking.
track rtr	Tracks the state of an SLA monitoring operation.

backup-package auto

To configure automatic backup and restore operations on a Cisco ISA 3000, use the **backup-package auto** command in privileged EXEC mode. To disable automatic backup or restore, use the **no** form of this command.

backup-package { **backup** | **restore** } **auto**
no backup-package { **backup** | **restore** } **auto**

Syntax Description

backup	Indicates that you are configuring automatic backup.
restore	Indicates that you are configuring automatic restore.

Command Default

The default backup and restore modes are manual.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

The backup and restore modes are independent and you can configure them separately.

Use the **backup-package location** command to specify the backup and restore configuration parameters for automatic backup and restore operations.

Examples

The following example shows the use of the **backup-package** command to set automatic back-up:

```
ciscoasa# backup-package backup auto
```

Related Commands

Command	Description
show backup-package summary	Displays a summary of back-up and restore package parameters.

backup-package location

To configure the backup and restore locations to be used in subsequent backup and restore operations on a Cisco ISA 3000, use the **backup-package location** command in privileged EXEC mode. To reset the backup or restore location to the default value, use the **no** form of this command.

backup-package { **backup** | **restore** } [**interface** *name*] **location disk** *n* **:** [**passphrase** *string*
no backup-package { **backup restore** } **location**

Syntax Description

backup	Indicates that you are defining backup parameters.
interface *name*	(Optional) The name of the interface to be used for backup or restore communications.
location disk*n***:**	The storage-media location where the back-up package information is stored.
passphrase *string*	(Optional) The passphrase to be used for encrypting the backup information, or retrieving the backed-up information.
restore	Indicates that you are defining restore parameters.

Command Default

The default **location** is **disk3:**, which contains an SD card.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

The backup and restore operations are independent and can be configured separately.

Generally, configuring **backup-package** information is a one-time operation to let you subsequently manually back up and restore the device configuration without having to provide additional parameters.

Examples

The following example shows the use of the **backup-package location** command to set the backup parameters, with “cisco” as the encryption passphrase:

```
ciscoasa# backup-package backup location disk3: passphrase cisco
```

Related Commands

Command	Description
show backup-package status	Displays package information for either backup or restore.
show backup-package summary	Displays a summary of backup and restore package parameters.

backup-servers

To configure backup servers, use the **backup-servers** command in group-policy configuration mode. To remove a backup server, use the **no** form of this command.

backup-servers { *server1 server2....server10* | **clear-client-config | keep-client-config** }
no backup-servers { *server1 server2....server10* | **clear-client-config | keep-client-config** }

Syntax Description

clear-client-config	Specifies that the client uses no backup servers. The ASA pushes a null server list.
keep-client-config	Specifies that the ASA sends no backup server information to the client. The client uses its own backup server list, if configured.
server1 server 2 .... server10	Provides a space delimited, priority-ordered list of servers for the VPN client to use when the primary ASA is unavailable. Identifies servers by IP address or hostname. The list can be 500 characters long, but can contain only 10 entries.

Command Default

Backup servers do not exist until you configure them, either on the client or on the primary ASA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To remove the backup-servers attribute from the running configuration, use the **no** form of this command without arguments. This enables inheritance of a value for backup servers from another group policy.

IPsec backup servers let a VPN client connect to the central site when the primary ASA is unavailable. When you configure backup servers, the ASA pushes the server list to the client as the IPsec tunnel is established.

Configure backup servers either on the client or on the primary ASA. If you configure backup servers on the ASA, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.

Note If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. In addition, if you use hostnames and the DNS server is unavailable, significant delays can occur.

Examples

The following example shows how to configure backup servers with IP addresses 10.10.10.1 and 192.168.10.14, for the group policy named “FirstGroup”:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 backup-servers 10.10.10.1 192.168.10.14
```

banner (global)

To configure the ASDM, session, login, or message-of-the-day banner, use the banner command in global configuration mode. To remove the banner for a given keyword, use the **no** form of this command with a keyword.

banner { **asdm** | **exec** | **login** | **motd** *text* }
no banner { **asdm** | **exec** | **login** | **motd** }

Syntax Description

asdm	Configures the system to display a banner after you successfully log in to ASDM. The user is prompted to either continue to complete login, or to disconnect. This option lets you require users to accept the terms of a written policy before connecting.
exec	Configures the system to display a banner before displaying the enable prompt.
login	Configures the system to display a banner before the password login prompt when accessing the ASA using Telnet or a serial console.
motd	Configures the system to display a message-of-the-day banner when you first connect. The banner also shows information about the failover state and the last failover time of the unit you are logging into. This information is useful if you are performing actions at the CLI, such as troubleshooting, and a failover occurs between sessions.
text	Line of message text to display. The maximum length is 235 characters or 31 words, whichever limitation is reached first. Spaces in the text are preserved. However, you cannot enter tabs through the CLI. The tokens $(domain) and $(hostname) are replaced with the hostname and domain name of the ASA. When you enter a $(system) token in a context configuration, the context uses the configured in the system configuration.

Command Default

The default is no banner.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(4)/8.0(3)	The **asdm** keyword was added.
9.0(1)	The **banner login** command now supports serial console connections.

Release	Modification
9.22(3)/9.24(1)	The **motd** option now includes the failover state and the last failover time.

Usage Guidelines

The **banner** command configures a banner to display for the keyword specified.

Multiple lines in a banner are handled by entering a new **banner** command for each line that you want to add. Each line is then appended to the end of the existing banner.

When accessing the ASA through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs. Only the **exec** and **motd** s support access to the ASA through SSH. The login banner does not support SSHv1 clients or SSH clients that do not pass the username as part of the initial connection.

To replace a banner, use the **no banner** *keyword* command before reentering the **banner** *keyword text* command.

The **no banner** command does not selectively delete text strings, so any *text* that you enter at the end of the **no banner** *keyword* command is ignored.

Examples

The following example shows how to configure the **asdm**, **exec**, **login**, and **motd** banners:

```
ciscoasa(config)#  banner asdm You successfully logged in to ASDM
ciscoasa(config)#  banner motd Think on These Things
ciscoasa(config)#  banner exec Enter your password carefully
ciscoasa(config)#  banner login Enter your password to log in
ciscoasa(config)# show running-config banner
asdm:
You successfully logged in to ASDM
exec:
Enter your password carefully
login:
Enter your password to log in
motd:
Think on These Things
```

The following example shows how to add a second line to the **motd** banner:

```
ciscoasa(config)# banner motd and Enjoy Today
ciscoasa(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

The following example shows the information displayed on login to the active unit in a failover pair when the **banner motd** command is configured.

```
Last login: Fri Jun 27 06:15:29 UTC 2025 from 10.16.0.101 on pts/0
Successful login attempts for user 'dwinchester' : 1
Last login: Fri Jun 27 06:16:21 2025 from 10.16.0.101

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             05:40:48 UTC Jun 27 2025

====Configuration State===
```

```
 Sync Done
====Communication State===
 Mac set

Last Failover at: 05:40:30 UTC Jun 27 2025
"This is the active device"
User dwinchester logged in to active
Logins over the last 1 days: 3.  Last login: 06:15:29 UTC Jun 27 2025 from console
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
active>
```

Related Commands

Command	Description
clear configure	Removes all banners.
show running-config	Displays all banners.

banner (group-policy)

To display a banner or welcome text on remote clients when they connect, use the **banner** command in group-policy configuration mode. To delete a banner, use the **no** form of this command.

banner { **value** *_string* | **none** }
no banner



Note If you configure multiple banners under a VPN group policy, and you delete any one of the banners, all banners are deleted.

Syntax Description

none	Sets a banner with a null value, thereby disallowing a banner. Prevents inheriting a banner from a default or specified group policy.
value *banner_string*	Constitutes the banner text. Maximum string size is 4000 characters for post-login banners. Use the "\n" sequence to insert a carriage return. The recommended configuration is around 80 to 100 characters per line since clients and browser wrap it up around that limit for display per line.

Command Default

There is no default banner.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(1)	Increased the post-login banner length value to 4000.

Usage Guidelines

The banner is locally configured on the ASA, and the user must click either Accept or Disconnect to the post-login banner.



Note The behavior on older architectures, such as IKEv1 and Secure Client version 3.0, is supported without error.

To prevent inheriting a banner, use the **banner none** command.

The IPsec VPN client supports full HTML for the banner. However, the clientless portal and the Secure Client support partial HTML. To ensure the banner displays correctly to remote users, follow these guidelines:

- For IPsec client users, use the /n tag.
- For Secure Client, use the <BR> tag.
- For clientless users, use the <BR> tag.

Examples

The following example shows how to create a banner for the group policy named “FirstGroup”:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# banner
value Welcome to Cisco Systems
7.0.
```

base-url

(Optional) Configures the base URL of the Clientless VPN. This URL is used in SAML metadata, which is provided to third-party IdPs, so that IdPs can redirect endpoint users back to the ASA.

(Optional) From version 9.17.1, this command configures the base URL of the SAML service provider for VPN authentication. This URL is used in SAML metadata, which is provided to third-party IdPs, so that IdPs can redirect endpoint users back to the ASA.

To disable this feature, use the **no** form of this command

base-url { **value _ string** }
no base-url

Syntax Description

base-url	URL of the Clientless VPN

Command Default

None.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

- When base-url is configured, it is the base URL of AssertionConsumerService and SingleLogoutService, and is displayed in **show saml metadata**.
- When base-url is not configured, the base URL is created from the ASA's hostname and domain-name. For example, **https://ssl-vpn.cisco.com** is the base URL in **show saml metadata** when hostname is "ssl-vpn" and domain-name is "cisco.com".
- When neither base-url or hostname and domain-name are configured, **show saml metadata** displays an error.

Examples

The following example sets up a base-url:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp myIdp
ciscoasa(config-webvpn-saml-idp)# base url https://ClientlessVPN.com
```

Related Commands

Command	Description
signature	Enable or disable signature in SAML request. By default, the signature is disabled.
timeout	Configures the SAML IdP timeout.
trustpoint	Configures the trustpoint in saml-idp sub-mode.
url	Configures the SAML IdP URL.

basic-mapping-rule

To configure the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **basic-mapping-rule** command in MAP domain configuration mode. Use the **no** form of this command to delete the basic mapping rule.

basic-mapping-rule
no basic-mapping-rule

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The customer edge (CE) device uses the basic mapping rule to determine its dedicated IPv4 addressing or shared address and port set assignment. The CE device first translates the system's IPv4 address to an IPv4 address and port within the pool's prefix and port range (using NAT44), then MAP translates the new IPv4 address to an IPv6 address within the pool defined by the rule's IPv6 prefix. The packet is then ready to be transmitted over the service provider's IPv6-only network to a border relay (BR) device.

When you enter the **basic-mapping-rule** command, you enter MAP domain basic mapping rule configuration mode, where you can configure the IPv4, IPv6, and port properties of the rule.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
```

```
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

basic-security

To define an action when the Security (SEC) option occurs in a packet header with IP Options inspection, use the **basic-security** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

basic-security action { **allow** | **clear** }
no basic-security action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Security IP option.
clear	Remove the Security option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Security IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# basic-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

bfd echo

To enable BFD echo mode on the interface, use the bfd **echo** command in interface configuration mode. To disable BFD echo mode, use the **no** form of this command.

bfd echo
no bfd echo

Syntax Description

This command has not arguments or keywords.

Command Default

BFD echo mode is disabled by default for BFD IPv4 sessions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Echo mode is enabled by default, but not supported in BFD IPv6 sessions. Entering the **no bfd echo** command without any keywords turns off the sending of echo packets and signifies that the ASA is unwilling to forward echo packets received from BFD neighbor routers.

When echo mode is enabled, the minimum echo transmit interval and required minimum transmit interval values are taken from the **bfd interval milliseconds min_rx milliseconds** parameters, respectively.

Before using BFD echo mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the **no ip redirects** command to avoid high CPU utilization.

Examples

The following example associates a BFD template with a BFD map.

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd echo
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd interval	Configures the baseline BFD parameters on the interface.

Command	Description
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd interval

To configure the baseline BFD parameters on the interface, use the bfd command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*
no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Syntax Description

interval	Specifies the rate at which BFD control packets are sent to BFD peers. The range is 50 to 999 milliseconds.
min_rx	Specifies the rate at which BFD control packets are expected to be received from BFD peers. The range is 50 to 999 milliseconds.
multiplier	Specifies the rate at which BFD control packets must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The range is 3 to 50.
milliseconds	The value in milliseconds.
multiplier-value	The value of the multiplier.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example associates a BFD template with a BFD map.

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd map

To configure a BFD map that associates addresses with multi-hop templates, use the bfd map command in global configuration mode. To delete a BFD map, use the **no** form of this command.

bfd map { **ipv4** | **ipv6** } *destination/cdir source/cdir template-name*
no bfd map

Syntax Description

ipv4	Configures an IPv4 address.
ipv6	Configures an IPv6 address.
destination/cdir	The destination prefix/length.
source/cdir	The source prefix/length.
template-name	Name of the BFD template associated with the BFD map.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example associates a BFD template with a BFD map.

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 multihop-template1
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.

Command	Description
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd slow-timers

To configure the BFD slow timers value, use the bfd slow-timers command in global configuration mode.

bgp slow-timers [*milliseconds*]

Syntax Description

milliseconds	(Optional) The BFD slow timers value in milliseconds. The range is 1000 to 30,000. The default is 1000.

Command Default

The default value of the BFD slow timer is 1000 milliseconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example configures BFD slow timers for 14,000 milliseconds.

```
ciscoasa(config)# bfd slow-timers 14000
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.

Command	Description
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd-template

To configure the BFD template and enter BFD configuration mode, use the bfd-template command in global configuration mode. To disable a BFD template, use the **no** form of this command.

bfd-template [**single-hop** | **multi-hop**] *template-name*
no bfd-template [**single-hop** | **multi-hop**] *template-name*

Syntax Description

single-hop	Specifies a single-hop BFD template.
multi-hop	Specifies a multi-hop BFD template.
template-name	Name of the BFD template.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to create a BFD template and enter BFD configuration mode. You can also specify a set of BFD interval values in the template. BFD interval values specified as part of the BFD template are not specific to a single interface.

Examples

The following example configures a single-hop BFD template.

```
ciscoasa(config)# bfd single-hop node1
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

The following example configures multi-hop BFD template.

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bgp aggregate-timer

To set the interval at which BGP routes will be aggregated or to disable timer-based route aggregation, use the bgp aggregate-timer command in address family configuration mode. To restore the default value, use the no form of this command.

bgp aggregate-timer *seconds*
no bgp aggregate-timer

Syntax Description

seconds The interval (in seconds) at which the system will aggregate BGP routes.

Valid values are in the range from 6 to 60 or else 0 (zero).

The default value is 30.

A value of 0 (zero) disables timer-based aggregation and starts aggregation immediately.

Command Default

The default value of the bgp aggregate timer is 30 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration, Address-family IPv6 sub mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

Use this command to change the default interval at which BGP routes are aggregated.

In very large configurations, even if the aggregate-address summary-only command is configured, more specific routes are advertised and later withdrawn. To avoid this behavior, configure the bgp aggregate-timer to 0 (zero), and the system will immediately check for aggregate routes and suppress specific routes.

Examples

The following example configures BGP route aggregation at 20-second intervals:

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

The following example starts BGP route aggregation immediately:

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

Related Commands

Command	Description
address-family ipv4	Enters the address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes.
aggregate-address	Creates an aggregate entry in a Border Gateway Protocol (BGP) database.

bgp always-compare-med

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the bgp always-compare-med command in router configuration mode. To disallow the comparison, use the no form of this command.

bgp always-compare-med
no bgp always-compare-med

Syntax Description

This command has no arguments or keywords.

Command Default

ASA routing software does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the no form of this command is entered.

The MED is compared only if the autonomous system path for the compared routes is identical.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The MED, as stated in RFC 1771, is an optional non-transitive attribute that is a four octet non-negative integer. The value of this attribute may be used by the BGP best path selection process to discriminate among multiple exit points to a neighboring autonomous system.

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. During the best-path selection process, MED comparison is done only among paths from the same autonomous system. The bgp always-compare-med command is used to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

The bgp deterministic-med command can be configured to enforce deterministic comparison of the MED value between all paths received from within the same autonomous system.

Examples

In the following example, the local BGP routing process is configured to compare the MED from alternative paths, regardless of the autonomous system from which the paths are received:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp always-compare-med
```

Related Commands

Command	Description
bgp deterministic-med	Enforces the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system.

bgp asnotation dot

To change the default display and regular expression match format of Border Gateway Protocol (BGP) 4-byte autonomous system numbers from asplain (decimal values) to dot notation, use the bgp asnotation dot command in router configuration mode. To reset the default 4-byte autonomous system number display and regular expression match format to asplain, use the no form of this command.

bgp asnotation dot
no bgp asnotation dot

Syntax Description

This command has no arguments or keywords.

Command Default

BGP autonomous system numbers are displayed using asplain (decimal value) format in screen output, and the default format for matching 4-byte autonomous system numbers in regular expressions is asplain.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, A Border Gateway Protocol 4 (BGP-4).

Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, Textual Representation of Autonomous System (AS) Numbers, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal numbers).

Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular

expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default show command output to display 4-byte autonomous system numbers in the asdot format, use the bgp asnotation dot command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. Tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display show command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format.

To display 4-byte autonomous system numbers in show command output and to control matching for regular expressions in the asdot format, you must configure the bgp asnotation dot command. After enabling the bgp asnotation dot command, a hard reset must be initiated for all BGP sessions by entering the clearbgp * command.

Table 3: Default Asplain 4-byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65534-byte: 65536 to 4294967295	2-byte: 1 to 65534-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65534-byte: 1.0 to 65535.65535	2-byte: 1 to 65534-byte: 65536 to 4294967295

Table 4: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 655354-byte: 65536 to 4294967295	2-byte: 1 to 655354-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 655354-byte: 1.0 to 65535.65535	2-byte: 1 to 655354-byte: 1.0 to 65535.65535

Examples

The following output from the show bgp summary command shows the default asplain format of the 4-byte autonomous system numbers. Note the asplain format of the 4-byte autonomous system numbers, 65536 and 65550.

```
ciscoasa(config-router)# show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

 Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
 192.168.1.2     4        65536       7       7        1    0    0 00:03:04      0
 192.168.3.2     4        65550       4       4        1    0    0 00:00:15      0
```

The following configuration is performed to change the default output format to the asdot notation format:

```
ciscoasa# configure terminal
ciscoasa(config)# router bgp 65538
ciscoasa(config-router)# bgp asnotation dot
```

After the configuration is performed, the output is converted to asdot notation format as shown in the following output from the show bgp summary command. Note the asdot format of the 4-byte autonomous system numbers, 1.0 and 1.14 (these are the asdot conversions of the 65536 and 65550 autonomous system numbers).

```
ciscoasa(config-router)# show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13     0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24     0
```

After the bgp asnotation dot command is configured, the regular expression match format for 4-byte autonomous system paths is changed to asdot notation format. Although a 4-byte autonomous system number can be configured in a regular expression using either asplain format or asdot format, only 4-byte autonomous system numbers configured using the current default format are matched. In the first example, the show bgp regexp command is configured with a 4-byte autonomous system number in asplain format. The match fails because the default format is currently asdot format and there is no output. In the second example using asdot format, the match passes and the information about the 4-byte autonomous system path is shown using the asdot notation.

```
ciscoasa(config-router)# show bgp regexp ^65536$
ciscoasa(config-router)# show bgp regexp ^1\.0$
BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

Note The asdot notation uses a period, which is a special character in Cisco regular expressions. To remove the special meaning, use a backslash before the period.

Related Commands

Command	Description
show bgp summary	Displays the status of all Border Gateway Protocol (BGP) connections.
show bgp regexp	Displays routes matching the autonomous system path regular expression.

bgp bestpath compare-routerid

To configure a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path, use the bgp bestpath compare-routerid command in router configuration mode.

To return the BGP routing process to the default operation, use the no form of this command.

bgp bestpath compare-routerid
no bgp bestpath compare-routerid

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is disabled by default; BGP selects the route that was received first when two routes with identical attributes are received.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp bestpath compare-routerid command is used to configure a BGP routing process to use the router ID as the tie breaker for best path selection when two identical routes are received from two different peers (all the attributes are the same except for the router ID). When this command is enabled, the lowest router ID will be selected as the best path when all other attributes are equal.

Examples

In the following example, the BGP routing process is configured to compare and use the router ID as a tie breaker for best path selection when identical paths are received from different peers:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath compare-routerid
```

bgp bestpath med missing-as-worst

To configure a Border Gateway Protocol (BGP) routing process to assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute (making the path without a MED value the least desirable path), use the bgp bestpath med missing-as-worst command in router configuration mode. To return the router to the default behavior (assign a value of 0 to the missing MED), use the no form of this command.

bgp bestpath med missing-as-worst
no bgp bestpath med missing-as-worst
bgp bestpath med missing-as-worst

Syntax Description

This command has no arguments or keywords.

Command Default

ASA software assigns a value of 0 to routes that are missing the MED attribute, causing the route with the missing MED attribute to be considered the best path.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Examples

In the following example, the BGP router process is configured to consider a route with a missing MED attribute as having a value of infinity (4294967294), making this path the least desirable path:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath med missing-as-worst
```

bgp-community new-format

To configure BGP to display communities in the format AA:NN (autonomous system:community number/4-byte number), use the bgp-community new-format command in global configuration mode. To configure BGP to display communities as a 32-bit number, use the no form of this command.

bgp-community new-format
no bgp-community new-format

Syntax Description

This command has no arguments or keywords.

Command Default

BGP communities (also when entered in the AA:NN format) are displayed as a 32-bit numbers if this command is not enabled or if the no form is entered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp-community new-format command is used to configure the local router to display BGP communities in the AA:NN format to conform with RFC-1997.

This command only affects the format in which BGP communities are displayed; it does not affect the community or community exchange. However, expanded IP community lists that match locally configured regular expressions may need to be updated to match on the AA:NN format instead of the 32-bit number.

RFC 1997, BGP Communities Attribute, specifies that a BGP community is made up of two parts that are each 2 bytes long. The first part is the autonomous system number and the second part is a 2-byte number defined by the network operator.

Examples

In the following example, a router that uses the 32-bit number community format is upgraded to use the AA:NN format:

```
ciscoasa(config)# bgp-community new-format
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

The following sample output shows how BGP community numbers are displayed when the bgp-community new-format command is enabled:

```
ciscoasa(router)# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
Advertised to non peer-group peers:
10.0.33.35
35
10.0.33.35 from 10.0.33.35 (192.168.3.3)
Origin incomplete, metric 10, localpref 100, valid, external
Community: 1:1
Local
0.0.0.0 from 0.0.0.0 (10.0.33.34)
Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

bgp default local-preference

To change the default local preference value, use the bgp default local-preference command in router configuration mode. To return the local preference value to the default setting, use the no form of this command.

bgp default local-preference *number*
no bgp default local-preference *number*

Syntax Description

number	Local preference value from 0 to 4294967295.

Command Default

ASA software applies a local preference value of 100 if this command is not enabled or if the no form of this command is entered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The local preference attribute is a discretionary attribute that is used to apply the degree of preference to a route during the BGP best path selection process. This attribute is exchanged only between iBGP peers and is used to determine local policy. The route with the highest local preference is preferred.

Examples

In the following example, the local preference value is set to 200:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp default local-preference 200
```

bgp deterministic-med

To enforce the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system use the bgp deterministic-med command in router configuration mode. To disable the required MED comparison, use the no form of this command.

bgp deterministic-med
no bgp deterministic-med

Syntax Description

This command has no arguments or keywords.

Command Default

ASA software does not enforce the deterministic comparison of the MED variable between all paths received from the same autonomous system.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp always-compare-med command is used to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. After the bgp always-compare-med command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted).

The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

Examples

In the following example, BGP is configured to compare the MED during path selection for routes advertised by the same sub autonomous system within a confederation:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp deterministic-med
```

The following example show bgp command output shows how route selection is affected by the configuration of the bgp deterministic-med command. The order in which routes are received affects how routes are selected for best path selection when the bgp deterministic-med command is not

enabled. The following sample output from the show bgp command shows three paths that are received for the same prefix (10.100.0.0), and the bgp deterministic-med command is not enabled:

```
ciscoasa(router)# show bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external, best
```

If the bgp deterministic-med feature is not enabled on the router, the route selection can be affected by the order in which the routes are received. Consider the following scenario in which a router received three paths for the same prefix:

The clear bgp * command is entered to clear all routes in the local routing table.

```
ciscoasa(router)# clear bgp *
```

The show bgp command is issued again after the routing table has been repopulated. Note that the order of the paths changed after clearing the BGP session. The results of the selection algorithm also changed because the order in which the paths were received was different for the second session.

```
ciscoasa(router)# show bgp 10.100.0.0


BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal, best
```

If the bgp deterministic-med command is enabled, then the result of the selection algorithm will always be the same, regardless of the order in which the paths are received by the local router. The following output is always generated when the bgp deterministic-med command is entered on the local router in this scenario:

```
ciscoasa(router)# show bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 15
Paths: (3 available, best #1, advertised over EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal, best 3
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
```

Related Commands

Command	Description
bgp always compare-med	Enables the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.
clear bgp	Resets BGP connections using hard or soft reconfigurations.
show bgp	Displays entries in the Border Gateway Protocol (BGP) routing table.

bgp enforce-first-as

To configures an ASA to deny an update received from an external BGP (eBGP) peer that does not list its autonomous system number at the beginning of the AS_PATH in the incoming update, use the bgp enforce-first-as command in router configuration mode. To disable this behavior, use the no form of this command.

bgp enforce-first-as
no bgp enforce-first-as

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp enforce-first-as command is used to deny incoming updates received from eBGP peers that do not list their autonomous system number as the first segment in the AS_PATH attribute. Enabling this command prevents a misconfigured or unauthorized peer from misdirecting traffic (spoofing the local router) by advertising a route as if it was sourced from another autonomous system.

Examples

In the following example, all incoming updates from eBGP peers are examined to ensure that the first autonomous system number in the AS_PATH is the local AS number of the transmitting peer. In the following example, updates from the 10.100.0.1 peer will be discarded if the first AS number is not 65001:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp enforce-first-as
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.100.0.1 remote-as 65001
```

Related Commands

Command	Description
address-family ipv4	Enter address-family configuration mode.
neighbor remote-as	Add an entry to the BGP or the multiprotocol BGP routing table.

bgp fast-external-fallover

To configure a Border Gateway Protocol (BGP) routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down, use the bgp fast-external-fallover command in router configuration mode. To disable BGP fast external fallover, use the no form of this command.

bgp fast-external-fallover
no bgp fast-external-fallover

Syntax Description

This command has no arguments or keywords.

Command Default

BGP fast external fallover is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp fast-external-fallover command is used to disable or enable fast external fallover for BGP peering sessions with directly connected external peers. The session is immediately reset if link goes down. Only directly connected peering sessions are supported. If BGP fast external fallover is disabled, the BGP routing process will wait until the default hold timer expires (3 keepalives) to reset the peering session. BGP fast external fallover can also be configured on a per-interface basis using the ip bgp fast-external-fallover interface configuration command.

Examples

In the following example, the BGP fast external fallover feature is disabled. If the link through which this session is carried flaps, the connection will not be reset.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# no bgp fast-external-fallover
```

Related Commands

Command	Description
ip bgp fast-external-fallover	Configure per-interface fast external fallover.

bgp graceful-restart

To configure a Border Gateway Protocol (BGP) routing process for graceful restart in a non-stop forwarding configuration, use the **bgp graceful-restart** command in router configuration mode. To disable BGP graceful restart, use the **no** form of this command.

bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]
no bgp graceful-restart [**restart-time** *seconds* | **stalepath-time seconds**]

Syntax Description

restart-time *seconds*	The maximum time period (in seconds) that the system will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default is 120 seconds. Values are from 1 to 3600 seconds.
stalepath-time *seconds*	The maximum time period (in seconds) that the system will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value is 360 seconds. Values are from 1 to 3600 seconds.

Command Default

BGP graceful restart is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	• Yes

Command History

Release	Modification
9.3(1)	This command was added.
9.19(1)	This command was extended to support graceful restart for IPv6 address family.

Usage Guidelines

Use this command to enable graceful restart for non-stop forwarding. With graceful restart, the system can advertise the ability to maintain the forwarding state for an address group during restart. Use the **neighbor ha-mode graceful-restart** command to configure restart capability for each BGP neighbor router.

Examples

The following example shows how to enable graceful restart globally using the default timers.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp graceful-restart
```

Related Commands

Command	Description
neighbor ha-mode graceful-restart	Configure the Border Gateway Protocol (BGP) graceful restart capability for a BGP neighbor

bgp inject-map

To configure conditional route injection to inject more specific routes into a Border Gateway Protocol (BGP) routing table, use the bgp inject-map command in address family configuration mode. To disable a conditional route injection configuration, use the no form of this command.

bgp inject-map *inject-map exist-map* **exist-map** [**copy-attributes**]
no bgp inject-map *inject-map exist-map* **exist-map**

Syntax Description

inject-map	Name of the route map that specifies the prefixes to inject into the local BGP routing table.
exist-map exist-map	Specifies the name of the route map containing the prefixes that the BGP speaker will track.
copy-attributes	(Optional) Configures the injected route to inherit attributes of the aggregate route.

Command Default

No specific routes are injected into a BGP routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration, Address-family IPv6 sub mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

The bgp inject-map command is used to configure conditional route injection. Conditional route injection allows you to originate a more specific prefix into a BGP routing table without a corresponding match. Two route maps (exist-map and inject-map) are configured in global configuration mode and then specified with the bgp inject-map command in address family configuration mode.

The exist-map argument specifies a route map that defines the prefix that the BGP speaker will track. This route map must contain a match ip address prefix-list command statement to specify the aggregate prefix and a match ip route-source prefix-list command statement to specify the route source.

The inject-map argument defines the prefixes that will be created and installed into the routing table. Injected prefixes are installed in the local BGP RIB. A valid parent route must exist; Only prefixes that are equal to or more specific than the aggregate route (existing prefix) can be injected.

The optional copy-attributes keyword is used to optionally configure the injected prefix to inherit the same attributes as the aggregate route. If this keyword is not entered, the injected prefix will use the default attributes for locally originated routes.

Examples

In the following example, conditional route injection is configured. Injected prefixes will inherit the attributes of the aggregate (parent) route.

```
ciscoasa(config)# ip prefix-list ROUTE permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
ciscoasa(config)# route-map LEARNED_PATH permit 10
ciscoasa(config-route-map)# match ip address prefix-list ROUTE
ciscoasa(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
ciscoasa(config-route-map)# exit
ciscoasa(config)# route-map ORIGINATE permit 10
ciscoasa(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
ciscoasa(config-route-map)# set community 14616:555 additive
ciscoasa(config-route-map)# exit
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH copy-attributes
```

Related Commands

Command	Description
ip prefix-list	Creates a prefix-list or adds a prefix-list entry.
set community	Sets the BGP communities attributes.
address-family ipv4	Enters the address-family configuration mode.

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the bgp log-neighbor-changes command in router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use theno form of this command.

bgp log-neighbor-changes
no bgp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of BGP neighbor is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp log-neighbor-changes command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the bgp log-neighbor-changes command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging.

The neighbor status change messages are not tracked if the bgp log-neighbor-changes command is not enabled, except for the reset reason, which is always available as output of the show bgp neighbors command.

The eigrp log-neighbor-changes command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the bgp log-neighbor-changes command.

Use the show logging command to display the log for the BGP neighbor changes.

Examples

The following example logs neighbor changes for BGP in router configuration mode.

```
ciscoasa(config)# bgp router 40000
ciscoasa(config-router)# bgp log-neighbor-changes
```

Related Commands

Command	Description
show BGP neighbors	Displays information about BGP connection to neighbors.

bgp maxas-limit

To configure Border Gateway Protocol (BGP) to discard routes that has a number of autonomous system numbers in AS-path that exceed the specified value, use the bgp maxas-limit command in router configuration mode. To return the router to default operation, use the no form of this command.

bgp max-as limit *number*
no bgp max-as limit

Syntax Description

number	Maximum number of autonomous system numbers in the AS-path attribute of the BGP Update message, ranging from 1 to 254. In addition to setting the limit on the number of autonomous system numbers within the AS-path segment, the command limits the number of AS-path segments to ten. The behavior to allow ten AS-path segments is built into the bgp maxas-limit command.

Command Default

No routes are discarded.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp maxas-limit command is used to limit the number of autonomous system numbers in the AS-path attribute that are permitted in inbound routes. If a route is received with an AS-path segment that exceeds the configured limit, the BGP routing process will discard the route.

Examples

This example sets a maximum number of autonomous systems numbers in the AS-path attribute to 30.

```
ciscoasa(config)# router bgp 4000
ciscoasa(config)# bgp maxas-limit 30
```

bgp nexthop

To configure Border Gateway Protocol (BGP) next-hop address tracking, use the bgp nexthop command in address family or router configuration mode. To disable BGP next-hop address tracking, use the no form of this command.

bgp nexthop { **trigger** { **delay** *seconds* | **enable** } | **route-map** *map-name* }
no bgp nexthop { **trigger** { **delay** *seconds* | **enable** } | **route-map** *map-name* }

Syntax Description

trigger	Specifies the use of BGP next-hop address tracking. Use this keyword with the delay keyword to change the next-hop tracking delay. Use this keyword with the enable keyword to enable next-hop address tracking.
delay	Changes the delay interval between checks on updated next-hop routes installed in the routing table.
seconds	Number of seconds specified for the delay. Valid values are from 0 to 100. Default is 5.
enable	Enables BGP next-hop address tracking.
route-map	Specifies the use of a route map that is applied to the route in the routing table that is assigned as the next-hop route for BGP prefixes.
map-name	Name of a route map.

Command Default

BGP next-hop address tracking is enabled by default for IPv4.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration Address family IPv6 sub mode	• Yes	—	• Yes	—	• Yes

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to BGP as they are updated in the routing information base (RIB). This optimization improves overall BGP convergence by reducing the response time to next-hop

changes for routes installed in the RIB. When a best-path calculation is run in between BGP scanner cycles, only the changes are processed and tracked.

Note BGP next-hop address tracking improves BGP response time significantly. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP. We recommend that you aggressively dampen unstable IGP peering sessions to mitigate the possible impact to BGP.

- BGP next-hop address tracking is not supported under the IPv6 address family.

Use the trigger keyword with the delay keyword and seconds argument to change the delay interval between routing table walks for BGP next-hop address tracking. You can increase the performance of BGP next-hop address tracking by tuning the delay interval between full routing table walks to match the tuning parameters for the IGP. The default delay interval is 5 seconds, which is an optimal value for a fast-tuned IGP. In the case of an IGP that converges more slowly, you can change the delay interval to 20 seconds or more, depending on the IGP convergence time.

Use the trigger keyword with the enable keyword to enable BGP next-hop address tracking. BGP next-hop address tracking is enabled by default.

Use the route-map keyword and map-name argument to allow a route map to be used. The route map is used during the BGP best-path calculation and is applied to the route in the routing table that covers the Next_Hop attribute for BGP prefixes. If the next-hop route fails the route-map evaluation, the next-hop route is marked as unreachable. This command is per address family, so different route maps can be applied for next-hop routes in different address families.

Note Only the match ip address command is supported in the route map. No set commands or other match commands are supported.

Examples

The following example shows how to change the delay interval between routing table walks for BGP next-hop address tracking to occur every 20 seconds under an IPv4 address family session.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop trigger delay 20
```

The following example shows how to disable next-hop address tracking for the IPv4 address family:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# no bgp nexthop trigger enable
```

The following example shows how to configure a route map that permits a route to be considered as a next-hop route only if the address mask length is more than 25. This configuration will avoid any prefix aggregates being considered as a next-hop route.

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP
ciscoasa(config-router-af)# exit-address-family
```

```
ciscoasa(config-router)# exit
ciscoasa(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
ciscoasa(config)# route-map CHECK-NEXTHOP permit 10
ciscoasa(config)# match ip address prefix-list FILTER25
```

bgp redistribute-internal

To configure iBGP redistribution into an interior gateway protocol (IGP), such as EIGRP or OSPF, use the bgp redistribute-internal command in address family configuration mode. To return the router to default behavior and stop iBGP redistribution into IGPs, use the no form of this command.

bgp redistribute-internal
no bgp redistribute-internal

Syntax Description

This command has no arguments or keywords.

Command Default

IBGP routes are redistributed into IGPs.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration Address-family IPv6 sub mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

The bgp redistribute-internal command is used to configure iBGP redistribution into an IGP. The clear bgp command must be entered to reset BGP connections after this command is configured.

When redistributing BGP into any IGP, be sure to use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed.



Caution Exercise caution when redistributing iBGP into an IGP. Use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed. Redistributing an unfiltered BGP routing table into an IGP can have a detrimental effect on normal IGP network operation.

Examples

In the following example, BGP to OSPF route redistribution is enabled:

```
ciscoasa(config)# router ospf 300
```

```
ciscoasa(config-router)# redistribute bgp 200
ciscoasa(config-router)# exit
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp redistribute-internal
```

bgp router-id

To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the bgp router-id command in address family router configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the no form of this command.

bgp router-id *ip-address*
no bgp router-id

Syntax Description

ip-address	Router identifier in the form of an IP address.

Command Default

When this command is not enabled, the router ID is set to the highest IP address on a physical interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration Router configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified.

Usage Guidelines

The bgp router-id command is used to configure a fixed router ID for the local BGP routing process. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the router.Peering sessions are automatically reset when the router ID is changed. Separate router ID per context is possible.

Examples

The following example shows how to configure the local router with a fixed BGP router ID of 192.168.254.254

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP) routers for next hop validation use the bgp scan-time command in address family configuration mode. To return the scanning interval of a router to its default scanning interval of 60 seconds, use the no form of this command.

bgp scan-time *scanner-interval*
no bgp scan-time *scanner-interval*

Syntax Description

scanner-interval	The scanning interval of BGP routing information. Valid values are from 15 to 60 seconds. The default is 60 seconds

Command Default

The default scanning interval is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address family configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Entering the no form of this command does not disable scanning, but removes it from the output of the show running-config command.

While bgp nexthop address tracking (NHT) is enabled for an address family, the bgp scan-time command will not be accepted in that address family and will remain at the default value of 60 seconds. NHT must be disabled before the bgp scan-time command will be accepted in either router mode or address family mode.

Examples

In the following router configuration example, the scanning interval for next hop validation of IPv4 unicast routes for BGP routing tables is set to 20 seconds:

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp scan-time 20
```

Related Commands

Command	Description
show running-config	Displays the configuration that is currently displayed on the ASA.
bgp nexthop	Configures BGP next-hop address tracking.

bgp suppress-inactive

To suppress the advertisement of routes that are not installed in the routing information base (RIB), use the bgp suppress-inactive command in address family or router configuration mode.

bgp suppress-inactive
no bgp suppress-inactive

Syntax Description

This command has no arguments or keywords.

Command Default

No routes are suppressed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address family configuration Address family IPv6 sub-mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

The bgp suppress-inactive command is used to prevent routes that are not installed in the RIB (inactive routes) from being advertised to peers. If this feature is not enabled or if the no form of this command is used, Border Gateway Protocol (BGP) will advertise inactive routes.



Note BGP marks routes that are not installed into the RIB with a RIB-failure flag. This flag will also appear in the output of the show bgp command; for example, Rib-Failure (17). This flag does not indicate an error or problem with the route or the RIB, and the route may still be advertised depending on the configuration of this command. Enter the show bgp rib-failure command to see more information about the inactive route.

Examples

In the following example, the BGP routing process is configured to not advertise routes that are not installed in the RIB:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp suppress-inactive
```

Related Commands

Command	Description
show bgp	Displays entries in the BGP routing table.
show bgp rib-failure	Displays BGP routes that failed to install in the Routing Information Base (RIB) table.

bgp transport

To enable TCP transport session parameters globally for all Border Gateway Protocol (BGP) sessions, use the bgp transport command in router configuration mode. To disable TCP transport session parameters globally for all BGP sessions, use the no form of this command.

bgp transport path-mtu-discovery
no bgp transport path-mtu-discovery

Syntax Description

path-mtu-discovery	Enables transport path maximum transmission unit (MTU) discovery.

Command Default

TCP path MTU discovery is enabled by default for all BGP sessions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

This command is enabled by default because it is used to allow BGP sessions to take advantage of larger MTU links, which can be very important for internal BGP (iBGP) sessions. Use the show bgp neighbors command to ensure that TCP path MTU discovery is enabled.

Examples

The following example shows how to disable TCP path MTU discovery for all BGP sessions:

```
ciscoasa(config)# router bgp 4500
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

The following example shows how to enable TCP path MTU discovery for all BGP sessions:

```
iscoasa(config)# router bgp 4500
ciscoasa(config-router)# bgp transport path-mtu-discovery
```

Related Commands

Command	Description
show bgp neighbors	Displays information about BGP connections to neighbors.

blocks

To allocate additional memory to block diagnostics (displayed by the **show blocks** command), use the **blocks** command in privileged EXEC mode. To set the value back to the default, use the **no** form of this command.

blocks queue history enable [*memory_size*]
no blocks queue history enable [*memory_size*]

Syntax Description

memory_sizes	(Optional) Sets the memory size for block diagnostics in bytes, instead of applying the dynamic value. If this value is greater than free memory, an error message appears and the value is not accepted. If this value is greater than 50% of free memory, a warning message appears, but the value is accepted.

Command Default

The default memory assigned to track block diagnostics is 2136 bytes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To view the currently allocated memory, enter the **show blocks queue history** command.

If you reload the ASA, the memory allocation returns to the default.

The amount of memory allocated will be at most 150 KB, but never more than 50% of free memory. Optionally, you can specify the memory size manually.

Examples

The following example increases the memory size for block diagnostics:

```
ciscoasa# blocks queue history enable
```

The following example increases the memory size to 3000 bytes:

```
ciscoasa# blocks queue history enable 3000
```

The following example attempts to increase the memory size to 3000 bytes, but the value is more than the available free memory:

```
ciscoasa# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

The following example increases the memory size to 3000 bytes, but the value is more than 50% of the free memory:

```
ciscoasa# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

Related Commands

Command	Description
clear blocks	Clears the system buffer statistics.
show blocks	Shows the system buffer usage.

boot

To specify which image the system uses at the next reload and which configuration file the system uses at startup, use the **boot** command in global configuration mode. To restore the default value, use the **no** form of this command.

boot { **config** | **system** } *url*
no boot { **config** | **system** } *url*

Syntax Description

config	Specifies which configuration file to use when the system is loaded.
system	Specifies which image file to use when the system is loaded.
url	Sets the location of the image or configuration. In multiple context mode, all remote URLs must be accessible from the admin context. See the following URL syntax: • **disk0:**/[*path*/]*filename* For the ASA, this URL indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* For the ASA, this URL indicates the external Flash memory card. This option is not available for the ASA Services Module. • **flash:**/[*path*/]*filename* This URL indicates the internal Flash memory. • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address. This option is available for the **boot system** command for the ASA 5500 series only; the **boot config** command requires the startup configuration to be on the flash memory. Only one **boot system tftp:** command can be configured, and it must be the first one configured.

Command Default

- ASA image:
  - Firepower 1000, and 2100 in Appliance mode—Boots the previously-running boot image.
  - Other Physical ASAs—Boots the first application image that it finds in internal flash memory.
  - ASA Virtual—Boots the image in the read-only boot:/ partition that was created when you first deployed.
  - Firepower 4100/9300 chassis—The Secure Firewall eXtensible Operating System (FXOS) determines which ASA image to boot. You cannot use this procedure to set the ASA image.
  - Firepower 2100 in Platform mode—The FXOS system determines which ASA/FXOS package to boot. You cannot use this procedure to set the ASA image.

- Startup configuration—By default, the ASA boots from a startup configuration that is a hidden file.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	This command added Firepower 1000 and 2100 in Appliance mode support.

Usage Guidelines

If you have more than one ASA or ASDM image, you should specify the image that you want to boot. If you do not set the image, the default boot image is used, and that image may not be the one intended. For the startup configuration, you can optionally specify a configuration file.

See the following model guidelines:

- Firepower 4100/9300 chassis—ASA upgrades are managed by FXOS; you cannot upgrade the ASA within the ASA operating system, so do not use this command for the ASA image. You can upgrade ASA and FXOS separately from each other, and they are listed separately in the FXOS directory listing. The ASA package always includes ASDM.
- Firepower 2100 in Platform mode—The ASA, ASDM, and FXOS images are bundled together into a single package. Package updates are managed by FXOS; you cannot upgrade the ASA within the ASA operating system, so do not use this command for the ASA image. You cannot upgrade ASA and FXOS separately from each other; they are always bundled together.
- Firepower 1000 and 2100 in Appliance mode—The ASA, ASDM, and FXOS images are bundled together into a single package. Package updates are managed by ASA using this command. Although these platforms use the ASA to identify the image to boot, the underlying mechanism is different from legacy ASAs.
- ASA Virtual—The initial deployment ASA Virtual package puts the ASA image in the read-only boot:/ partition. When you upgrade the ASA Virtual, you specify a different image in flash memory. Note that if you later clear your configuration (**clear configure all**), then the ASA Virtual will revert to loading the original deployment image. The initial deployment ASA Virtual package also includes an ASDM image that it places in flash memory. You can upgrade the ASDM image separately.

When you save the **boot config** command to the startup configuration using the **write memory** command, you also save the settings to the CONFIG_FILE environment variable, which the ASA uses to determine the startup configuration to boot when it restarts.

If you want to use a startup configuration file at the new location that is different from the current running configuration, then be sure to copy the startup configuration file to the new location after you save the running

configuration. Otherwise, the running configuration will overwrite the new startup configuration when you save it.

Tip The ASDM image file is specified by the asdm image command.

boot system for the Firepower 1000 and 2100 in Appliance Mode

You can only enter a single **boot system** command. If you upgrade to a new image, then you must enter **no boot system** to remove the previous image you set.

Note that you may not have a **boot system** command present in your configuration; for example, if you installed the image from ROMMON, have a new device, or you removed the command manually.

The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA. If you change your mind prior to reloading, you can enter the **no boot system** command to delete the new image from the boot location, so the current image continues to run. You can even delete the original image file from the ASA flash memory after you enter this command, and the ASA will boot correctly from the boot location.

Unlike other models, this command in the startup configuration does not affect the booting image, and is essentially cosmetic. The last-loaded boot image will always run upon reload. If you do not save the configuration after you enter this command, then when you reload, the old command will be present in your configuration, even though the new image was booted. Be sure to save the configuration so that the configuration remains in sync.

You can only load images with the original filename from the Cisco download site. If you change the filename, it will not load. You can also reimage to the Secure Firewall Threat Defense (formerly Firepower Threat Defense) by loading an Firewall Threat Defense image. In this case, you are prompted to reload immediately.

boot system for Other Models

You can enter up to four **boot system** command entries to specify different images to boot from in order; the ASA boots the first image it finds successfully. When you enter the **boot system** command, it adds an entry at the bottom of the list. To reorder the boot entries, you must remove all entries using the **clear configure boot system** command, and re-enter them in the order you desire. Only one **boot system tftp** command can be configured, and it must be the first one configured.

When you save the **boot system** command to the startup configuration using the **write memory** command, you also save the settings to the BOOT environment variable, which the ASA uses to determine the startup image to boot when it restarts.

Examples

The following example specifies that at startup the ASA should load a configuration file called configuration.txt:

```
ciscoasa(config)# boot config disk0:/configuration.txt
```

Related Commands

Command	Description
asdm image	Specifies the ASDM software image.

Command	Description
show bootvar	Displays boot file and configuration environment variables.

border style

To customize the border of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **border style** command in customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

border style *value*
no border style *value*

Syntax Description

value Specifies the Cascading Style Sheet (CSS) parameters to use. The maximum number of characters allowed is 256.

Command Default

The default style of the border is background-color:#669999;color:white.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma-separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.



Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the background color of the border to the RGB color #66FFFF, a shade of green:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# border style background-color:66FFFF
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

breakout

To break out 10GB ports from a 40GB or higher interface, use the **breakout** command in global configuration mode. To rejoin the interfaces, use the **no** form of the command.

breakout *slot port*
no breakout *slot port*

Syntax Description

slot *port*	Specifies the interface slot and port that you want to break out. For example, to break out the Ethernet2/1 40GB interface, you would specify **2** for the slot and 1 for the port

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.18(1)	This command was added.

Usage Guidelines

Breakout ports can be used just like any other physical Ethernet port, including being added to EtherChannels.

If an interface is already in use in your configuration, you will have to manually remove any configuration related to interfaces that will no longer be present.

You must use a supported breakout cable. See the hardware installation guide for more information.

For clustering or failover, make sure the cluster/failover link is not using the parent interface (for breaking out) or the child interface (for rejoining); you cannot make changes to the interface if it is in use for the cluster/failover link.

For clustering or failover, enter this command on the control node/active unit; the module state is replicated to the other nodes.

For rejoining, you must rejoin all child ports for the interface.

Examples

The following example breaks out the Ethernet2/1 40GB interface. The resulting child interfaces will be identified as Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, and Ethernet2/1/4.

```
ciscoasa(config)# breakout 2 1
```

The following example rejoins the Ethernet2/1 40GB interface.

```
ciscoasa(config)# no breakout 2 1
```

Related Commands

Command	Description
interface	Configures an interface.

bridge-group

To assign an interface to a bridge group, use the **bridge-group** command in interface configuration mode. To unassign an interface, use the **no** form of this command. Bridge groups connect the same network on its interfaces.

bridge-group *number*
no bridge-group *number*

Syntax Description

number	Specifies an integer between 1 and 100. For 9.3(1) and later, the range is increased to between 1 and 250.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.3(1)	The number range was increased to between 1 and 250 to support 250 BVIs.
9.6(2)	The maximum interfaces per bridge group was increased from 4 to 64.
9.7(1)	Support for routed mode was added.

Usage Guidelines

For 9.2 and earlier, You can configure up to 8 bridge groups in single mode or per context in multiple mode; for 9.3(1) and later, you can configure up to 250 bridge groups. Each bridge group can include up to 64 interfaces (4 interfaces for 9.6(1) and earlier). You cannot assign the same interface to more than one bridge group. Note that you must use at least 1 bridge group; data interfaces must belong to a bridge group.

Note Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group.

Assign a management IP address to the bridge group using the **interface bvi** command and then the **ip address** command.

Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA.

You might want to use more than one bridge group if you do not want the overhead of security contexts, or want to maximize your use of security contexts. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

Examples

The following example assigns GigabitEthernet 1/1 to bridge group 1:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# bridge-group 1
```

Related Commands

Command	Description
interface	Configures an interface.
interface bvi	Enters the interface configuration mode for a bridge group so you can set the management IP address.
ip address	Sets the management IP address for a bridge group.
nameif	Sets the interface name.
security-level	Sets the interface security level.

browse-networks

To customize the Browse Networks box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **browse-networks** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

browse-networks { **title** | **message** | **dropdown** } { **text** | **style** } *value*
no browse-networks [{ **title** | **message** | **dropdown** } { **text** | **style** } *value*]

Syntax Description

dropdown	Specifies a change to the drop-down list.
message	Specifies youa change to the message displayed under the title.
style	Specifies a change to the style.
text	Specifies a change to the text.
title	Specifies a change to the title.
value	Indicates the actual text to display. The maximum number of characters allowed is 256. This value applies to Cascading Style Sheet (CSS) parameters also.

Command Default

The default title text is “Browse Networks”.

The default title style is:

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text is “Enter Network Path”.

The default message style is:

background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is “File Folder Bookmarks”.

The default dropdown style is:

border:1px solid black;font-weight:bold;color:black;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the title to “Browse Corporate Networks”, and the text within the style to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
ciscoasa(config-webvpn-custom)# browse-networks title style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.



PART II

C Commands

- ca - cld, on page 475
- clear a – clear k, on page 561
- clear l – clear z, on page 679
- clf - crx, on page 771
- crypto a – crypto ir, on page 915
- crypto is – cz, on page 1041



ca - cld

- cache, on page 477
- ca-check, on page 479
- cache-static-content, on page 480
- cache-time, on page 481
- call-agent, on page 482
- call-duration-limit, on page 484
- call-party-numbers, on page 485
- call-home, on page 486
- call-home send, on page 490
- call-home send alert-group, on page 492
- call-home test, on page 494
- capability lls, on page 496
- capability opaque, on page 497
- captive-portal, on page 498
- capture, on page 500
- cd, on page 515
- cdp-url, on page 516
- certificate, on page 518
- certificate-group-map, on page 520
- chain, on page 522
- change-password, on page 523
- changeto, on page 525
- channel-group, on page 527
- character-encoding, on page 530
- checkheaps, on page 532
- check-retransmission, on page 534
- checksum-verification, on page 536
- checksum-verification, on page 538
- cipc security-mode authenticated (Deprecated), on page 540
- clacp static-port-priority, on page 542
- clacp system-mac, on page 544
- class (global), on page 546
- class (policy-map), on page 548

- class-map, on page 551
- class-map type inspect, on page 554
- class-map type management, on page 557
- class-map type regex, on page 559

cache

To enter cache mode and set values for caching attributes, enter the **cache** command in webvpn configuration mode. To remove all cache related commands from the configuration and reset them to their default values, enter the **no** form of this command.

cache
no cache

Command Default

Disabled.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	The default changed from enabled to disabled.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, so that many applications run much more efficiently.

Note Enabling the content cache may cause some systems to become less reliable. If you experience random crashes after enabling the content cache, disable it.

The following example shows how to enter cache mode:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache-static-content	Caches content not subject to rewriting.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum size of an object to cache.

ca-check

To configure the basic constraints extension and set the CA flag in a trustpoint certificate, use the **ca-check** command in crypto ca trustpoint configuration mode. To not set the basic constraints extension and CA flag, use the **no** form of this command.

ca-check
no ca-check

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the basic constraints extension and CA flag are set. You must use the **no** form to disable them.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

The basic constraints extension identifies whether the subject of the certificate is a Certificate Authority (CA), in which case the certificate can be used to sign other certificates. The CA flag is part of this extension. The presence of these items in a certificate indicates that the certificate's public key can be used to validate certificate signatures.

Examples

The following example shows how to disable the CA flag and basic constraints extension.

```
ciscoasa(config)# crypto ca trustpoint newtrust

ciscoasa(config-ca-trustpoint)# no ca-check

ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode. Use this command in global configuration mode.

cache-static-content

To cache all static content used for Clientless SSL VPN connections, enter the cache-static-content command in webvpn cache configuration mode. To disable caching of static content, enter the **no** form of this command.

cache-static-content enable
no cache-static-content enable

Syntax Description

enable	Enables the loading of all static content into cache memory.

Command Default

Disabled.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn cache configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Configuring the security appliance to store all cache-able static content in the appliance cache increases the performance of back-end SSL VPN connections. Static content includes objects not rewritten by the security appliance, such as PDF files and images.

Examples

The following example enables caching of static content:

```
ciscoasa(config-webvpn-cache)# cache-static-content enable
```

Related Commands

Command	Description
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.

cache-time

To specify in minutes how long to allow a CRL to remain in the cache before considering it stale, use the **cache-time** command in ca-crl configuration mode, which is accessible from crypto ca trustpoint configuration mode. To return to the default value, use the **no** form of this command.

cache-time *refresh-time*
no cache-time

Syntax Description

refresh-time	Specifies the number of minutes to allow a CRL to remain in the cache. The range is 1 - 1440 minutes. If the NextUpdate field is not present in the CRL, the CRL is not cached.

Command Default

The default setting is 60 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters ca-crl configuration mode, and specifies a cache time refresh value of 10 minutes for trustpoint central:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# cache-time 10
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
enforcenextupdate	Specifies how to handle the NextUpdate CRL field in a certificate.

call-agent

To specify a group of call agents, use the **call-agent** command in mgcp map configuration mode. To remove the configuration, use the **no** form of this command.

call-agent *ip_address group_id*
no call-agent *ip_address group_id*

Syntax Description

group_id	The ID of the call agent group, from 0 to 2147483647.
ip_address	The IP address of the gateway.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Mgcp map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the call-agent command to specify a group of call agents that can manage one or more gateways. The call agent group information is used to open connections for call agents in the group (other than the one to which a gateway sends a command) so that any of the call agents can send the response. Call agents with the same >*group_id* belong to the same group. A call agent may belong to more than one group.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
ciscoasa(config)# mgcp-map mgcp_inbound
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debugging information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

call-duration-limit

To configure the call duration for an H.323 call, use the **call-duration-limit** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

call-duration-limit hh:mm:ss
no call-duration-limit hh:mm:ss

Syntax Description

hh:mm:ss	Specifies the duration in hours, minutes, and seconds.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure the call duration for an H.323 call:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-duration-limit 0:1:0
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3 or 4 policy map.
show running-config policy-map	Displays all current policy map configurations.

call-party-numbers

To enforce sending call party numbers during an H.323 call setup, use the **call-party-numbers** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

call-party-numbers
no call-party-numbers

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to enforce call party numbers during call setup for an H.323 call:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-party-numbers
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3 or 4 policy map.
show running-config policy-map	Displays all current policy map configurations.

call-home

To enter call home configuration mode, use the **call-home** command in global configuration mode.

call-home

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

After you enter the **call-home** command, the prompt changes to hostname (cfg-call-home)#, and you have access to the following Call Home configuration commands:

- [no] alert-group {group name | all}—Enables or disables the Smart Call Home group. The default is enabled for all alert-groups.group name: Syslog, diagnostic, environment, inventory, configuration, snapshot, threat, telemetry, test.
- [no] contact-e-mail-addr e-mail-address—Specifies the customer contact e-mail address. This field is required.e-mail-address: A customer e-mail address of up to 127 characters.
- [no] contact-name contact name—Specifies the customer name.e-mail-address: A customer name of up to 127 characters.
- [no] contract-id contract-id-string—Specifies customer contract identification.contract-id-string: An identification number up to 128 characters. Spaces are allowed, but you must use quotes around the string if it includes spaces.
- copy profile src-profile-name dest-profile-name—Copies the content of an existing profile (**src-profile-name**) to a new profile (**dest-profile-name**).src-profile-name: An existing profile name of up to 23 characters.dest-profile-name: A new profile name of up to 23 characters.
- rename profile src-profile-name dest-profile-name—Changes the name of an existing profile.src-profile-name: An existing profile name of up to 23 characters.dest-profile-name: A new profile name of up to 23 characters.
- source-interface—Specifies the source interface.

- no configuration all—Clears the Smart Call-home configuration.[no] customer-id customer-id-string—Specifies the customer ID.customer-id-string: A customer ID of up to 64 characters. This field is required for XML format messages.
- [no] event-queue-size queue_size—Specifies the event queue size.queue-size: The number of events from 5-60. The default is 10.
- [no] mail-server ip-address | name priority 1-100 all—Specifies the SMTP mail server. Customers can specify up to five mail servers. At least one mail server is required for using e-mail transport for Smart Call Home messages. ip-address: The IPv4 or IPv6 address of the mail server.name: The hostname of the mail server.1-100: The priority of the mail server. The lower the number, the higher the priority.
- [no] phone-number phone-number-string—Specifies the customer phone number. This field is optional.phone-number-string: The phone number.
- [no] rate-limit msg-count—Specifies the number of messages that Smart Call Home can send per minute.msg-count: The number of messages per minute. The default is 10.
- [no] sender {from e-mail-address | reply-to e-mail-address} —Specifies the from/reply-to e-mail address of an e-mail message. This field is optional.e-mail-address: The from and reply-to e-mail address.
- [no] site-id site-id-string—Specifies the customer site ID. This field is optional.site-id-string: A site ID to identify the location of the customer.
- [no] street-address street-address—Specifies the customer address. This field is optional.street-address: A free-format string of up to 255 characters.
- [no] alert-group-config environment—Enters environment group configuration mode.[no] threshold {cpu | memory} low-high—Specifies the environmental resource threshold.low, high: Valid values are 0-100. The default is 85-90.
- [no] alert-group-config snapshot—Enters snapshot group configuration mode.system, user: To run the CLI in sysem or user context (available only in multimode).
- [no] add-command “cli command” [{system | user}] —Specifies CLI commands to capture in the snapshot group.cli command: The CLI command to be entered.system, user: To run the CLI in the system or in user context (available only in multiple mode). If both the system and user are not specified, the CLI will be run in both the system and user contexts. The default is the user context.
- All bullets below moved to profile command.
- [no] profile profile-name | no profile all—Creates, deletes, or edits a profile. Enters profile configuration mode and changes the prompt to hostname (cfg-call-home-profile)#. profile-name: A profile name of up to 20 characters.
- [no] active—Enables or disables a profile. The default is enabled.no destination address {e-mail | http} all | [no] destination {address {e-mail | http} e-mail-address | http-url [msg-format short-text | long-text | xml] | message-size-limit max-size | preferred-msg-format short-text | long-text | xml | transport-method e-mail | http}—Configures the destination, message size, message format, and transport method for the Smart Call Home message receiver. The default message format is XML, and the default enabled transport method is e-mail.e-mail-address: The e-mail address of the Smart Call Home receiver, which can be up to 100 characters.http-url: The HTTP or HTTPS URL.max-size: The maximum message size in bytes. 0 means no limit. The default is 5 MB.
- [no] subscribe-to-alert-group alert-group-name [severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging}]—Subscribes to events of a group

with a specified severity level.alert-group-name: Syslog, diagnostic, environment, or threat are valid values.

- [no] subscribe-to-alert-group syslog [{severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging} | message start [-end]}]—Subscribes to syslogs with a severity level or message ID.start-[end]: One syslog message ID or a range of syslog message IDs.



Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

- [no] subscribe-to-alert-group inventory [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]—Subscribes to inventory events.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group configuration [export full | minimum] [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]—Subscribes to configuration events.full: Configuration to export the running configuration, startup configuration, feature list, number of elements in an access list, and the context name in multimode.minimum: Configuration to export-only feature list, number of elements in an access list, and the context name in multimode.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group telemetry periodic {hourly | daily | monthly day_of_month | weekly day_of_week [hh:mm]—Subscribes to telemetry periodic events.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group snapshot periodic {interval minutes | hourly [mm] | daily | monthly day_of_month |weekly day_of_week [hh:mm]}—Subscribes to snapshot periodic events.minutes: The interval in minutes.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.

Examples

The following example show how to configure contact information:

```
hostname(config)# call-home
hostname(cfg-call-home)# contact-e-mail-addr username@example.com
hostname(cfg-call-home)# customer-id Customer1234
hostname(cfg-call-home)# phone-number +1-800-555-0199
hostname(cfg-call-home)# site-id Site1
hostname(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

The following example shows how to configure the Call Home message rate-limit threshold:

```
hostname(config)# call-home
hostname(cfg-call-home)# rate-limit 50
```

The following example shows how to set the Call Home message rate-limit threshold to the default setting:

```
hostname(config)# call-home
hostname(cfg-call-home)# default
rate-limit
```

The following example shows how to create a new destination profile with the same configuration settings as an existing profile:

```
hostname(config)# call-home
hostname(cfg-call-home)# copy profile profile1 profile1a
```

The following example shows how to configure the general e-mail parameters, including a primary and secondary e-mail server:

```
hostname(config)# call-home
hostname(cfg-call-home)# mail-server smtp.example.com priority 1
hostname(cfg-call-home)# mail-server 192.168.0.1 priority 2
hostname(cfg-call-home)# sender from username@example.com
hostname(cfg-call-home)# sender reply-to username@example.com
```

Related Commands

Command	Description
alert-group	Enables an alert group.
profile	Enters call-home profile configuration mode.
show call-home	Displays Call Home configuration information.

call-home send

To execute a CLI command and e-mail the command output to a specified address, use the **call-home send** command in privileged EXEC mode.

call-home send cli command [**email** *email*] [**service-number** *service number*]

Syntax Description

cli-command	Specifies the CLI command to be executed. The command output is sent by e-mail.
email *email*	Specifies the e-mail address to which the CLI command output is sent. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com.
service-number *service number*	Specifies an active TAC case number to which the command output pertains. This number is required only if no e-mail address (or a TAC e-mail address) is specified, and will appear in the e-mail subject line.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

This command causes the specified CLI command to be executed on the system. The specified CLI command must be enclosed in quotes (“”), and can be any **run** or **show** command, including commands for all modules.

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com. The e-mail is sent in long text format with the service number, if specified, in the subject line.

Examples

The following example shows how to send a CLI command and have the command output e-mailed:

```
hostname# call-home send "show diagnostic result module all" email support@example.com
```

Related Commands

call-home	Enters call home configuration mode.

call-home test	Sends a Call Home test message that you define.
service call-home	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home send alert-group

To send a specific alert group message, use the **call-home send alert-group** command in privileged EXEC mode.

call-home send alert-group { **configuration** | **telemetry** | **inventory** | **group snapshot** } [**profile** *profile-name*]

Syntax Description

configuration	Sends the configuration alert-group message to the destination profile.
group snapshot	Sends the snapshot group.
inventory	Sends the inventory call-home message.
profile *profile-name*	(Optional) Specifies the name of the destination profile.
telemetry	Sends the diagnostic alert-group message to the destination profile for a specific module, slot/subslot, or slot/bay number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

If you do not specify the profile *profile-name*, the message is sent to all subscribed destination profiles.

Only the configuration, diagnostic, and inventory alert groups can be manually sent. The destination profile need not be subscribed to the alert group.

Examples

The following example shows how to send the configuration alert-group message to the destination profile:

```
hostname# call-home send alert-group configuration
```

The following example shows how to send the diagnostic alert-group message to the destination profile for a specific module, slot/subslot, or slot/bay number:

```
hostname# call-home send alert-group diagnostic module 3 5/2
```

The following example shows how to send the diagnostic alert-group message to all destination profiles for a specific module, slot/subslot, or slot/bay number:

```
hostname# call-home send alert-group diagnostic module 3 5/2 profile Ciscotac1
```

This example shows how to send the inventory call-home message:

```
hostname# call-home send alert-group inventory
```

Related Commands

call-home	Enters call home configuration mode.
call-home test	Sends a Call Home test message that you define.
service call-home	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home test

To manually send a Call Home test message using the configuration of a profile, use the **call-home test** command in privileged EXEC mode.

call-home test [*"test-message"*] **profile** *profile-name*

Syntax Description

profile *profile-name*	Specifies the name of the destination profile.
"*test-message*"	(Optional) Test message text.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

This command sends a test message to the specified destination profile. If you enter test message text, you must enclose the text in quotes ("") if it contains spaces. If you do not enter a message, a default message is sent.

Note The **call-home test** command is applicable only for Smart Software Managers that manage the device licenses online, and not for Smart Software Manager On-Prem servers.

Examples

The following example shows how to manually send a Call Home test message:

```
hostname# call-home test "test of the day" profile Ciscotac1
```

Related Commands

call-home	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.

service call-home	Enables or disables Call Home.
show call-home	Displays Call Home configuration information.

capability lls

The LLS capability is enabled by default. To explicitly enable the use of the Link-Local Signalling (LLS) data block in originated OSPF packets and re-enable OSPF NSF awareness, use the capability lls command in the router-configuration mode. To disable LLS and OSPF NSF awareness, use the no form of this command.

capability lls
no capability lls

Syntax Description

This command has no arguments or keywords.

Command Default

LLS capability is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router-configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was introduced.

Usage Guidelines

You might want to disable NSF awareness by disabling the use of the LLS data block in originated OSPF packets. You might want to disable NSF awareness if the router has no applications using LLS.

If NSF is configured and you try to disable LLS, you will receive the error message, "OSPF Non-Stop Forwarding (NSF) must be disabled first."

If LLS is disabled and you try to configure NSF, you will receive the error message, "OSPF Link-Local Signaling (LLS) capability must be enabled first."

Examples

The following example enables LLS support and OSPF awareness:

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability lls
```

Related Commands

capability opaque	Enable MPLS TE information to be flooded to through the network using opaque LSAs

capability opaque

To enable Multiprotocol Label Switching traffic engineering (MPLS TE) topology information to flood the network through opaque LSAs, use the capability opaque command in the router-configuration mode. To disable MPLS TE topology information flooding through opaque LSAs to the network, use the no form of the command.

capability opaque
no capability opaque

Syntax Description

This command has no arguments or keywords.

Command Default

Opaque LSAs are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router-configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was introduced.

Usage Guidelines

The capability opaque command floods MPLS TE information (Types 1 and 4) through opaque LSAs of all scope (Types 9, 10, and 11).

Control opaque LSA support capability must be enabled for OSPF to support MPLS TE.

The MPLS TE topology information is flooded to the area through opaque LSAs by default.

Examples

The following example enables opaque capability:

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability opaque
```

Related Commands

capability lls	Enables use of LLS data-block in OSPF originated packets and enables OSPF NSF awareness.

captive-portal

To enable captive portal for the ASA FirePOWER module, use the **captive-portal** command in global configuration mode. To disable captive portal, use the **no** form of this command.

captive-portal { **global** | **interface** *name* } [**port** *number*]
no captive-portal { **global** | **interface** *name* } [**port** *number*]

Syntax Description

global	Enables captive portal globally on all interfaces.
interface *name*	Enables captive portal on the specified interface only. You can enter the command multiple times to enable it on more than one interface. You can use this approach if you are redirecting traffic for only a subset of interfaces to the ASA FirePOWER module.
port *number*	(Optional.) Sets the authentication proxy port to 1025 higher. Do not specify the keyword if you want to configure the default port, which is 885.

Command Default

The default port is 885 (TCP).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Captive portal works in conjunction with the identity policy defined on the ASA FirePOWER module.

For HTTP/HTTPS connections, you can define identity rules that collect user identification through active authentication. If you want to implement active authentication identity rules, you must configure captive portal on the ASA to act as the authentication proxy port. When a connection matches an identity rule that requests active authentication, the ASA FirePOWER module redirects the authentication request to the ASA interface IP address/captive portal. The default port is 885, which you can change.

If you do not enable captive portal for the authentication proxy, only passive authentication is available.

Examples

The following example enables captive portal globally on the default port 885:

```
ciscoasa(config)# captive-portal global
```

```
ciscoasa(config)#
```

Related Commands

Command	Description
sfr	Redirects traffic to the ASA FirePOWER module.
show running-config captive-portal	Displays the captive portal configuration.
show service-policy	Shows service policy statistics.

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command in privileged EXEC mode. To disable packet capture capabilities, use the **no** form of this command.

Capture network traffic:

capture *capture_name* [**type** { **asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user* }] [**access-list** *access_list_name* { **interface** { *interface_name* | **asa_dataplane asa_mgmt_plane** | **cplane** } } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**match** *protocol* { **host** *source-ip* | *source-ip mask* | **any** | **any4** | **any6** } [*operator src_port*] { **host** *dest_ip* | *dest_ip mask* | | **any** | **any4** | **any6** } [*operator dest_port*]] [**switch**] [**offload**] [**ivlan** *number*] [**ovlan** *number*]

Capture cluster control-link traffic:

capture *capture_name* { **type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]
capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**cp-cluster**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**match** *protocol* { **host** *source-ip* | *source-ip mask* | **any** | **any4** | **any6** } [*operator src_port*] { **host** *dest_ip* | *dest_ip mask* | | **any** | **any4** | **any6** } [*operator dest_port*]]

Ingress switch capture packets for Secure Firewall 3100 model devices:

capture *capture_name* **switch interface** *interface_name* [**drop** { **disable** | **mac-filter** }]

Bi-directional switch packet capture for 1200/4200/6100 model devices:

capture *capture_name* **switch interface** *interface_name* [**direction** { { **both** | **egress** } [**drop disable**] | **ingress** [**drop** { **disable** | **mac-filter** }] }]

Note For Secure Firewall 4200 model devices, the **mac-filter** option is supported only for the **ingress** direction.

Note For Secure Firewall 6100 model devices, the **drop** option is supported only for the ingress direction.

Capture packets cluster-wide:

cluster exec capture *capture_name* [**persist**] [**include-decrypted**]

Clear persistent packet traces cluster-wide:

cluster exec clear packet-trace

Remove the packet capture:

no capture *capture_name* [*arguments*]

Manually stop or start the packet capture:

capture *capture_name* **stop**
no capture *capture_name* **stop**

Syntax Description

access-list *access_list_name*	(Optional) Captures traffic that matches an access list. In multiple context mode, this is only available within a context.
any	Specifies all IPv4 traffic.
any4	Specifies all IPv4 traffic.
any6	Specifies all IPv6 traffic.
all	Captures all packets dropped by the accelerated security path.
asa_dataplane	Captures packets on the ASA backplane that pass between the ASA and a module that uses the backplane, such as the ASA FirePOWER module.
asp-drop *drop-code*	(Optional) Captures packets dropped by the accelerated security path. The *drop-code* specifies the type of traffic that is dropped by the accelerated security path. See the **show asp drop frame** command for a list of drop codes. You can enter this keyword with the **packet-length**, **circular-buffer**, and **buffer** keywords, but not with the **interface** or **ethernet-type** keyword. In a cluster, dropped forwarded data packets from one unit to another are also captured. In multiple context mode, when this option is issued in the system execution space, all dropped data packets are captured; when this option is issued in a context, only dropped data packets that enter from interfaces belonging to the context are captured.
buffer *buf_size*	(Optional) Defines the buffer size used to store the packet in bytes. Once the byte buffer is full, packet capture stops. When used in a cluster, this is the per-unit size, not the sum of all units.
capture_name	Specifies the name of the packet capture. Use the same name on multiple **capture** statements to capture multiple types of traffic. When you view the capture configuration using the **show capture** command, all options are combined on one line.
circular-buffer	(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.
cp-cluster	(Optional) Capture control packets on cluster interface.
direction	(Optional. Supported on: Secure Firewall 1220, Secure Firewall 4200, Secure Firewall 6100 devices.) Specifies the direction of the switch traffic to be captured. It can be one of the following: • **both**—To capture switch bi-directional traffic • **egress**—To capture switch egressing traffic • **ingress**—To capture switch ingressing traffic

drop	Specifies the packet capture configuration of the mac-filter drop: • **disable**—To disable capture of packets dropped from switch. • **mac-filter**—To capture switch mac-filter drop. **Note** • For the Secure Firewall 3100, **drop** is available when you select the interface. • For the Secure Firewall 4200, the **drop** keyword is available only when you select the direction. However, the **mac-filter** option is supported only for the ingress packet capture direction. • For the Secure Firewall 6100, the **drop** keyword is available only for the ingress packet capture direction.
ethernet-type *type*	(Optional) Selects an Ethernet type to capture. Supported Ethernet types include 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP, and VLAN. An exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner Ethernet type is used for matching.
host *ip*	Specifies the single IP address of the host to which the packet is being sent.
include-decrypted	(Optional) Captures decrypted IPsec packets which contain both normal and decrypted traffic once they enter the firewall device. It also captures packets of SSL decrypted traffic. However, the capture does not include the decrypted packets from VTI because they are available only on the VTI interface and not on the outside interface.
inline-tag *tag*	Specifies a tag for a particular SGT value or leaves it unspecified to capture a tagged packet with any SGT value.
interface *interface_name*	Sets the name of the interface on which to use packet capture. You must configure an interface for any packets to be captured except for **type asp-drop**. You can configure multiple interfaces using multiple **capture** commands with the same name. To capture packets on the dataplane, management plane, or control plane of an ASA, you can use the **interface** keyword with **asa_dataplane**, **asa_mgmt_plane**, or **cplane** as the interface name.You can specify **cluster** as the interface name to capture the traffic on the cluster control link interface. If the type **lacp** capture is configured, the interface name is the physical name.
ikev1 or **ikev2**	Captures only IKEv1 or IKEv2 protocol information.
isakmp	(Optional) Captures ISAKMP traffic for VPN connections. The ISAKMP subsystem does not have access to the upper layer protocols. The capture is a pseudo capture, with the physical, IP, and UDP layers combined together to satisfy a PCAP parser. The peer addresses are obtained from the SA exchange and are stored in the IP layer.
lacp	(Optional) Captures LACP traffic. If configured, the interface name is the physical interface name.

mask	The subnet mask for the IP address. When you specify a network mask, the method is different from the Cisco IOS software access-list command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
match *protocol*	Specifies the packets that match the five-tuple to allow filtering of those packets to be captured. You can use this keyword up to three times on one line.
operator	(Optional) Matches the port numbers used by the source or destination. The permitted operators are as follows: • lt—less than • gt—greater than • eq—equal to • **neq**—not equal to • **range**—range
packet-length *bytes*	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
persit	(Optional) Captures persistent packets on cluter units.
port	(Optional) If you set the protocol to tcp or udp, specifies the integer or name of a TCP or UDP port.
raw-data	(Optional) Captures inbound and outbound packets on one or more interfaces.
real-time	Displays the captured packets continuously in real-time. To terminate real-time packet capture, enter **Ctrl + c.** To permanently remove the capture, use the **no** form of this command. This option applies only to **raw-data**, **switch**, and **asp-drop** captures. This option is not supported when you use the **cluster exec capture** command.
reinject-hide	(Optional) Specifies that no reinjected packets will be captured. Applies only in a clustering environment.
stop	(Optional) Manually stops the capture without removing it. Use the **no** form of this command to start the capture.
tls-proxy	(Optional) Captures decrypted inbound and outbound data from TLS proxy on one or more interfaces.
trace *trace_count*	(Optional) Captures packet trace information, and the number of packets to capture. This option is used with an access list to insert trace packets into the data path to determine whether or not the packet has been processed as expected.
type	(Optional) Specifies the type of data captured.
user *webvpn-user*	(Optional) Specifies a username for a WebVPN capture.
webvpn	(Optional) Captures WebVPN data for a specific WebVPN connection.

Command Default

The defaults are as follows:

- The default **type** is **raw-data**
- The default buffer *size* is 512 KB .
- The default Ethernet type is IP packets.
- The default **packet-length** is 1518 bytes.
- The default **direction** is ingress.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
6.2(1)	This command was added.
7.0(1)	This command was modified to include the following keywords: **type asp-drop**, **type isakmp**, **type raw-data**, and **type webvpn**.
7.0(8)	Added the all option to capture all packets that the ASA drops.
7.2(1)	This command was modified to include the following options: **trace** *trace_count*, **match** *prot*, **real-time, host** *ip*, **any**, *mask*, and *operator.*
8.0(2)	This command was modified to update the path to capture contents.
8.4(1)	The new type keywords ikev1 and ikev2 were added.
8.4(2)	Additional detail was added to the output for IDS.
8.4(4.1)	The **asa_dataplane** option was added to support traffic over the backplane to the ASA CX module.
9.0(1)	The **cluster, cluster exec,** and **reinject-hide** keywords were added. The new **type** option **lacp** was added. Support for multiple-context mode was added for ISAKMP.

Release	Modification
9.1(3)	Supports filtering of packets captured on the ASA CX backplane with the **asa_dataplane** option.
9.2(1)	The **asa_dataplane** option was extended to support the ASA FirePOWER module.
9.3(1)	The **inline-tag** *tag* keyword-argument pair was added to support the SGT plus Ethernet Tagging feature.
9.6(2)	Packet capture of **type asp-drop** supports ACL and match filtering.
9.7(1)	Added the **stop** keyword to manually stop and start the packet capture.
9.8(1)	This command was updated to store the contents of all the active captures to files on flash or disks at the time of box crash.
9.9(1)	Support for capturing clustering persistent tracing and decrypted packets. New options were added: **persist** and **include-decrypted**. In addition, the **ethernet-type ipx** was removed, because IPX corresponds to 3 separate ethernet-types. Instead, use the hexadecimal value of the IPX type you want to capture.
9.10(1)	Added the any4 and any6 keywords for the **match** option to capture IPv4 and IPv6 network traffic respectively.
9.12(1)	Added **cp-cluster** to capture control packets on cluster interface.
9.18(1)	Included **real-time** keyword to enable real-time switch packet capture.
9.20(1)	The **direction** keyword was added to capture switch traffic that flows in **egress**, **ingress**, or **both** directions. This keyword is applicable only for Secure Firewall 4200 model devices.

Usage Guidelines

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. You can create multiple captures. The **capture** command is not saved to the running configuration, and is not copied to the standby unit during failover.

The ASA is capable of tracking all IP traffic that flows across it and of capturing all the IP traffic that is destined to it, including all the management traffic (such as SSH and Telnet traffic).

The ASA architecture consists of three different sets of processors for packet processing; this architecture poses certain restrictions on the capability of the capture feature. Typically most of the packet forwarding

functionality in the ASA is handled by the two front-end network processors, and packets are sent to the control-plane general-purpose processor only if they need application inspection. The packets are sent to the session management path network processor only if there is a session miss in the accelerated path processor.

Because all the packets that are forwarded or dropped by the ASA hits the two front-end network processors, the packet capture feature is implemented in these network processors. So all the packets that hit the ASA can be captured by these front end processors, if an appropriate capture is configured for those traffic interfaces. On the ingress side, the packets are captured the moment the packet hits the ASA interfaces, and on the egress side the packets are captured just before they are sent out on the wire.



Note Enabling WebVPN capture affects the performance of the ASA. Be sure to disable the capture after you generate the capture files that you need for troubleshooting.

Save the Capture

The contents of any active capture on ASA are saved when the box crashes.

When you activate captures as part of the troubleshooting process, you must note the following points:

- The size of capture buffer to use and if there is enough space on flash/disk.
- The capture buffer should be marked as circular for all the use cases, so that captured packets are the most recent before crash.

The name of the file for saving contents of an active capture is in the format of:

[<context_name>.]<capture_name>.pcap

The *context_name* indicates the name of the user context in which capture is activated in the multi-context mode. For the single context mode, the *context_name* is not applicable.

The *capture_name* indicates the name of the capture that is activated.

The capture save happens before the console or crash dump. This increases the crash downtime by about 5 seconds for a 33 MB capture buffer. The risk of a nested crash is minimal because copying the captured contents to a file is a simple process.

View the Capture

- To view the packet capture at the CLI, use the **show capture** *name* command.
- To save the capture to a file, use the **copy capture** command.
- To see the packet capture information with a web browser, use the **https://***ASA-ip-address***/admin/capture/***capture_name*[**/pcap**] command.

  You are prompted for a username and password. See the **username** command to add a username to the local database.

  If you specify the **pcap** keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)

If you copy the buffer contents to a TFTP server in ASCII format, you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and read it with TCPDUMP or Ethereal.

Stop and Start the Capture

The packets can be stopped from being captured without removing them from the buffer. The stopped status of the capture is displayed. The captured packet is retained in the buffer.

Use the following command to manually stop packet capture:

capture *name* **stop**

Use the following command to start capturing packets:

no capture *name* **stop**

Delete the Capture

Entering **no capture** without any keywords deletes the capture. To preserve the capture, specify the **access-list** or **interface** keyword; the capture is detached from the specified ACL or interface and the capture is preserved.

Real Time Operations

You cannot perform any operations on a capture while the real-time display is in progress. Using the **real-time** keyword with a slow console connection may result in an excessive number of non-displayed packets because of performance considerations. The fixed limit of the buffer is 1000 packets. If the buffer fills up, a counter is maintained of the captured packets. If you open another session, you can disable the real-time display be entering the **no capture real-time** command.

Clustering

You can precede the **capture** command with **cluster exec** to issue the **capture** command on one unit and run the command in all the other units at the same time. After you have performed cluster-wide capture, to copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the **cluster exec copy** command on the master unit.

```
ciscoasa# cluster exec capture
capture_name arguments
ciscoasa# cluster exec copy
 /pcap capture
: cap_name
 tftp
://location
/path
/filename
.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as filename_A.pcap, filename_B.pcap, and so on. In this example, A and B are cluster unit names.

When you capture traces on cluster units, they are persistent on each cluster node until you manually clear them from the buffer. Decrypted IPsec packets are captured once they enter ASA. The captured packet includes both normal and decapsulated traffic.

Note A different destination name is generated if you add the unit name at the end of the filename.

Limitations

The following are some of the limitations of the capture feature. Most of the limitations are caused by the distributed nature of the ASA architecture and by the hardware accelerators that are being used in the ASA.

- You can configure captures on the cluster control link within a context; only the packet that is associated with the context sent in the cluster control link is captured.
- For a shared VLAN, the following guidelines apply:
  - You can only configure one capture for the VLAN; if you configure a capture in multiple contexts on the shared VLAN, then only the last capture that was configured is used.
  - If you remove the last-configured (active) capture, no captures become active, even if you have previously configured a capture in another context; you must remove and readd the capture to make it active.
  - All traffic that enters the interface to which the capture is attached (and that matches the capture access list) is captured, including traffic to other contexts on the shared VLAN.
  - Therefore, if you enable a capture in Context A for a VLAN that is also used by Context B, both Context A and Context B ingress traffic are captured.
- For egress traffic, only the traffic of the context with the active capture is captured. The only exception is when you do not enable the ICMP inspection (therefore the ICMP traffic does not have a session in the accelerated path). In this case, both ingress and egress ICMP traffic for all contexts on the shared VLAN is captured.
- Configuring a capture typically involves configuring an access list that matches the traffic that needs to be captured. After an access list that matches the traffic pattern is configured, then you need to define a capture and associate this access list to the capture, along with the interface on which the capture needs to be configured. Note that a capture only works if an access list and an interface are associated with a capture for capturing IPv4 traffic. The access list is not required for IPv6 traffic.
- For the ASA CX module traffic, captured packets contain an additional AFBP header that your PCAP viewer might not understand; be sure to use the appropriate plugin to view these packets.
- For inline SGT tagged packets, captured packets contain an additional CMD header that your PCAP viewer might not understand.
- When performing a switch packet capture on Secure Firewall SGT-tagged packets are not captured if you apply a filter for SGT-tagged packets. However, SGT traffic can be captured on an interface if no filtering is applied.
- If there is no ingress interface and therefore no global interface, packets sent on the backplane are treated as control packets in the system context. These packets bypass the access list check and are always captured. This behavior applies in both single mode and multiple context mode.
- The **show capture** command shows the correct reason when capturing a specific asp-drop. However, the **show capture** command does not show the correct reason when capturing all asp-drops.
- The switch packet capture feature for Secure Firewall 6100 series has these limitations:
  - Egress capture supports 11 bytes of IPv6 source and destination address match.
  - The packet capture feature is not supported on the management port.
- The switch packet capture feature for Secure Firewall 4200 and Secure Firewall 6100 series has these limitations:

- The Marvell 98CX8540 switch used in 4200 and 6100 Series device has a hardware limitation. Due to this limitation IPv6 packets with extension headers cannot be captured using egress switch packet capture when filters are based on IP protocol or TCP/UDP port ranges.

  This is because the egress processing is unaware of the Layer 4 protocol type.

Examples

To capture a packet, enter the following command:

```
ciscoasa# capture captest interface inside
ciscoasa# capture captest interface outside
```

On a web browser, you can view the content of the **capture** command that was issued, named "captest," at the following location:

```
https://171.69.38.95/admin/capture/captest
```

To download a libpcap file (that web browsers use) to a local machine, enter the following command:

```
https://171.69.38.95/capture/http/pcap
```

The following example shows how to capture a packet in the single-mode when the ASA box crashes:

```
ciscoasa# capture 123 interface inside
```

The contents of capture '123' is saved as *123.pcap* file.

The following example shows how to capture a packet in the multi-mode when the ASA box crashes:

```
ciscoasa# capture 456 interface inside
```

The contents of capture '456' in 'admin' context is saved as *admin.456.pcap* file.

The following example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
ciscoasa# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
ciscoasa# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
ciscoasa# capture http access-list http packet-length 74 interface inside
```

The following example shows how to capture ARP packets:

```
ciscoasa# capture arp ethernet-type arp interface outside
```

The following example inserts five tracer packets into the data stream, where *access-list 101* defines traffic that matches TCP protocol FTP:

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

To view the traced packets and information about packet processing in an easily readable manner, use the **show capture ftptrace** command.

The following example shows how to display captured packets in real-time:

```
ciscoasa# capture test interface outside real-time
```

```
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.
10 packets displayed
12 packets not displayed due to performance limitations
```

The following example shows how to configure an extended access list that matches the IPv4 traffic that needs to be captured:

```
ciscoasa (config)# access-list capture extended permit ip any any
```

The following examples shows how to configure the capture:

```
ciscoasa (config)# capture name access-list acl_name interface interface_name
```

By default, configuring a capture creates a linear capture buffer of size 512 KB. You can optionally configure a circular buffer. By default, only 68 bytes of the packets are captured in the buffer. You can optionally change this value.

The following example creates a capture called “ip-capture” using the capture access list previously configured that is applied to the outside interface:

```
ciscoasa (config)# capture ip-capture access-list capture interface outside
```

The following example creates a capture called “switch-capture” on outside interface for Secure Firewall 3100:

```
ciscoasa (config)# capture switch-capture switch interface outside drop ?
exec mode commands/options:
  disable Disable capturing dropped packets from switch
  mac-filter To capture switch mac-filter drop
ciscoasa(config)# capture switch-capture switch interface outside drop mac-filter
```

The following example shows how to view the capture:

```
ciscoasa (config)# show capture name
```

The following example shows how to end the capture, but retain the buffer:

```
ciscoasa (config)# no capture name access-list acl_name interface interface_name
```

The following example shows how to end the capture and delete the buffer:

```
ciscoasa (config)# no capture name
```

The following example shows how to filter traffic captured on the backplane in single mode:

```
ciscoasa# capture x interface asa_dataplane access-list any4
ciscoasa# capture y interface asa_dataplane match ip any any
```



Note Control packets are captured in the single mode even though you have specified the access list.

The following examples show how to filter traffic captured on the backplane in multiple context mode:

Usage in user context:

```
ciscoasa (contextA)# capture x interface asa_dataplane access-list any4
ciscoasa (contextA)# capture y interface asa_dataplane match ip any any
```

Usage in system context:

```
ciscoasa# capture z interface asa_dataplane
```

Note In multiple context mode, the **access-list** and **match** options are not available in the system context.

Capture for Clustering

To enable capture on all units in the cluster, you can add the **cluster exec** keywords in front of each of these commands.

The following example shows how to create an LACP capture for the clustering environment:

```
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet0/0
```

The following example shows how to create a capture for control path packets in the clustering link:

```
ciscoasa (config)# cap cp interface cluster match udp any eq 49495 any
ciscoasa (config)# cap cp interface cluster match udp any any eq 49495
```

The following example shows how to create a capture for data path packets in the clustering link:

```
ciscoasa (config)# access-list ccl extended permit udp any any eq 4193
ciscoasa (config)# access-list ccl extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list ccl
```

The following example shows how to capture data path traffic through the cluster:

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match dup host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

The following example shows how to capture logical update messages for flows that match the real source to the real destination, and capture packets forwarded over CCL that match the real source to the real destination:

```
ciscoasa (config)# access-list dp permit
 real src real dst
```

The following example shows how to capture a certain type of data plane message, such as icmp echo request/response, that is forwarded from one ASA to another ASA using the **match** keyword or the access list for the message type:

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

The following example shows how to create a capture by using access list 103 on a cluster control link in a clustering environment:

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster
```

In the previous example, if A and B are IP addresses for the CCL interface, only the packets that are sent between these two units are captured.

If A and B are IP addresses for through-device traffic, then the following is true:

- Forwarded packets are captured as usual, provided the source and destination IP addresses are matched with the access list.
- The data path logic update message is captured provided it is for the flow between A and B or for an access list (for example, access-list 103). The capture matches the five-tuple of the embedded flow.
- Although the source and destination addresses in the UDP packet are CCL addresses, if this packet is to update a flow that is associated with addresses A and B, it is also captured. That is, as long as addresses A and B that are embedded in the packet are matched, it is also captured.

The following example shows how to configure capture with persistent option:

```
cluster2-asa5585a(config)# cluster exec capture test interface outside trace persist
  a(LOCAL):*************************************************************
  cluster2-asa5585a(config)#
```

Now, you can send some traffic.

```
cluster2-asa5585a(config)# cluster exec show packet-tracer

  a(LOCAL):*************************************************************
  tracer 29/25 (allocate/freed), handle 29/25 (allocated/freed), error 0
  =======  Tracer origin-id a:23, hop 0 =======
  packet-id: Protocol: 0 src-port: 0 dst-port: 0
  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: DROP
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  Action: drop
  Drop-reason: (l2_acl) FP L2 rule drop
```

The following example shows that, to free up some memory you must clear the captured persistent traces from the box.

```
ciscoasa# cluster exec clear packet-trace
```

The following example displays how to configure the capture with include-decrypted option:

```
  cluster2-asa5585a(config)# cluster exec show capture

  a(LOCAL):**********************************************************
  capture in type raw-data trace interface outside include-decrypted [Capturing – 588 bytes]

  capture out type raw-data trace interface outside include-decrypted [Capturing - 420
bytes]
  cluster2-asa5585a(config)#
```

Now, you can send some ICMP traffic through IPSec tunnel. The capture command obtains the decrypted ICMP packets as outlined:

```
  cluster2-asa5585a(config)# cluster exec show capture in | i icmp
  a(LOCAL):**********************************************************
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture out | i icmp
  a(LOCAL):**********************************************************
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture in | i icmp
  a(LOCAL):**********************************************************
     8: 07:22:57.065014       802.1Q vlan#212 P0 211.1.1.1 > 213.1.1.2: icmp: echo request

  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture out | i icmp
  a(LOCAL):**********************************************************
    10: 07:22:57.068004       802.1Q vlan#214 P0 213.1.1.2 > 211.1.1.1: icmp: echo reply
  b:**********************************************************************
  cluster2-asa5585a(config)#
```

The following example shows how to create and start an egress traffic capture for a switch:

```
ciscoasa(config)# capture switch_cap switch interface gigabitEthernet0/0 direction ?
exec mode commands/options:
  both     To capture switch bi-directional traffic
  egress   To capture switch egressing traffic
  ingress  To capture switch ingressing traffic

ciscoasa(config)# capture switch_cap switch interface gigabitEthernet0/0 direction egress
ciscoasa(config)# no capture switch_cap switch stop
```

If you want to capture packets where the accelerated security path (ASP) drop reason is dispatch-queue-limit, you need to enable debug to delay the packet drops. Otherwise, the packets have been dropped and they cannot be captured. If you have used **show asp drop** command and see that dispatch queue tail drops (dispatch-queue-limit) are increasing, enable debug on asp 38 before performing the capture. Do the following:

```
(Enable delayed drop for 20 packets. You can specify 0-100.
When the delayed drop count hits zero, the delayed drop
behavior stops automatically. You can see how many drops
are still available using debug menu asp 38 with no number)

ciscoasa(config)# debug menu asp 38 20

(Start the capture)

ciscoasa(config)# capture drop type asp-drop dispatch-queue-limit

(Generate the traffic that has been causing the drops, then view the capture.)
```

```
ciscoasa(config)# show capture drop
```

Related Commands

Command	Description
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.
show capture	Displays the capture configuration when no options are specified.

cd

To change the current working directory to the one specified, use the **cd** command in privileged EXEC mode.

cd [**disk0:** | **disk1:** | **flash:**] [*path* **]**

Syntax Description

disk0:	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the removable, external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
path	(Optional) The absolute path of the directory to change to.

Command Default

If you do not specify a directory, the directory is changed to the root directory.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to change to the “config” directory:

```
ciscoasa# cd flash:/config/
```

Related Commands

Command	Description
pwd	Displays the current working directory.

cdp-url

To specify the CDP to be included in certificates issued by the local CA, use the **cdp-url** command in ca server configuration mode. To revert to the default CDP, use the **no** form of this command.

[**no**] **cdp-url** *url*

Syntax Description

url Specifies the URL where a validating party obtains revocation status for certificates issued by the local CA. The URL must be less than 500 alphanumeric characters.

Note
ASA supports both IPv4 and IPv6 CDP URLs. Enclose IPv6 addresses in square brackets, for example: *http://[0:0:0:0:0.18:0a01:7c16]*.

Command Default

(For ASA versions 9.12(1) and earlier) The default CDP URL is that of the ASA that includes the local CA. The default URL is in the format: http://hostname.domain/+CSCOCA+/asa_ca.crl.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.20(1)	Support for IPv6 CDP URL was added.

Usage Guidelines

The CDP is an extension that can be included in issued certificates to specify the location where a validating party can obtain revocation status for the certificate. Only one CDP can be configured at a time.

Note If a CDP URL is specified, it is the responsibility of the administrator to maintain access to the current CRL from that location.

Examples

The following example (applicable only for ASA versions 9.12(1) and earlier) configures a CDP at 10.10.10.12 for certificates issued by the local CA server:

```
ciscoasa(config)# crypto ca server
ciscoasa
```

```
(config-ca-server)
# cdp-url http://10.10.10.12/ca/crl
ciscoasa
(config-ca-server)
#
```

The following example configures a CDP IPv6 url:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# cdp-url http://[0:0:0:0:0:ffff:0a01:7c16]
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to ca server configuration mode CLI command set, which allows you to configure and manage a local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by a local CA server as revoked in the certificate database and CRL.
crypto ca server unrevoke	Unrevokes a previously revoked certificate issued by a local CA server.
lifetime crl	Specifies the lifetime of the certificate revocation list.

certificate

To add the indicated certificate, use the **certificate** command in crypto ca certificate chain configuration mode. To delete the certificate, use the **no** form of this command.

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*
no certificate *certificate-serial-number*

Syntax Description

ca	Indicates that the certificate is a CA issuing certificate.
certificate-serial-number	Specifies the serial number of the certificate in hexadecimal format ending with the word "quit."
ra-encrypt	Indicates that the certificate is an RA key encipherment certificate used in SCEP.
ra-general	Indicates that the certificate is an RA certificate used for digital signing and key encipherment in SCEP messaging.
ra-sign	Indicates that the certificate is an RA digital signature certificate used in SCEP messaging.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca certificate chain configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When this command is issued, the ASA interprets the data included with it as the certificate in hexadecimal format. A **quit** string indicates the end of the certificate.

A CA is an authority in a network that issues and manages security credentials and public key for message encryption. As part of a public key infrastructure, a CA checks with a RA to verify information provided by the requester of a digital certificate. If the RA verifies the requester information, the CA can then issue a certificate.

Examples

The following example adds a CA certificate with the serial number 29573D5FF010FE25B45:

```
ciscoasa
(config)#
crypto ca trustpoint central
ciscoasa
(ca-trustpoint)#
crypto ca certificate chain central
ciscoasa
(ca-cert-chain)#
certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
crypto ca certificate chain	Enters certificate crypto ca certificate chain mode.
crypto ca trustpoint	Enters ca trustpoint mode.
show running-config crypto map	Displays all configuration for all the crypto maps.

certificate-group-map

To associate a rule entry from a certificate map with a tunnel group, use the **certificate-group-map** command in webvpn configuration mode. To clear current tunnel-group map associations, use the **no** form of this command.

certificate-group-map *certificate_map_name index tunnel_group_name*
no certificate-group-map

Syntax Description

certificate_map_name	The name of a certificate map.
index	The numeric identifier for a map entry in the certificate map. The index value can be in the range of 1-65535.
tunnel_group_name	The name of the tunnel group chosen if the map entry matches the certificate. The *tunnel-group name* must already exist.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

With the **certificate-group-map** command in effect, if a certificate received from a WebVPN client corresponds to a map entry, the resulting tunnel group is associated with the connection, overriding any tunnel group choice made by the user.

Multiple instances of the **certificate-group-map** command allow multiple mappings.

Examples

The following example shows how to associate rule 6 for a tunnel group named tgl:

ciscoasa (config)# webvpn

```
hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters ca certificate map configuration mode for configuring rules based on the certificate issuer and subject distinguished names (DNs).
tunnel-group-map	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups.

chain

To enable sending a certificate chain, use the **chain** command in tunnel-group ipsec-attributes configuration mode. To return this command to the default, use the **no** form of this command.

chain
no chain

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can apply this attribute to all IPsec tunnel group types.

Entering this command includes the root certificate and any subordinate CA certificates in the transmission.

Examples

The following example entered in tunnel-group-ipsec attributes configuration mode, enables sending a chain for an IPSec LAN-to-LAN tunnel group with the IP address of 209.165.200.225, which includes the root certificate and any subordinate CA certificates:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# chain
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the current tunnel group configuration.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

change-password

To enable users to change their own account passwords, use the **change-password** command in privileged EXEC mode.

change-password [**/silent**] [**old-password** *old-password* [**new-password** *new-password*]]

Syntax Description

new-password *new-password*	Specifies the new password.
old-password *old-password*	Reauthenticates the user.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	—	• Yes
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(4.1)	This command was added.

Usage Guidelines

If users omit the passwords, the ASA prompts them for input. When users enter the **change-password** command, they are asked to save their running configuration. After a user has successfully changed the password, a message appears to remind the user to save configuration changes.

Examples

The following example changes a user account password:

```
ciscoasa# change-password old-password
myoldpassword000
 new password
mynewpassword123
```

Related Commands

Command	Description
show run password-policy	Shows the password policy for the current context.
clear configure password-policy	Resets password policy for the current context to the default value.

Command	Description
clear configure username	Removes a username from a user account.

changeto

To change between security contexts and the system, use the **changeto** command in privileged EXEC mode.

changeto { **system** | **context** *name* }

Syntax Description

context *name*	Changes to the context with the specified name.
system	Changes to the system execution space.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you log into the system execution space or the admin context, you can change between contexts and perform configuration and monitoring tasks within each context. The "running" configuration that you edit in configuration mode, or that is used in the **copy** or **write** commands, depends on which execution space you are in. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context execution space, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) by entering the **show running-config** command. Only the current configuration appears.

Examples

The following example changes between contexts and the system in privileged EXEC mode:

```
ciscoasa/admin# changeto system
ciscoasa# changeto context customerA
ciscoasa/customerA#
```

The following example changes between the system and the admin context in interface configuration mode. When you change between execution spaces, and you are in a configuration mode, the mode changes to the global configuration mode in the new execution space.

```
ciscoasa(config-if)# changeto context admin
ciscoasa/admin(config)#
```

Related Commands

Command	Description
admin-context	Sets a context to be the admin context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

channel-group

To assign a physical interface to an EtherChannel, use the **channel-group** command in interface configuration mode. To unassaign the interface, use the **no** form of this command.

channel-group *channel_id* **mode** { **active** | **passive** | **on** } [**vss-id** { **1** | **2** }]
no channel-group *channel_id*

Syntax Description

channel_id	Specifies the EtherChannel to which you want to assign this interface, between 1 and 48.
vss-id {**1** | **2**}	(Optional) With clustering, if you are connecting the ASA to two switches in a VSS or vPC, then configure the **vss-id** keyword to identify to which switch this interface is connected (1 or 2). You must also use the **port-channel span-cluster vss-load-balance** command for the port-channel interface.
mode {**active** | **passive** | **on**}	You can configure each physical interface in an EtherChannel to be: • Active—Sends and receives Link Aggregation Control Protocol (LACP) updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic. • Passive—Receives LACP updates. A passive EtherChannel can only establish connectivity with an active EtherChannel. • On—The EtherChannel is always on, and LACP is not used. An "on" EtherChannel can only establish a connection with another "on" EtherChannel.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	We added this command.
9.0(1)	We added the **vss-id** keyword to support ASA clustering and spanned EtherChannels.

Usage Guidelines

Each channel group can have eight active interfaces. Note that you can assign up to 16 interfaces to a channel group. While only eight interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

If the port-channel interface for this channel ID does not yet exist in the configuration, one will be added:

```
interface port-channel
 channel_id
```

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices. LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

ASA Clustering

You can include multiple interfaces per ASA in a spanned EtherChannel. Multiple interfaces per ASA are especially useful for connecting to both switches in a VSS or vPC. If you are connecting the ASA to two switches in a VSS or vPC, then you should enable VSS load balancing by using the **vss-load-balance** keyword. This feature ensures that the physical link connections between the ASAs to the VSS (or vPC) pair are balanced. You must configure the **vss-id** keyword in the **channel-group** command for each member interface before enabling load balancing.

Examples

The following example assigns interfaces to channel group 1:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# channel-group 1 mode passive
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

character-encoding

To specify the global character encoding in WebVPN portal pages, use the **character-encoding** command in webvpn configuration mode. To remove the value of the character-encoding attribute, use the **no** form of this command.

character-encoding *charset*
no character-encoding *charset*

Syntax Description

charset String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets . You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850.

The string is case-insensitive. The command interpreter converts upper case to lower case in the ASA configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Character encoding , also called “character coding” and “a character set,” is the pairing of raw data (such as 0s and 1s) and characters to represent the data. The language determines the character encoding method to use. Some languages use the same method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the user can change this. The browser can also detect the encoding specified on the page, and render the document accordingly. The character-encoding attribute lets the user specify the value of the character-encoding method into the WebVPN portal page to ensure that the browser renders it correctly, regardless of the region in which the user is using the browser, or any changes made to the browser.

The character-encoding attribute is a global setting that, by default, all WebVPN portal pages inherit. However, the user can override the file-encoding attribute for Common Internet File System (CIFS) servers that use character encoding that differs from the value of the character-encoding attribute. Use different file-encoding values for CIFS servers that require different character encodings.

The WebVPN portal pages downloaded from the CIFS server to the WebVPN user encode the value of the WebVPN file-encoding attribute identifying the server, or if one does not, they inherit the value of the

character-encoding attribute. The remote user browser maps this value to an entry in its character encoding set to determine the proper character set to use. The WebVPN portal pages do not specify a value if WebVPN configuration does not specify a file-encoding entry for the CIFS server and the character-encoding attribute is not set. The remote browser uses its own default encoding if the WebVPN portal page does not specify the character encoding or if it specifies a character encoding value that the browser does not support.

The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the correct rendering of file names or directory paths, as well as pages, is an issue.



Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. The user needs to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

The encoding type set on the remote browser determines the character set for WebVPN portal pages when this attribute does not have a value.

Examples

The following example sets the character-encoding attribute to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# character-encoding shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

Related Commands

Command	Description
debug webvpn cifs	Displays debugging messages about the CIFS server.
file-encoding	Specifies CIFS servers and associated character encoding to override the value of this attribute.
show running-config [**all**] webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.

checkheaps

To configure checkheaps verification intervals, use the **checkheaps** command in global configuration mode. To set the value to the default, use the **no** form of this command.

checkheaps { **check-interval** | **validate-checksum** } *seconds*
no checkheaps { **check-interval** | **validate-checksum** } [*seconds*]

Syntax Description

check-interval	Sets the buffer verification interval. The buffer verification process checks the sanity of the heap (allocated and freed memory buffers). During each invocation of the process, the ASA checks the entire heap, validating each memory buffer. If there is a discrepancy, the ASA issues either an "allocated buffer error" or a "free buffer error." If there is an error, the ASA dumps traceback information when possible and reloads.
seconds	Sets the interval in seconds between 1 and 2147483.
validate-checksum	Sets the code space checksum validation interval. When the ASA first boots up, the ASA calculates a hash of the entire code. Later, during the periodic check, the ASA generates a new hash and compares it to the original. If there is a mismatch, the ASA issues a "text checksum checkheaps error." If there is an error, the ASA dumps traceback information when possible and reloads.

Command Default

The default intervals are 60 seconds each.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

Examples

The following example sets the buffer allocation interval to 200 seconds and the code space checksum interval to 500 seconds:

```
ciscoasa(config)# checkheaps check-interval 200
ciscoasa(config)# checkheaps validate-checksum 500
```

Related Commands

Command	Description
show checkheaps	Shows checkheaps statistics.

check-retransmission

To prevent against TCP retransmission style attacks, use the **check-retransmission** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

check-retransmission
no check-retransmission

Syntax Description

This command has no arguments or keywords.

Command Default

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. To prevent against TCP retransmission style attacks that arise from end-system interpretation of inconsistent retransmissions, use the **check-retransmission** command in tcp-map configuration mode.

The ASA will make efforts to verify if the data in retransmits are the same as the original. If the data does not match, then the connection is dropped by the ASA. When this feature is enabled, packets on the TCP connection are only allowed in order. For more details, see the **queue-limit** command.

Examples

The following example enables the TCP check-retransmission feature on all TCP flows:

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# check-retransmission
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

checksum-verification

To enable or disable TCP checksum verification, use the **checksum-verification** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

checksum-verification
no checksum-verification

Syntax Description

This command has no arguments or keywords.

Command Default

Checksum verification is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **checksum-verification** command in tcp-map configuration mode to enable TCP checksum verification. If the check fails, the packet is dropped.

Examples

The following example enables TCP checksum verification on TCP connections from 10.0.0.0 to 20.0.0.0:

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0 255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# checksum-verification
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

checksum-verification

To enable or disable TCP checksum verification, use the **checksum-verification** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

checksum-verification
no checksum-verification

Syntax Description

This command has no arguments or keywords.

Command Default

Checksum verification is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **checksum-verification** command in tcp-map configuration mode to enable TCP checksum verification. If the check fails, the packet is dropped.

Examples

The following example enables TCP checksum verification on TCP connections from 10.0.0.0 to 20.0.0.0:

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0 255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# checksum-verification
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

cipc security-mode authenticated (Deprecated)

To force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario, use the **cipc security-mode authenticated** command in phone-proxy configuration mode. To turn off this command when CIPC softphones support encryption, use the **no** form of this command.

cipc security-mode authenticated
no cipc security-mode authenticated

Syntax Description

This command has no arguments or keywords.

Command Default

Be default, this command is disabled via the no form of the command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

Separating voice and data traffic by using VLANs is a security best practice to hide voice streams from security threats that attempt to penetrate the data VLAN. However, Cisco IP Communicator (CIPC) softphone applications must connect to their respective IP phones, which reside on the voice VLAN. This requirement makes segregating voice and data VLANs an issue because the SIP and SCCP protocols dynamically negotiate the RTP/RTCP ports on a wide range of ports. This dynamic negotiation requires that a range of ports be open between the two VLANs.

Note Earlier versions of CIPC that do not support Authenticated mode are not supported with the Phone Proxy.

To allow CIPC softphones on the data VLAN to connect to their respective IP phones on the voice VLAN without requiring access between the VLANs on a wide range of ports, you can configure the Phone Proxy with the **cipc security-mode authenticated** command.

This command allows the Phone Proxy to look for CIPC configuration files and force CIPC softphones to be in authenticated mode rather than encrypted mode, because current versions of CIPC do not support encrypted mode.

When this command is enabled, the Phone Proxy parses the phones configuration file to determine if the phone is a CIPC softphone and changes the security mode to authenticated. Additionally, CIPC softphones support authenticated mode only while the Phone Proxy, by default, forces all phones to be in encrypted mode.

Examples

The following example shows the use of the **cipc security-mode authenticated** command to force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario:

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)#cipc security-mode authenticated
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

clacp static-port-priority

To disable dynamic port priority in LACP for a clustering spanned EtherChannel, which is required for more than 8 active EtherChannel members, use the **clacp static-port-priority** command in global configuration mode. To enable dynamic port priority, use the **no** form of this command.

Note Supported on ASA hardware models only.

clacp static-port-priority
no clacp static-port-priority

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default; dynamic port priority is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.2(1)	We added this command.

Usage Guidelines

Some switches do not support dynamic port priority, so this command improves switch compatibility. Moreover, it enables support of more than 8 active spanned EtherChannel members, up to 32 members. Without this command, only 8 active members and 8 standby members are supported.

ASA EtherChannels support up to 16 active links. With *spanned* EtherChannels, that functionality is extended to support up to 32 active links across the cluster when used with two switches in a vPC and when you disable dynamic port priority with the **clacp static-port-priority** command. The switches must support EtherChannels with 16 active links, for example, the Nexus 7000 with with F2-Series 10 Gigabit Ethernet Module.

For switches in a VSS or vPC that support 8 active links, you can configure 16 active links in the spanned EtherChannel (8 connected to each switch).

Note If you want to use more than 8 active links in a spanned EtherChannel, you cannot also have standby links; the support for 9 to 32 active links requires you to disable cLACP dynamic port priority that allows the use of standby links.

Examples

The following example disables dynamic port priority:

```
ciscoasa(config)# clacp static-port-priority
```

Related Commands

Command	Description
clacp system-mac	Sets the cLACP system ID.

clacp system-mac

To manually configure the cLACP system ID on the master unit in an ASA cluster, use the **clacp system-mac** command in cluster group configuration mode. To retsore the default setting, use the **no** form of this command.

clacp system-mac { *mac_address* | **auto** } [**system-priority** *number*]
no clacp system-mac { *mac_address* | **auto** } [**system-priority** *number*]

Syntax Description

mac_address	Manually sets the system ID in the form *H .H .H* , where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0A-00-00-AA-AA is entered as 000A.0000.AAAA.
auto	Auto-generates the system ID.
system-priority *number*	Sets the system priority, between 1 and 65535. The priority is used to decide which unit is in charge of making a bundling decision. By default, the ASA uses priority 1, which is the highest priority. The priority needs to be higher than the priority on the switch.

Command Default

By default, the system-mac is auto-generated (**auto**).

By default, the system-priority is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	We added this command.

Usage Guidelines

When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch. ASAs in a cluster collaborate in cLACP negotiation so that they appear as a single (virtual) device to the switch. One parameter in cLACP negotiation is a system ID, which is in the format of a MAC address. All ASAs use the same system ID: auto-generated by the master unit (the default) and replicated to all slaves; or manually specified in this command. You might want to manually configure the MAC address for troubleshooting purposes, for example, so you can use an easily identified MAC address. Typically, you would use the auto-generated MAC address.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units. However, you cannot change this value after you enable clustering.

Examples

The following example manually configures a system ID:

```
cluster group pod1
local-unit unit1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
health-check
clacp system-mac 000a.0000.aaaa
enable noconfirm
```

Related Commands

Command	Description
cluster group	Configures cluster parameters.

class (global)

To create a resource class to which to assign a security context, use the **class** command in global configuration mode. To remove a class, use the **no** form of this command.

class *name*
no class *name*

Syntax Description

name Specifies the name as a string up to 20 characters long. To set the limits for the default class, enter **default** for the name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the ASA, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.

The ASA manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

When you create a class, the ASA does not set aside a portion of the resources for each context assigned to the class; rather, the ASA sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can "use up" those resources, potentially affecting service to other contexts. See the **limit-resource** command to set the resources for the class.

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a 2 percent limit for all concurrent connections, but no other limits, then all other limits are inherited from the default class. Conversely, if you create a class with limits for all resources, the class uses no settings from the default class.

By default, the default class provides unlimited access to resources for all contexts, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions—5 sessions.
- SSH sessions—5 sessions.
- MAC addresses—65,535 entries.

Examples

The following example sets the default class limit for conns to 10 percent instead of unlimited:

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

All other resources remain at unlimited.

To add a class called gold, enter the following commands:

```
ciscoasa(config)# class gold
ciscoasa(config-class)#
limit-resource mac-addresses 10000
ciscoasa(config-class)#
limit-resource conns 15%
ciscoasa(config-class)#
limit-resource rate conns 1000
ciscoasa(config-class)#
limit-resource rate inspects 500
ciscoasa(config-class)#
limit-resource hosts 9000
ciscoasa(config-class)#
limit-resource asdm 5
ciscoasa(config-class)#
limit-resource ssh 5
ciscoasa(config-class)#
limit-resource rate syslogs 5000
ciscoasa(config-class)#
limit-resource telnet 5
ciscoasa(config-class)#
limit-resource xlates 36000
ciscoasa(config-class)#
limit-resource routes 5000
```

Related Commands

Command	Description
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.
show class	Shows the contexts assigned to a class.

class (policy-map)

To assign a class map to a policy map where you can assign actions to the class map traffic, use the **class** command in policy-map configuration mode. To remove a class map from a policy map, use the **no** form of this command.

class *classmap_name*
no class *classmap_name*

Syntax Description

classmap_name	Specifies the name for the class map. For a Layer 3/4 policy map (the **policy-map** command), you must specify a Layer 3/4 class map name (the **class-map** or **class-map type management** command). For an inspection policy map (the **policy-map type inspect** command), you must specify an inspection class map name (the **class-map type inspect** command).

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To use the **class** command, use the Modular Policy Framework. To use a class in a Layer 3/4 policy map, enter the following commands:

1. **class-map**—Identify the traffic on which you want to perform actions.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. *commands for supported features* —For a given class map, you can configure many actions for various features, including QoS, application inspection, CSC or AIP SSM, TCP and UDP connections limits and timeout, and TCP normalization. See the CLI configuration guide for more details about the commands available for each feature.
3. **service-policy**—Assigns the policy map to an interface or globally.

To use a class in an inspection policy map, enter the following commands:

1. **class-map type inspect**—Identify the traffic on which you want to perform actions.
2. **policy-map type inspect**—Identify the actions associated with each class map.
   a. **class**—Identify the inspection class map on which you want to perform actions.
   b. *commands for application types* —See the CLI configuration guide for commands available for each application type. Actions supported in class configuration mode of an inspection policy map include:
   c. Dropping a packet
   d. Dropping a connection
   e. Resetting a connection
   f. Logging
   g. Rate-limiting of messages
   h. Masking content
   i. **parameters**—Configure parameters that affect the inspection engine. The CLI enters parameters configuration mode. See the CLI configuration guide for available commands.
3. **class-map**—Identify the traffic on which you want to perform actions.
4. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the Layer 3/4 class map on which you want to perform actions.
   b. **inspect** *application inspect_policy_map* —Enables application inspection, and calls an inspection policy map to perform special actions.
5. **service-policy**—Assigns the policy map to an interface or globally.

The configuration always includes a class map called **class-default** that matches all traffic. At the end of every Layer 3/4 policy map, the configuration includes the **class-default** class map with no actions defined. You can optionally use this class map when you want to match all traffic, and do not want to bother creating another class map. In fact, some features are only configurable for the **class-default** class map, such as the **shape** command.

Including the **class-default** class map, up to 63 **class** and **match** commands can be configured in a policy map.

Examples

The following is an example of a **policy-map** command for connection policy that includes the **class** command. It limits the number of connections allowed to the web server 10.1.1.1:

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

The following example shows how multi-match works in a policy map:

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

When a Telnet connection is initiated, it matches **class telnet_traffic**. Similarly, if an FTP connection is initiated, it matches **class ftp_traffic**. For any TCP connection other than Telnet and FTP, it will match **class tcp_traffic**. Even though a Telnet or FTP connection can match **class tcp_traffic**, the ASA does not make this match because they previously matched other classes.

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
class-map type management	Creates a Layer 3/4 class map for management traffic.
clear configure policy-map	Removes all policy map configuration, except for any policy map that is in use in a **service-policy** command.
match	Defines the traffic-matching parameters.
policy-map	Configures a policy; that is, an association of one or more traffic classes, each with one or more actions.

class-map

When using the Modular Policy Framework, identify Layer 3 or 4 traffic to which you want to apply actions by using the **class-map** command (without the **type** keyword) in global configuration mode. To delete a class map, use the **no** form of this command.

class-map *class_map_name*
no class-map *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This type of class map is for Layer 3/4 through traffic only. For management traffic destined to the ASA, see the **class-map type management** command.

A Layer 3/4 class map identifies Layer 3 and 4 traffic to which you want to apply actions. You can create multiple Layer 3/4 class maps for each Layer 3/4 policy map.

Default Class Maps

The configuration includes a default Layer 3/4 class map that the ASA uses in the default global policy. It is called **inspection_default** and matches the default inspection traffic:

```
class-map inspection_default
 match default-inspection-traffic
```

Another class map that exists in the default configuration is called class-default, and it matches all traffic:

```
class-map class-default
 match any
```

This class map appears at the end of all Layer 3/4 policy maps and essentially tells the ASA to not perform any actions on all other traffic. You can use the class-default class map if desired, rather than making your own **match any** class map. In fact, some features are only available for class-default, such as QoS traffic shaping.

Maximum Class Maps

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types.

Configuration Overview

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Use the **class-map** command to enter class-map configuration mode. From class-map configuration mode, you can define the traffic to include in the class using the **match** command. A Layer 3/4 class map contains, at most, one **match** command (with the exception of the **matchtunnel-group** and **matchdefault-inspection-traffic** commands) that identifies the traffic included in the class map.

Examples

The following example creates four Layer 3/4 class maps:

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255
ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp
ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp
ciscoasa(config-cmap)# class-map all_http
ciscoasa(config-cmap)# description "This class-map matches all HTTP traffic"
ciscoasa(config-cmap)# match port tcp eq http
ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

Related Commands

Command	Description
class-map type management	Creates a class map for traffic to the ASA.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type inspect

When using the Modular Policy Framework, match criteria that is specific to an inspection application by using the **class-map type inspect** command in global configuration mode. To delete an inspection class map, use the **no** form of this command.

class-map type inspect *application* [**match-all** | **match-any**] *class_map_name*
class-map [**type inspect** *application* [**match-all** | **match-any**]] *class_map_name*

Syntax Description

application	Specifies the type of application traffic you want to match. Available types include: • **dcerpc** • **diameter** • **dns** • **ftp** • **h323** • **http** • **im** • **rtsp** • **scansafe** • **sip**
class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.
match-all	(Optional) Specifies that traffic must match all criteria to match the class map. **match-all** is the default if you do not specify an option.
match-any	(Optional) Specifies that traffic can match one or more criteria to match the class map.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The **match-any** keyword was added.
9.0(1)	The **scansafe** keyword was added.
9.5(2)	The **dcerpc** and **diameter** keywords were added.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the Layer 3/4 policy map, you can also optionally enable actions as defined in an *inspection policy map* (see the **policy-map type inspect** command).

In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map. The class map contains one or more **match** commands. (You can alternatively use **match** commands directly in the inspection policy map if you want to pair a single criterion with an action). You can match criteria that is specific to an application. For example, for DNS traffic, you can match the domain name in a DNS query.

A class map groups multiple traffic matches (in a match-all class map), or lets you match any of a list of matches (in a match-any class map). The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you group multiple match commands, and you can reuse class maps. For the traffic that you identify in this class map, you can specify actions such as dropping, resetting, and/or logging the connection in the inspection policy map.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates an HTTP class map that must match all criteria:

```
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
```

```
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
```

The following example creates an HTTP class map that can match any of the criteria:

```
ciscoasa(config-cmap)# class-map type inspect http match-any monitor-http
ciscoasa(config-cmap)# match request method get
ciscoasa(config-cmap)# match request method put
ciscoasa(config-cmap)# match request method post
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map for through traffic.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type management

When using the Modular Policy Framework, identify Layer 3 or 4 management traffic destined for the ASA to which you want to apply actions by using the **class-map type management** command in global configuration mode. To delete a class map, use the **no** form of this command.

class-map type management *class_map_name*
no class-map type management *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The s**et connection** command is now available for a Layer 3/4 management class map, for to-the-ASA management traffic. Only the **conn-max** and **embryonic-conn-max** keywords are available.

Usage Guidelines

This type of class map is for management traffic only. For through traffic, see the **class-map** command (without the **type** keyword).

For management traffic to the ASA, you might want to perform actions specific to this kind of traffic. The types of actions available for a management class map in the policy map are specialized for management traffic. For example, this type of class map lets you inspect RADIUS accounting traffic and set connection limits.

A Layer 3/4 class map identifies Layer 3 and 4 traffic to which you want to apply actions. The maximum number of class maps of all types is 255 in single mode or per context in multiple mode.

You can create multiple Layer 3/4 class maps (management or through traffic) for each Layer 3/4 policy map.

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** and **class-map type management** commands.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Use the **class-map type management** command to enter class-map configuration mode. From class-map configuration mode, you can define the traffic to include in the class using the **match** command. You can specify a management class map that can match an access list or TCP or UDP ports. A Layer 3/4 class map contains, at most, one **match** command that identifies the traffic included in the class map.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates a Layer 3/4 management class map:

```
ciscoasa(config)# class-map type management radius_acct
ciscoasa(config-cmap)# match port tcp eq 10000
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map for through traffic.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type regex

When using the Modular Policy Framework, group regular expressions for use with matching text by using the **class-map type regex** command in global configuration mode. To delete a regular expression class map, use the **no** form of this command.

class-map type managementclass_map_name *class_map_name*
no class-map [**type regex match-any**] *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.
match-any	Specifies that the traffic matches the class map if it matches only one of the regular expressions. **match-any** is the only option.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the Layer 3/4 policy map, you can also optionally enable actions as defined in an *inspection policy map* (see the **policy-map type inspect** command).

In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map containing one or more **match** commands or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression; for example, you can match URL strings inside HTTP packets. You can group regular expressions in a regular expression class map.

Before you create a regular expression class map, create the regular expressions using the **regex** command. Then, identify the named regular expressions in class-map configuration mode using the **match regex** command.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates two regular expressions, and adds them to a regular expression class map. Traffic matches the class map if it includes the string “example.com” or “example2.com.”

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match
 regex
 url_example
ciscoasa(config-cmap)# match
 regex
 url_example2
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
regex	Creates a regular expression.



clear a – clear k

- clear aaa kerberos, on page 563
- clear aaa local user, on page 565
- clear aaa sdi node-secret, on page 567
- clear aaa-server statistics, on page 568
- clear access-list, on page 570
- clear arp, on page 572
- clear asp, on page 573
- clear avc, on page 575
- clear bfd counters, on page 576
- clear bgp, on page 578
- clear blocks, on page 581
- clear-button, on page 582
- clear capture, on page 584
- clear clns cache, on page 585
- clear clns is-neighbors, on page 586
- clear clns neighbors, on page 587
- clear clns route, on page 588
- clear cluster info, on page 589
- clear compression, on page 590
- clear configuration session, on page 591
- clear configure, on page 592
- clear conn, on page 594
- clear console-output, on page 597
- clear coredump, on page 598
- clear counters, on page 599
- clear cpu profile, on page 601
- clear crashinfo, on page 602
- clear crypto accelerator statistics, on page 603
- clear crypto ca crls, on page 604
- clear crypto ca trustpool, on page 605
- clear crypto ikev1, on page 606
- clear crypto ikev2, on page 608
- clear crypto ipsec sa, on page 610

- clear crypto ipsec stats, on page 612
- clear crypto isakmp, on page 613
- clear crypto protocol statistics, on page 614
- clear crypto ssl, on page 616
- clear cts, on page 617
- clear dhcpd, on page 619
- clear dhcprelay statistics, on page 620
- clear dns, on page 621
- clear dns-hosts cache, on page 623
- clear dynamic-filter dns-snoop, on page 624
- clear dynamic-filter reports, on page 626
- clear dynamic-filter statistics, on page 629
- clear eigrp events, on page 631
- clear eigrp neighbors, on page 632
- clear eigrp topology, on page 634
- clear facility-alarm output, on page 635
- clear failover statistics, on page 637
- clear flow-export counters, on page 638
- clear flow-offload, on page 639
- clear flow-offload-ipsec, on page 640
- clear fragment, on page 641
- clear gc, on page 643
- clear igmp counters, on page 644
- clear igmp group, on page 645
- clear igmp traffic, on page 646
- clear ikev1, on page 647
- clear ikev2, on page 649
- clear interface, on page 651
- clear ip audit count, on page 653
- clear ipsec sa, on page 654
- clear ipsec stats, on page 656
- clear ipv6 access-list counters (Deprecated), on page 657
- clear ipv6 dhcprelay, on page 658
- clear ipv6 dhcp statistics, on page 659
- clear ipv6 eigrp, on page 662
- clear ipv6 router eigrp, on page 663
- clear ipv6 mld traffic, on page 664
- clear ipv6 neighbors, on page 665
- clear ipv6 ospf, on page 666
- clear ipv6 prefix-list, on page 668
- clear ipv6 route, on page 669
- clear ipv6 traffic, on page 670
- clear ip verify statistics, on page 672
- clear isakmp sa, on page 673
- clear isis, on page 674

clear aaa kerberos

To clear Kerberos information, use the **clear aaa kerberos** command in privileged EXEC mode.

clear aaa kerberos { **tickets** [**username** *user*] | **keytab** }

Syntax Description

keytab	Clears the Kerberos keytab file.
tickets [**username** *user*]	Clears Kerberos ticket information. All tickets are cleared unless you include the username keyword, which specifies the user whose ticket you want to clear.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.8(4)	The **keytab** keyword was added.

Examples

The following example shows how to clear all Kerberos tickets.

```
ciscoasa# clear aaa kerberos tickets

Proceed with deleting kerberos tickets? [confirm] y
```

The following example shows how to display, and then clear, the Kerberos keytab file.

```
ciscoasa# show aaa kerberos keytab

Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
ciscoasa# clear aaa kerberos keytab

ciscoasa# show aaa kerberos keytab

No keys found
ciscoasa#
```

Related Commands

Command	Description
show aaa kerberos	Displays all the Kerberos tickets cached on the system, or the keytab file.

clear aaa local user

To unlock a user, or to reset a user's failed authentication attempts to zero, use the **clear aaa local user** command in Privileged EXEC mode.

clear aaa local user { **fail-attempts** | **lockout** } { **username** *name* | **all** }

Syntax Description

all	Either unlocks all locked-out users, or resets the failed-attempts counter to 0 for all users.
failed-attempts	Resets the failed attempts counter to 0 for the specified user or all users.
lockout	Unlocks users that are currently locked out and resets to the failed-attempts counter for the users to 0. This option has no impact on users who are not locked out. The administrator cannot be locked out of the device.
username *name*	Specifies a specific username to unlock or reset the failed-attempts counter to 0.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use this command if a user fails to authenticate after a few attempts.

After the configured number of failed authentication attempts, the user is locked out of the system and cannot successfully log in until either a system administrator unlocks the username or the system reboots. The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates, or when the system reboots. In addition, the system resets the counter to zero when the configuration has recently been modified.

Locking or unlocking a username results in a system log message. A system administrator with a privilege level of 15 cannot be locked out.

Examples

The following example shows how to reset the failed-attempts counter to 0 for the username anyuser:

```
ciscoasa# clear aaa local user fail-attempts
            username anyuser
ciscoasa#
```

The following example shows how to reset the failed-attempts counter to 0 for all users:

```
ciscoasa# clear aaa local user fail-attempts
            all
ciscoasa#
```

The following example shows to clear the lockout condition and reset the failed-attempts counter to 0 for the username anyuser:

```
ciscoasa# clear aaa local user lockout username anyuser
ciscoasa#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
show aaa local user	Shows the list of usernames with the failed attempts counter and lockout status.

clear aaa sdi node-secret

To delete the node secret file for an RSA SecurID server, use the **clear aaa sdi node-secret** command in privileged EXEC mode.

clear aaa sdi node-secret *rsa_server_address*

Syntax Description

rsa_server_address	The IP address or fully-qualified hostname of the RSA SecurID/Authentication Manager server whose node secret file you want to delete.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.15(1)	This command was added.

Examples

The following example shows how to view the list of node secret files, then delete one of them. Use the aaa sdi import-node-secret command to import a new node secret file for the server, if necessary.

```
ciscoasa# show aaa sdi node-secrets

Last update                    SecurID server
--------------------           --------------------
15:16:13 Jun 24 2020           rsaam.example.com
15:20:07 Jun 24 2020           10.11.12.13
ciscoasa# clear aaa sdi node-secret rsaam.example.com
```

Related Commands

Command	Description
aaa sdi import-node-secret	Imports an RSA SecurID Authentication Manager node secret file.
show aaa sdi node-secrets	Displays all the SecurID node secret files.

clear aaa-server statistics

To reset the statistics for AAA servers, use the **clear aaa-server statistics** command in privilged EXEC mode.

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

groupname	(Optional) Clears statistics for servers in a group.
host *hostname*	(Optional) Clears statistics for a particular server in the group.
LOCAL	(Optional) Clears statistics for the LOCAL user database.
protocol *protocol*	(Optional) Clears statistics for servers of the specified protocol: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Command Default

Remove all AAA server statistics across all groups.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines. In the protocol values, **nt** replaces the older **nt-domain**, and **sdi** replaces the older **rsa-ace**.

Examples

The following example shows how to reset the AAA statistics for a specific server in a group:

```
ciscoasa
(config)#

clear aaa-server statistics svrgrp1 host 1.2.3.4
```

The following example shows how to reset the AAA statistics for an entire server group:

```
ciscoasa
(config)#

clear aaa-server statistics svrgrp1
```

The following example shows how to reset the AAA statistics for all server groups:

```
ciscoasa
(config)#
clear aaa-server statistics
```

The following example shows how to reset the AAA statistics for a particular protocol (in this case, TACACS+):

```
ciscoasa
(config)#
clear aaa-server statistics protocol tacacs+
```

Related Commands

Command	Description
aaa-server protocol	Specifies and manages the grouping of AAA server connection data.
clear configure aaa-server	Removes all nondefault AAA server groups or clear the specified group.
show aaa-server	Displays AAA server statistics.
show running-config aaa-server	Displays the current AAA server configuration values.

clear access-list

To clear an access-list counter, use the **clear access-list** command in global configuration mode.

clear access-list *id* **counters**

Syntax Description

counters	Clears access list counters.
id	Name or number of an access list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you enter the **clear access-list** command, you must specify the *id* of an access list to clear the counters .

Examples

The following example shows how to clear a specific access list counter:

```
ciscoasa# clear access-list inbound counters
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays the access list entries by number.

Command	Description
show running-config access-list	Displays the access list configuration that is running on the adaptive security appliance.

clear arp

To clear dynamic ARP entries or ARP statistics, use the **clear arp** command in privileged EXEC mode.

clear arp [**statistics**]

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears all ARP statistics:

```
ciscoasa# clear arp statistics
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear asp

To clear accelerated security path (ASP) statistics, use the **clear asp** command.

clear asp { **cluster counter** | **drop** [**flow** | **frame**] | **event dp-cp** | **queue-exhaustion** [**snapshot** *number*] | **load-balance history** | **overhead** | **table** [**arp** | **classify** | **network-object** | **filter** [**access-list** *acl_name*]] }

Syntax Description

access-list *acl_name*	(Optional) Clears the hit counters only for a specified access list.
arp	(Optional) Clears the hits counters in ASP ARP tables only.
classify	(Optional) Clears the hits counters in ASP classify tables only
cluster counter	Clears cluster counters.
event	Clears data-path to control-plane event statistics.
filter	(Optional) Clears the hits counters in ASP filter tables only
flow	(Optional) Clears the dropped flow statistics.
frame	(Optional) Clears the dropped frame/packet statistics.
load-balance history	Clears the history of ASP load balancing per packet and reset the number of times an automatic switch occurred
network-object	(Optional) Clears the hits counters in ASP network object tables only. These tables are used when object group search is enabled.
overhead	Clears all ASP multiprocessor overhead statistics.
queue-exhaustion	Clears the data-path inspection Snort queue snapshot.
snapshot *number*	(Optional) Clears the queue exhaustion by snapshot ID.
table	Clears the hit counters in the ARP tables. Specify the table type to limit the action.

Command Default

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)	We added the **table** keyword.
8.2(2)	We added the **filter** keyword.
9.3(1)	We added the **load-balance history** keywords.
9.22(1)	The **table network-object** option was added.

Examples

The following example clears all ASP table statistics:

```
ciscoasa# clear asp table
Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! ciscoasa#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
 of other modules and output of other "show" commands! ciscoasa#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits statistic
 of other modules and output of other "show" commands! ciscoasa(config)# clear asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! ciscoasa# sh asp table arp
Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0
Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

Related Commands

Command	Description
asp load-balance per-packet	Changes the load balancing behavior.
show asp load-balance	Displays a histogram of the load balancer queue sizes.
show asp load-balance per-packet	Displays current status, high and low watermarks, and the global threshold.
show asp load-balance per-packet history	Displays current status, high and low watermarks, the global threshold, the times of switching ASP load balancing per packet on and off since the last reset, the history of ASP load balancing per packet with time stamps, and the reasons for switching it on and off.
show asp	Shows ASP statistics.

clear avc

To clear statistics and hit counts for the Application Visibility and Control (AVC) feature, use the clear avc command in Privileged EXEC mode.

clear avc

Command Default

No defaults

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.24(1)	This command was added.

Example

The following example clears AVC counters.

```
ciscoasa# clear avc
```

Related Commands

Command	Description
avc	Enable Application Visibility and Control (AVC).
show avc	Display AVC information.

clear bfd counters

To clear the BFD counters, use the **clear bfd counters** command in privileged EXEC mode.

clear bfd counters [**ld** *local_discr* | *interface_name* | **ipv4** *ip-address* | **ipv6** *ipv6-address*]

Syntax Description

ld *local_discr*	(Optional) Clears BFD counters for the specified local discriminator, 1 - 4294967295.
interface_name	(Optional) Clears BFD counters for the specified interface.
ipv4 *ip_address*	(Optional) Clears BFD counters for the specified neighbor IP address.
ipv6 *ip_address*	(Optional) Clears BFD counters for the specified neighbor IPv6 address.

Command Default

This command clears all BFD counters.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example clears all BFD counters.

```
ciscoasa# clear bfd counters
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.

Command	Description
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

clear bgp

Note ASA platforms do not support the legacy neighbor soft-reconfiguration inbound CLI or memory caching of inbound BGP updates. Instead, ASA relies exclusively on BGP Dynamic Route Refresh (RFC 2918) for inbound policy changes. The **clear bgp <neighbor> in** command triggers a route refresh using this mechanism.

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the **clear bgp** command in privileged EXEC mode.

clear bgp { [***** | **external**] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map** }

Syntax Description

*	Specifies that all current BGP sessions will be reset.
as_number	(Optional) Number of the autonomous system in which all BGP peer sessions will be reset.
external	Specifies that all external BGP sessions will be reset.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
ipv4 unicast	Resets BGP connections using hard or soft econfiguration for IPv4 address family sessions.
ipv6 unicast	Resets BGP connections using hard or soft econfiguration for IPv6 address family sessions.
neighbor_address	(Optional) Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
soft	(Optional) Triggers a soft reconfiguration. For inbound sessions, this utilizes BGP Dynamic Route Refresh (RFC 2918) to request updates from the peer without tearing down the BGP session.
table-map	Clears table-map configuration information in BGP routing tables. This command can be used to clear traffic-index information configured with the BGP Policy Accounting feature.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was introduced.

Usage Guidelines

The **clear bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration triggers the BGP Dynamic Route Refresh (RFC 2918) process to reconfigure and activate BGP routing tables without tearing down existing peering sessions. This allows you to apply a new BGP policy without disrupting the network and does not require additional memory for storing inbound routing updates.

Only the **clear bgp *** command is available in the system execution space in multiple context mode.

Examples

In the following example, all the BGP sessions in all contexts are reset when the **clear bgp** command is given in the system execution space. A warning is issued to confirm the action as this command will reset all the BGP sessions:

```
ciscoasa# clear bgp *
This command will reset BGP in ALL contexts.
Are you sure you want to continue? [no]:
```

In the following example, all the BGP sessions are reset in single mode or in a multiple context mode context:

```
ciscoasa# clear bgp *
```

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
ciscoasa# clear bgp 10.100.0.1 soft in
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers, a soft reconfiguration is initiated for the inbound session with the neighbor 172.16.10.2, and the outbound session is unaffected:

```
ciscoasa# clear bgp 172.16.10.2 in
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
ciscoasa# clear bgp 35700
```

In the following example, a soft reconfiguration is configured for all inbound eBGP peering sessions:

```
ciscoasa# clear bgp external soft in
```

In the following example, all outbound address family IPv4 multicast eBGP peering sessions are cleared:

```
ciscoasa# clear bgp external ipv4 multicast out
```

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in IPv4 unicast address family sessions in autonomous system 65400, and the outbound session is unaffected:

```
ciscoasa# clear bgp ipv4 unicast 65400 soft in
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation:

```
ciscoasa# clear bgp ipv4 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation:

```
ciscoasa# clear bgp ipv4 unicast 1.2
```

The following example clears the table map for IPv4 unicast peering sessions:

```
ciscoasa# clear bgp ipv4 unicast table-map
```

clear blocks

To reset the packet buffer counters such as the exhaustion condition and history information, use the **clear blocks** command in privileged EXEC mode.

clear blocks [**exhaustion** { **history** | **snapshot** } | **export-failed** | **queue** [**history** [**core-local** [*number*]]]]

Syntax Description

core-local [*number*]	(Optional) Clears system buffers queued by application for all cores, or if you specify the core number, a specific core.
exhaustion	(Optional) Clears the exhaustion condition.
export-failed	(Optional) Clears the export failed counters.
history	(Optional) Clears the history.
queue	(Optional) Clears queued blocks.
snapshot	(Optional) Clears the snapshot information.

Command Default

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was added.
9.1(5)	The **history** and **snapshot** options were added.

Usage Guidelines

Resets the low watermark counters to the current available blocks in each pool. Additionally, this command clears the history information stored during the last buffer allocation failure.

Examples

The following example clears the blocks:

```
ciscoasa# clear blocks
```

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics.
show blocks	Shows the system buffer utilization.

clear-button

To customize the Clear button of the WebVPN page login field that is displayed to WebVPN users when they connect to the ASA, use the **clear-button** command in customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

clear-button { **text** | **style** } *value*
no clear-button [{ **text** | **style** }] *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display or Cascading Style Sheet (CSS) parameters, each with a maximum of 256 characters allowed.

Command Default

The default text is “Clear”.

The default style is border:1px solid black;background-color:white;font-weight:bold;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the default background color of the Clear button from black to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# clear-button style background-color:blue
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page Login field.
login-button	Customizes the login button of the WebVPN page Login field.
login-title	Customizes the title of the WebVPN page Login field.
password-prompt	Customizes the password prompt of the WebVPN page Login field.
username-prompt	Customizes the username prompt of the WebVPN page Login field.

clear capture

To clear the capture buffer, use the **clear capture** command in privileged EXEC configuration mode.

clear capture { **/all** | *capture_name* }

Syntax Description

/all	Clears packets on all interfaces.
capture_name	Specifies the name of the packet capture.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The shortened form of the **clear capture** (for example, **cl cap** or **clear cap**) is n ot supported to prevent accidental destruction of all the packet captures.

Examples

This example shows how to clear the capture buffer for the capture buffer “example”:

```
ciscoasa
(config)#
clear capture example
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
show capture	Displays the capture configuration when no options are specified.

clear clns cache

To clear and reinitialize the Connectionless Network Service (CLNS) routing cache, use the clear clns cache EXEC command.

clear clns cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear routing cache information, use the **clear clns cache** command.

Examples

The following example clears CLNS routing cache:

```
ciscoasa# clear clns cache
```

Related Commands

Command	Description
show clns cache	Shows clns routing cache.

clear clns is-neighbors

To remove IS neighbor information from the adjacency database, use the clear clns is-neighbors EXEC command.

clear clns is-neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear IS neighbor information from the adjacency database, use the **clear clns is-neighbors** command.

Examples

The following example clears CLNS es-neighbor:

```
ciscoasa# clear clns is-neighbors
```

Related Commands

Command	Description
clear clns neighbors	Removes clns neighbor information.
show clns is-neighbors	Shows clns is neighbor information.

clear clns neighbors

To remove CLNS neighbor information from the adjacency database, use the clear clns neighbors EXEC command.

clear clns neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear neighbor information from the adjacency database, use the **clear clns neighbors** command.

Examples

The following example removes the CLNS neighbor information from the adjacency database:

```
ciscoasa# clear clns neighbors
```

Related Commands

Command	Description
clear clns is-neighbors	Removes clns is-neighbor information.
show clns neighbors	Shows clns neighbor information.

clear clns route

To remove all of the dynamically derived CLNS routing information, use the clear clns route EXEC command.

clear clns route

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To clear routing information, use the **clear clns is-neighbors** command.

Examples

The following example removes all of the dynamically derived CLNS routing information:

```
ciscoasa# clear clns route
```

Related Commands

Command	Description
show clns route	Shows clns route information.

clear cluster info

To clear cluster statistics, use the **clear cluster info** command in privileged EXEC mode.

clear cluster info { **flow-mobility counters** | **health details** | **trace** | **transport** }

Syntax Description

flow-mobility counters	Clears the cluster flow-mobility counters.
health details	Clears cluster health information.
trace	Clears cluster event trace information.
transport	Clears cluster transport statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2)	We introduced the **flow-mobility counters** keywords.
9.0(1)	This command was added.

Usage Guidelines

To view cluster statistics, use the **show cluster info** command.

Examples

The following example clears cluster event trace information:

```
ciscoasa# clear cluster info trace
```

Related Commands

Command	Description
show cluster info	Shows cluster statistics.

clear compression

To clear compression statistics for all SVC and WebVPN connections, use the **clear compression** command in privileged EXEC mode.

clear compression { **all** | **anyconnect-ssl** | **http-comp** }

Syntax Description

all	Clears all compressions statistics.
http-comp	Clears HTTP-COMP statistics.
anyconnect-ssl	Clears anyconnect-ssl compression statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.
8.4(1)	anyconnect-ssl replaced svc.
9.5(2)	Support for multiple context mode was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, clears the compression configuration for the user:

```
hostname# clear configure compression
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of data over an SVC connection for a specific group or user.

clear configuration session

To delete a configuration session, use the **clear configuration session** command in global configuration mode.

clear configuration session [*session_name*]

Syntax Description

session_name	The name of an existing configuration session. Use the **show configuration session** command for a list of current sessions. If you omit this parameter, all existing sessions are deleted.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Use this command in conjunction with the **configure session** command, which creates isolated sessions for editing ACLs and their objects. If you decide you no longer need a session you created, and you do not want to commit the changes defined in the session, use this command to remove the session and the changes it contains.

If you want to simply clear the changes made within a session without deleting the session, use the **clear session** command instead of this one.

Examples

The following example deletes the session named old-session:

```
ciscoasa(config)# clear configuration session old-session
```

Related Commands

Command	Description
clear session	Clears the contents of a configuration session or resets its access flag.
configure session	Creates or opens a session.
show configuration session	Shows the changes made in each current session.

clear configure

To clear the running configuration, use the **clear configure** command in global configuration mode.

clear configure { **primary** | **secondary** | **all** | *command* }

Syntax Description

all	Clears the entire running configuration.
command	Clears the configuration for a specified command. For available commands, use the **clear configure ?** command for CLI help.
primary	For a failover pair, clears the primary unit configuration.
secondary	For a failover pair, clears the secondary unit configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you enter this command in a security context, you clear only the context configuration. If you enter this command in the system execution space, you clear the system running configuration as well as all context running configurations. Because you cleared all context entries in the system configuration (see the **context** command), the contexts are no longer running, and you cannot change to a context execution space.

Before clearing the configuration, make sure you save any changes to the **boot config** command (which specifies the startup configuration location) to the startup configuration; if you changed the startup configuration location only in the running configuration, then when you restart, the configuration loads from the default location.

If you clear an object that is being used in another command, such as an access list, the object is emptied but not removed. After you remove the object from all commands that refer to it, you can use the no form of the object or object-group commands to delete the object.

Note When you enter the **clear configure all** command, the master pass phrase used in password encryption is not removed. For more information about the master pass phrase, see the **config key password-encryption** command.

Examples

The following example clears the entire running configuration:

```
ciscoasa(config)# clear configure all
```

The following example clears the AAA configuration:

```
ciscoasa(config)# clear configure aaa
```

Related Commands

Command	Description
show running-config	Shows the running configuration.

clear conn

To clear a specific connection or multiple connections, use the clear **conn** command in privileged EXEC mode.

clear conn [**all**] [**tcp | udp** | **sctp** }] [**address** *src_ip*] [- *src_ip*] [**netmask** *mask*]] [**port** *src_port* [- *src_port*]] [**address** *dest_ip* [- *dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [- *dest_port*] [**user** [*domain_nickname*\ ] *user_name* | **user-group** [*domain_nickname*\\ ] *user_group_name*] | **zone** [*zone_name*]] [**data-rate**]

Syntax Description

address	(Optional) Clears connections with the specified source or destination IP address.
all	(Optional) Clears all connections, including to-the-box connections. Without the **all** keyword, only through-the-box connections are cleared.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Clears connections with the specified source or destination port.
protocol {tcp | udp | **sctp}**	(Optional) Clears connections with the specified protocol.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
user [*domain_nickname* \ ] *user_name*	(Optional) Clears connections that belong to the specified user. When you do not include the *domain_nickname* argument, the ASA clears connections for the user in the default domain.
user-group [*domain_nickname* \\ ] *user_group_name*	(Optional) Clears connections that belong to the specified user group. When you do not include the *domain_nickname* argument, the ASA clears connections for the user group in the default domain.
zone [*zone_name*]	Clears connections that belong to a traffic zone.

data-rate	(Optional) Clears the current maximum data-rate stored.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	This command was added.
8.4(2)	Added the **user** and **user-group** keywords to support the Identity Firewall.
9.3(2)	The **zone** keyword was added.
9.5(2)	The **protocol sctp** keyword was added.
9.14(1)	The **data-rate** keyword was added.

Usage Guidelines

This command supports IPv4 and IPv6 addresses.

When you make security policy changes to the configuration, all *new* connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy using the **clear conn** command. You can alternatively use the **clear local-host** command to clear connections per host, or the **clear xlate** command for connections that use dynamic NAT.

When the ASA creates a pinhole to allow secondary connections, this is shown as an incomplete connection in the **show conn** command output. To clear this incomplete connection, use the **clear conn** command.

Examples

The following example shows how to view all connections and then clear the management connection between 10.10.10.108:4168 and 10.0.8.112:22:

```
ciscoasa# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB
ciscoasa# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

The following example shows how to clear connection maximum data-rate stored in the extension memory:

```
ciscoasa# clear conn data-rate
Released conn extension memory for 10 connection(s)
```

Related Commands

Commands	Description
clear local-host	Clears all connections by a specific local host or all local hosts.
clear xlate	Clears a dynamic NAT session, and any connections using NAT.
show conn	Shows connection information.
show local-host	Displays the network states of local hosts.
show xlate	Shows NAT sessions.

clear console-output

To remove the currently captured console output, use the **clear console-output** command in privileged EXEC mode.

clear console-output

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to remove the currently captured console output:

```
ciscoasa# clear console-output
```

Related Commands

Command	Description
console timeout	Sets the idle timeout for a console connection to the ASA.
show console-output	Displays the captured console output.
show running-config console timeout	Displays the idle timeout for a console connection to the ASA.

clear coredump

To clear the coredump log, use the clear coredump command in global configuration mode.

clear coredump

Syntax Description

This command has no arguments or keywords.

Command Default

By default, coredumps are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Note For ASAs that are operating on 4100/9300 platforms, use the bootstrap CLI mode for working with coredumps.

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command removes the coredump file system contents and the coredump log. The coredump file system remains intact. The current coredump configuration remains unchanged.

Examples

The following example removes the coredump file system contents and the coredump log:

```
ciscoasa(config)# clear coredump
Proceed with removing the contents of the coredump filesystem on 'disk0:' [confirm]
```

Related Commands

Command	Description
coredump enable	Enables the coredump feature.
clear configure coredump	Removes the coredump file system and its contents from your system.
show coredump filesystem	Displays files on the coredump filesystem.
show coredump log	Shows the coredump log.

clear counters

To clear the protocol stack counters, use the **clear counters** command in global configuration mode.

clear counters [**all** | **context** *context-name* | **summary** | **top** *n*] [**detail**] [**protocol** *protocol_name* | *counter_name*]] [**threshold** *n*]

Syntax Description

all	(Optional) Clears all filter details.
context *context-name*	(Optional) Specifies the context name.
counter_name	(Optional) Specifies a counter by name. Use the **show counters protocol** command to see which counters are available.
detail	(Optional) Clears detailed counters information.
protocol *protocol_name*	(Optional) Clears the counters for the specified protocol.
summary	(Optional) Clears the counter summary.
threshold *n*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.
top *n*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.

Command Default

The **clear counters summary detail** command is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to clear the protocol stack counters:

```
ciscoasa(config)# clear counters
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.

clear cpu profile

To clear the CPU profiling statistics, use the **clear cpu profile** command in privileged EXEC mode.

clear cpu profile

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to delete the crash file:

```
ciscoasa# clear cpu profile
```

Related Commands

show cpu	Displays information about the CPU.
show cpu profile	Displays CPU profiling data.

clear crashinfo

To delete all the crash information files stored in flash memory, use the **clear crashinfo** command in privileged EXEC mode.

clear crashinfo [**module** { **0** | **1** }]

Syntax Description

module {**0** | **1**}	(Optional) Clears the crash file for a module in slot 0 or 1.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	The output was updated to delete all the crashinfo files that are written to flash memory.

Examples

The following example shows how to delete the crash file:

```
ciscoasa# clear crashinfo
```

Related Commands

crashinfo force	Forces a crash of the ASA.
crashinfo save disable	Disables crash information from writing to flash memory.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo	Displays the contents of the latest crash information file stored in flash memory.
show crashinfo files	Displays the last five crash information files based on the date and timestamp.

clear crypto accelerator statistics

To clear the the global and accelerator-specific statistics from the crypto accelerator MIB, use the **clear crypto accelerator statistics** command in privileged EXEC mode.

clear crypto accelerator statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example entered in global configuration mode, displays crypto accelerator statistics:

```
ciscoasa(config)# clear crypto accelerator statistics
ciscoasa(config)#
```

Related Commands

Command	Description
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

clear crypto ca crls

To empty the CRL cache of all CRLs associated with a specified trustpoint, all CRLs associated with the trustpool from the cache, or the CRL cache of all CRLs, use the **clear crypto ca crls** command in privileged EXEC mode.

clear crypto ca crls [**trustpoool** | **trustpoint** *trust_point_name*]

Syntax Description

trustpoint *trust_point_name*	The name of a trustpoint. If you do not specify a name, this command clears all CRLs cached on the system. If you give the trustpoint keyword without a *trust_point_name* , the command fails.
trustpool	Indicates that the action should be applied only to the CRLs that are associated with certificates in the trustpool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following independent examples issued in privileged EXEC configuration mode clear all of the trustpool CRLs, clears all of the CRLs associated with trustpoint123, and removes all of the cached CRLs from the ASA:

```
ciscoasa# clear crypto ca crl trustpool
ciscoasa# clear crypto ca crl trustpoint trustpoint123
ciscoasa# clear crypto ca crl
```

Related Commands

Command	Description
crypto ca crl request	Downloads the CRL based on the CRL configuration of the trustpoint.
show crypto ca crl	Displays all cached CRLs or CRLs cached for a specified trustpoint.

clear crypto ca trustpool

To remove all certificates from the trustpool, use the **clear crypto ca trustpool** command in privileged EXEC mode.

clear crypto ca trustpool [**noconfirm**]

Syntax Description

noconfirm (Optional) Suppresses user confirmation prompts, and the command will be processes as requested.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes		—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The user is asked to confirm this action before carrying it out.

Examples

The following example clears all certificates:

```
ciscoasa# clear crypto ca trustpool
You are about to clear the trusted certificate pool. Do you want to continue? (y/n) y
ciscoasa#
```

Related Commands

Command	Description
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.
crypto ca trustpool remove	Removes a single specified certificate from the trustpool.

clear crypto ikev1

To remove the IPsec IKEv1 SAs or statistics, use the **clear crypto ikev1** command in privileged EXEC mode. To clear all IKEv1 SAs, use this command without arguments.

clear crypto ikev1 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv1 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv1 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv1 statistics from the ASA:

```
ciscoasa# clear crypto ikev1 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear crypto ikev1 sa peer 10.86.1.1
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto ikev2

To remove the IPsec IKEv2 SAs or statistics, use the **clear crypto ikev2** command in privileged EXEC mode. To clear all IKEv2 SAs, use this command without arguments.

clear crypto ikev2 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv2 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv2 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv2 statistics from the ASA:

```
ciscoasa# clear crypto ikev2 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear crypto ikev2 sa peer 10.86.1.1
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto ipsec sa

To remove the IPsec SA counters, entries, crypto maps or peer connections, use the **clear crypto ipsec sa** command in privileged EXEC mode. To clear all IPsec SAs, use this command without arguments.

clear crypto ipsec sa [**counters** | **entry** *ip_address* { **esp** | **ah** } *spi* | **map** *map name* | **peer** *ip_address*]

Syntax Description

ah	Authentication header.
counters	Clears all IPsec per SA statistics.
entry *ip_address*	Deletes the tunnel that matches the specified IP address/hostname, protocol, and SPI value.
esp	Encryption security protocol.
map *map name*	Deletes all tunnels associated with the specified crypto map as identified by map name.
peer *ip_address*	Deletes all IPsec SAs to a peer as identified by the specified hostname or IP address.
spi	Identifies the Security Parameters Index (a hexidecimal number). This must be the inbound SPI. We do not support this command for the outbound SPI.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec SAs, use this command without arguments.

Examples

The following example removes all of the IPsec SAs from the ASA:

```
ciscoasa# clear crypto ipsec sa
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear crypto ipsec peer 10.86.1.1
```

ciscoasa#

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto ipsec stats

To remove the global IPsec statistics and reset the statistics, use the **clear crypto ipsec stats** command in privileged EXEC mode.

clear crypto ipsec stats

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.16(1)	This command was added.

Usage Guidelines

To clear all the global IPsec statistics, use this command without arguments.

Examples

The following example removes and resets the the IPsec statistics in the ASA:

```
ciscoasa# clear crypto ipsec stats
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
show ipsec stats	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto isakmp

To clear ISAKMP SAs or statistics, use the **clear crypto isakmp** command in privileged EXEC mode.

clear crypto isakmp [**sa** | **stats**]

Syntax Description

sa	Clears IKEv1 and IKEv2 SAs.
stats	Clears IKEv1 and IKEv2 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all ISAKMP operational data, use this command without arguments.

Examples

The following example removes all of the ISAKMP SAs:

```
ciscoasa# clear crypto isakmp sa
ciscoasa#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp	Clears all ISAKMP policy configuration.
show isakmp	Displays information about ISAKMP operational data.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto protocol statistics

To clear the protocol-specific statistics in the crypto accelerator MIB, use the **clear crypto protocol statistics** command in privileged EXEC mode.

clear crypto protocol statistics *protocol*

Syntax Description

protocol Specifies the name of the protocol for which you want to clear statistics. Protocol choices are as follows:

- **all**—All protocols currently supported.
- **ikev1**—Internet Key Exchange (IKE) version 1.
- **ikev2**—Internet Key Exchange (IKE) version 2.
- **ipsec-client**—IP Security (IPsec) Phase-2 protocols.
- **other**—Reserved for new protocols.
- srtp—Secure RTP (SRTP) protocol
- ssh—Secure Shell (SSH) protocol
- ssl-client— Secure Socket Layer (SSL) protocol.

Command Default

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The **ikev1** and ikev2 keywords were added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example clears all crypto accelerator statistics:

```
ciscoasa# clear crypto protocol statistics all
ciscoasa#
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics in the crypto accelerator MIB.

clear crypto ssl

To clear SSL information, use the **clear crypto ssl** command in privileged EXEC mode.

clear crypto ssl { **cache** [**all**] | **errors** | **mib** | **objects** }

Syntax Description

cache	Clears expired sessions in the SSL session cache.
all	(Optional) Clears all sessions and statistics in the SSL session cache.
errors	Clears SSL errors.
mib	Clears SSL MIB statistics.
objects	Clears SSL object statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example clears all SSL cache sessions and statistics:

```
ciscoasa# clear crypto ssl cache all
ciscoasa#
```

Related Commands

Command	Description
show crypto ssl	Displays the SSL information.

clear cts

To clear data used by the ASA when integrated with Cisco TrustSec, use the **clear cts** command in global configuration mode:

clear cts { **environment-data** | **pac** } [**noconfirm**]

Syntax Description

noconfirm	Clears the data without asking for confirmation.
environment-data	Clears all CTS environment data downloaded from Cisco ISE.
pac	Clears the CTS PAC information stored in NVRAM.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If you clear the environment data, you can trigger the next environment data refresh manually or the system will refresh the data when the refresh timer expires. Clearing environment data does not remove the Cisco TrustSec PAC from the system, but it does impact traffic policy.

Before clearing the stored PAC, please understand that without a PAC, the system cannot download Cisco TrustSec environment data. However, environment data that is already on the system remains in use. Running the **clear cts pac** command renders the system unable to retrieve environment data updates.

In a cluster, you can use this command on the master unit only. In active/standby high-availability (failover), you can use it on the active unit only.

Examples

The following examples show how to clear CTS data from the system.

```
ciscoasa# clear cts pac
Are you sure you want to delete the cts PAC? (y/n) y

ciscoasa# clear cts environment-data
Are you sure you want to delete the cts environment data? (y/n) y
```

Related Commands

Command	Description
clear configure cts	Clears the configuration for integrating the ASA with Cisco TrustSec.
cts sxp enable	Enables the SXP protocol on the ASA.
show cts	Displays Cisco Trustsec (CTS) information.

clear dhcpd

To clear the DHCP server bindings and statistics, use the **clear dhcp** command in privileged EXEC mode.

clear dhcpd { **binding** [**all** | *ip_address*] | **statistics** }

Syntax Description

all	(Optional) Clears all dhcpd bindings.
binding	Clears all the client address bindings.
ip_address	(Optional) Clears the binding for the specified IP address.
statistics	Clears statistical information counters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you include the optional IP address in the **clear dhcpd binding** command, only the binding for that IP address is cleared.

To clear all of the DHCP server commands, use the **clear configure dhcpd** command.

Examples

The following example shows how to clear the **dhcpd** statistics:

```
ciscoasa# clear dhcpd statistics
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show dhcpd	Displays DHCP binding, statistic, or state information.

clear dhcprelay statistics

To clear the DHCP relay statistic counters, use the **clear dhcprelay statistics** command in privileged EXEC mode.

clear dhcprelay statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear dhcprelay statistics** command only clears the DHCP relay statistic counters. To clear the entire DHCP relay configuration, use the **clear configure dhcprelay** command.

Examples

The following example shows how to clear the DHCP relay statistics:

```
ciscoasa# clear dhcprelay statistics
ciscoasa#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcprelay	Displays debugging information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

clear dns

To clear IP addresses associated with fully qualified domain name (FQDN) hosts, use the **clear dns** command in privileged EXEC mode.

clear dns [**host** *fqdn_name* | **ip-cache** [**counters**]]

Syntax Description

host *fqdn_name*	(Optional) Specifies the fully qualified domain name of the host whose addresses should be cleared.
ip-cache [**counters**]	Clear the IP cache that is used to hold domain name resolutions for network-service objects. Once removed, domains in network-service objects will not be matched until client DNS resolution requests are resolved and snooped to rebuild the cache. Include the **counters** keyword to simply reset the hit counts for the domains and leave the IP cache in place.

Command Default

Without parameters, all DNS resolutions are cleared for hosts used in access control rules. For domain names used in network-service objects, the counters are cleared, but the IP cache is not removed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.
9.17(1)	The **ip-cache** keyword was added.

Examples

The following example clears the IP address associated with the specified FQDN host used in an FQDN network object:

```
ciscoasa# clear dns host www.example.com
```

Note The setting of the **dns expire-entry** keyword is ignored when resolutions are cleared. New DNS queries are sent for each activated FQDN host specified in an FQDN network object.

The following example clears hit counts for domains used in network-service objects.

```
ciscoasa# clear dns ip-cache counters
```

Related Commands

Command	Description
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
show dns ip-cache	Shows the DNS resolution IP cache used for network-service objects.
show dns-hosts	Shows the DNS cache.

clear dns-hosts cache

To clear the DNS cache, use the **clear dns-hosts cache** command in privileged EXEC mode.

clear dns-hosts cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command does not clear static entries that you added with the name command.

Examples

The following example clears the DNS cache:

```
ciscoasa# clear dns-hosts cache
```

Related Commands

Command	Description
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the ASA does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
show dns-hosts	Shows the DNS cache.

clear dynamic-filter dns-snoop

To clear Botnet Traffic Filter DNS snooping data, use the **clear dynamic-filter dns-snoop** command in in privileged EXEC mode.

clear dynamic-filter dns-snoop

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following example clears all Botnet Traffic Filter DNS snooping data:

```
ciscoasa# clear dynamic-filter
 dns-snoop
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.

Command	Description
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear dynamic-filter reports

To clear report data for the Botnet Traffic Filter, use the **clear dynamic-filter reports** command in privileged EXEC mode.

clear dynamic-filter reports { **top** [**malware-sites** | **malware-ports** | **infected-hosts**] | **infected-hosts** }

Syntax Description

malware-ports	(Optional) Clears report data for the top 10 malware ports.
malware-sites	(Optional) Clears report data for the top 10 malware sites.
infected-hosts (**top**)	(Optional) Clears report data for the top 10 infected hosts.
top	Clears report data for the top 10 malware sites, ports, and infected hosts.
infected-hosts	Clears report data for infected hosts.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.
8.2(2)	The **botnet-sites** and **botnet-ports** keywords were changed to **malware-sites** and **malware-ports**. The **top** keyword was added to differentiate clearing the top 10 reports and the new infected-hosts reports. The **infected-hosts** keyword was added (without **top**).

Examples

The following example clears all Botnet Traffic Filter top 10 report data:

```
ciscoasa# clear dynamic-filter
 reports top
```

The following example clears only the top 10 malware sites report data:

```
ciscoasa# clear dynamic-filter
 reports top malware-sites
```

The following example clears all infected hosts report data:

```
ciscoasa# clear dynamic-filter
 reports infected-hosts
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.

Command	Description
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports infected-hosts	Generates reports of infected hosts.
show dynamic-filter reports top	Generates reports of the top 10 malware sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear dynamic-filter statistics

To clear Botnet Traffic Filter statistics, use the **clear dynamic-filter statistics** command in in privileged EXEC mode.

clear dynamic-filter statistics [**interface** *name*]

Syntax Description

interface *name*	(Optional) Clears statistics for a particular interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following example clears all Botnet Traffic Filter DNS statistics:

```
ciscoasa# clear dynamic-filter
 statistics
```

Related Commands

Command	Description
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.

Command	Description
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports infected-hosts	Generates reports of infected hosts.
show dynamic-filter reports top	Generates reports of the top 10 malware sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear eigrp events

To clear the EIGRP event log, use the **clear eigrp events** command in privileged EXEC mode.

clear eigrp [*as-number*] **events**

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are clearing the event log. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

You can use the **show eigrp events** command to view the EIGRP event log.

Examples

The following example clears the EIGRP event log:

```
ciscoasa# clear eigrp events
```

Related Commands

Command	Description
show eigrp events	Displays the EIGRP event log.

clear eigrp neighbors

To delete entries from the EIGRP neighbor table, use the **clear eigrp neighbors** command in privileged EXEC mode.

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the process ID.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name removes all neighbor table entries that were learned through this interface.
ip-addr	(Optional) The IP address of the neighbor you want to remove from the neighbor table.
soft	Causes the ASA to resynchronize with the neighbor without resetting the adjacency.

Command Default

If you do not specify a neighbor IP address or an interface name, all dynamic entries are removed from the neighbor table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **clear eigrp neighbors** command does not remove neighbors defined using the **neighbor** command from the neighbor table. Only dynamically discovered neighbors are removed.

You can use the **show eigrp neighbors** command to view the EIGRP neighbor table.

Examples

The following example removes all entries from the EIGRP neighbor table:

```
ciscoasa# clear eigrp neighbors
```

The following example removes all entries learned through the interface named “outside” from the EIGRP neighbor table:

```
ciscoasa# clear eigrp neighbors outside
```

Related Commands

Command	Description
debug eigrp neighbors	Displays debugging information for EIGRP neighbors.
debug ip eigrp	Displays debugging information for EIGRP protocol packets.
show eigrp neighbors	Displays the EIGRP neighbor table.

clear eigrp topology

To delete entries from the EIGRP topology table, use the **clear eigrp topology** command in privileged EXEC mode.

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the process ID.
ip-addr	The IP address to clear from the topology table.
mask	(Optional) The network mask to apply to the *ip-addr* argument.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command clears existing EIGRP entries from the EIGRP topology table. You can use the **show eigrp topology** command to view the topology table entries.

Examples

The following example removes entries in the 192.168.1.0 network from EIGRP topology table:

```
ciscoasa# clear eigrp topology 192.168.1.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp topology	Displays the EIGRP topology table.

clear facility-alarm output

To de-energize the output relay and clear the alarm state of the LED in the ISA 3000, use the **clear facility-alarm output** command in privileged EXEC mode.

clear facility-alarm output

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

This command de-energizes the output relay and clears the alarm state of the output LED. This turns off the external alarm. However, this command does not fix the alarm condition that triggered the external alarm: you still must resolve the problem. Use the **show facility-alarm status** command to determine the current alarm conditions.

Examples

The following example de-energizes the output relay and clears the alarm state of the output LED:

```
ciscoasa(config)# clear facility-alarm output
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.

Command	Description
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.

clear failover statistics

To clear the failover statistic counters, use the **clear failover statistics** command in privileged EXEC mode.

clear failover statistics [**np-clients** | **cp-clients**]

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.20(2)	The **np-clients** and **cp-clients** keywords were added.

Usage Guidelines

This command clears the statistics displayed with the **show failover statistics** command and the counters in the Stateful Failover Logical Update Statistics section of the **show failover** command output. The **np-clients** and **cp-clients** keywords clears the data plane and control plane statistics of HA clients displayed in the **show failover statistics bulk-sync** commnad.

To remove the failover configuration, use the **clear configure failover** command.

Examples

The following example shows how to clear the failover statistic counters:

```
ciscoasa# clear failover statistics
ciscoasa#
```

Related Commands

Command	Description
debug fover	Displays failover debugging information.
show failover	Displays information about the failover configuration and operational statistics.

clear flow-export counters

To reset runtime counters for NetFlow statistical and error data to zero, use the **clear flow-export counters** command in privileged EXEC mode.

clear flow-export counters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(1)	This command was added.

Examples

The following example shows how to reset NetFlow runtime counters:

```
ciscoasa# clear flow-export counters
```

Related Commands

Commands	Description
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays all NetFlow runtime counters.

clear flow-offload

To clear off-loaded flow statistics or off-loaded flows, use the **clear flow-offload** command in privileged EXEC mode.

clear flow-offload { **statistics** | **flow all** }

Syntax Description

statistics	Clear statistics for off-loaded flows.
flow all	Clear all off-loaded flows.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was introduced.

Usage Guidelines

The **clear flow-offload statistics** command resets statistics for off-loaded flows to zero.

If you use **clear flow-offload flow all** to remove off-loaded flows, subsequent packets for these flows would go to the ASA. The ASA would then off-load the flows again. Overall statistics for the flows that you cleared would not be correct. This command is meant for debugging purposes only.

Examples

The following example clears statistics:

```
ciscoasa# clear flow-offload statistics
```

Related Commands

Commands	Description
flow-offload	Enables flow off-load.
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.
show flow-offload	Displays information about flow off-loading.

clear flow-offload-ipsec

To clear information related to IPsec flow offload, use the **clear flow-offload-ipsec** command in privileged EXEC mode.

clear flow-offload-ipsec statistics

Syntax Description

statistics	Clear statistics related to IPsec flow offload.

Command Default

All statistics are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	This command was introduced.

Example

The following example clears all IPsec flow offload statistics.

```
ciscoasa# clear flow-offload-ipsec statistics
```

Related Commands

Command	Description
flow-offload-ipsec	Configures IPsec flow offload.
show flow-offload-ipsec	Displays IPsec flow offload statistics and information.

clear fragment

To clear the operational data of the IP fragment reassembly module, enter the **clear fragment** command in privileged EXEC mode.

clear fragment { **queue** | **statistics** [*interface_name*] }

Syntax Description

interface_name	(Optional) Specifies the ASA interface.
queue	Clears the IP fragment reassembly queue.
statistics	Clears the IP fragment reassembly statistics.

Command Default

If an *interface_name* is not specified, the command applies to all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The command was separated into two commands, **clear fragment** and **clear configure fragment**, to separate clearing of the configuration data from the operational data.

Usage Guidelines

This command clears either the currently queued fragments that are waiting for reassembly (if the **queue** keyword is entered) or clears all IP fragment reassembly statistics (if the **statistics** keyword is entered). The statistics are the counters, which tell how many fragments chains were successfully reassembled, how many chains failed to be reassembled, and how many times the maximum size was crossed resulting in overflow of the buffer.

Examples

The following example shows how to clear the operational data of the IP fragment reassembly module:

```
ciscoasa# clear fragment queue
```

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
fragment	Provides additional management of packet fragmentation and improves compatibility with the NFS.

Command	Description
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

clear gc

To remove the garbage collection (GC) process statistics, use the **clear** gc command in privileged EXEC mode.

clear gc

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to remove the GC process statistics:

```
ciscoasa# clear gc
```

Related Commands

Command	Description
show gc	Displays the GC process statistics.

clear igmp counters

To clear all IGMP counters, use the **clear igmp counters** command in privileged EXEC mode.

clear igmp counters [*if_name*]

Syntax Description

if_name	The interface name, as specified by the **nameif** command. Including an interface name with this command causes only the counters for the specified interface to be cleared.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the IGMP statistical counters:

```
ciscoasa# clear igmp counters
```

Related Commands

Command	Description
clear igmp group	Clears discovered groups from the IGMP group cache.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp group

To clear discovered groups from the IGMP group cache, use the **clear igmp** command in privileged EXEC mode.

clear igmp group [*group* | **interface** *name*]

Syntax Description

group	IGMP group address. Specifying a particular group removes the specified group from the cache.
interface *name*	Interface name, as specified by the **namif** command. When specified, all groups associated with the interface are removed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you do not specify a group or an interface, all groups are cleared from all interfaces. If you specify a group, only the entries for that group are cleared. If you specify an interface, then all groups on that interface are cleared. If you specify both a group and an interface, only the specified groups on the specified interface are cleared.

This command does not clear statically configured groups.

Examples

The following example shows how to clear all discovered IGMP groups from the IGMP group cache:

```
ciscoasa# clear igmp group
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP counters.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp traffic

To clear the IGMP traffic counters, use the **clear igmp traffic** command in privileged EXEC mode.

clear igmp traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the IGMP statistical traffic counters:

```
ciscoasa# clear igmp traffic
```

Related Commands

Command	Description
clear igmp group	Clears discovered groups from the IGMP group cache.
clear igmp counters	Clears all IGMP counters.

clear ikev1

To remove the IPsec IKEv1 SAs or statistics, use the **clear ikev1** command in privileged EXEC mode. To clear all IKEv1 SAs, use this command without arguments.

clear ikev1 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv1 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv1 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv1 statistics from the ASA:

```
ciscoasa# clear ikev1 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear ikev1 sa peer 10.86.1.1
```

ciscoasa#

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear ikev2

To remove the IPsec IKEv2 SAs or statistics, use the **clear ikev2** command in privileged EXEC mode. To clear all IKEv2 SAs, use this command without arguments.

clear ikev2 { **sa** *ip_address* | **stats** }

Syntax Description

sa **ip_address**	Clears the SA.
stats	Clears the IKEv2 statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear all IPsec IKEv2 SAs, use this command without arguments.

Examples

The following example removes all of the IPsec IKEv2 statistics from the ASA:

```
ciscoasa# clear ikev2 stats
ciscoasa#
```

The following example deletes SAs with a peer IP address of 10.86.1.1:

```
ciscoasa# clear ikev2 sa peer 10.86.1.1
```

ciscoasa#

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.

Command	Description
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPsec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear interface

To clear interface statistics, use the **clear interface** command in privileged EXEC mode.

clear interface [*physical_interface* [**.** *subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Command Default

By default, this command clears all interface statistics.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the ASA clears only statistics for the current context. If you enter this command in the system execution space, the ASA clears the combined statistics.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following example clears all interface statistics:

```
ciscoasa# clear interface
```

Related Commands

Command	Description
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Displays the interface configuration.

clear ip audit count

To clear the count of signature matches for an audit policy, use the **clear ip audit count** command in privileged EXEC mode.

clear ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Clears the number of matches for all interfaces.
interface *interface_name*	(Optional) Clears the number of matches for the specified interface.

Command Default

If you do not specify a keyword, this command clears the matches for all interfaces (**global**).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the count for all interfaces:

```
ciscoasa# clear ip audit count
```

Related Commands

Command	Description
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show ip audit count	Shows the count of signature matches for an audit policy.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

clear ipsec sa

To clear IPsec SAs entirely or based on specified parameters, use the **clear ipsec sa** command in privileged EXEC mode.

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

Syntax Description

counters	(Optional) Clears all counters.
entry	(Optional) Clears IPsec SAs for a specified IPsec peer, protocol and SPI.
inactive	(Optional) Clears IPsec SAs that are unable to pass traffic.
map*map-name*	(Optional) Clears IPsec SAs for the specified crypto map.
peer	(Optional) Clears IPsec SAs for a specified peer.
peer-addr	Specifies the IP address of an IPsec peer.
protocol	Specifies an IPsec protocol: **esp** or **ah**
spi	Specifies an IPsec SPI.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can also use an alternate form of this command to perform the same function: **clear crypto ipsec sa**.

Examples

The following example, entered in global configuration mode, clears all IPsec SA counters:

```
ciscoasa# clear ipsec sa counters
ciscoasa#
```

Related Commands

Command	Description
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec stats	Displays global IPsec statistics from the IPsec flow MIB.

clear ipsec stats

To clear IPsec statistics and reset the statstics, use the **clear ipsec stats** command in privileged EXEC mode.

clear ipsec stats

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.16(1)	This command was added.

Usage Guidelines

You can also use an alternate form of this command to perform the same function: **clear crypto ipsec stats**.

Examples

The following example, entered in global configuration mode, clears all IPsec statistics:

```
ciscoasa# clear ipsec stats
ciscoasa#
```

Related Commands

Command	Description
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec stats	Displays global IPsec statistics from the IPsec flow MIB.

clear ipv6 access-list counters (Deprecated)

To clear the IPv6 access list statistical counters, use the **clear ipv6 access-list counters** command in privileged EXEC mode.

clear ipv6 access-list *id* **counters**

Syntax Description

id	The IPv6 access list identifier.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	This command was deprecated.

Examples

The following example shows how to clear the statistical data for the IPv6 access list 2:

```
ciscoasa# clear ipv6 access-list 2 counters
ciscoasa#
```

Related Commands

Command	Description
clear configure ipv6	Clears the **ipv6 access-list** commands from the current configuration.
ipv6 access-list	Configures an IPv6 access list.
show ipv6 access-list	Displays the **ipv6 access-list** commands in the current configuration.

clear ipv6 dhcprelay

To clear the IPv6 DHCP relay binding entries and statistics, use the **clear ipv6 dhcprelay** command in privileged EXEC mode.

clear ipv6 dhcprelay { **binding** [*ip_address*] | **statistics** }

Syntax Description

binding	Clears the IPv6 DHCP relay binding entries.
ip_address	(Optional) Specifies the IPv6 address for the DHCP relay binding. If the IP address is specified, only the relay binding entries associated with that IP address are cleared.
statistics	Clears the IPv6 DHCP relay agent statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows how to clear the statistical data for the IPv6 DHCP relay binding:

```
ciscoasa# clear ipv6 dhcprelay binding
ciscoasa#
```

Related Commands

Command	Description
show ipv6 dhcprelay binding	Shows the relay binding entries created by the relay agent.
show ipv6 dhcprelay statistics	Shows the IPv6 DHCP relay agent information.

clear ipv6 dhcp statistics

To clear DHCPv6 client and Prefix Delegation client statistics, use the **clear ipv6 dhcp client statistics** command in privileged EXEC mode.

clear ipv6 dhcp { **client** [**pd**] | **interface** *interface_name* | **server** } **statistics**

Syntax Description

client	Clears the DHCPv6 client statistics.
interface *interface_name*	Clears the DHCPv6 statistics for the specified interface.
pd	Clears the Prefix Delegation client statistics.
server	Clears the DHCPv6 server statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

This command clears DHCPv6 client statistics.

Examples

The following example clears the DHCPv6 client statistics:

```
ciscoasa# clear ipv6 dhcp client statistics
```

The following example clears the DHCPv6 Prefix Delegation client statistics:

```
ciscoasa# clear ipv6 dhcp client pd statistics
```

The following example clears statistics on the outside interface:

```
ciscoasa# clear ipv6 dhcp interface outside statistics
```

The following example clears DHCPv6 server statistics:

```
ciscoasa# clear ipv6 dhcp server statistics
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.

Command	Description
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

clear ipv6 eigrp

To remove IPv6 router configuration, use the **clear ipv6 eigrp** command

clear ipv6 eigrp

Syntax Description

ipv6_address	Neighbor address.
interface_name	Interface name.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
9.20(1)	This command was added.

Examples

```
ciscoasa# clear ipv6 eigrp
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on an interface.
show ipv6 eigrp	Displays the EIGRP router configuration mode commands in the running configuration. Displays information about interfaces configured with IPv6 EIGRP.

clear ipv6 router eigrp

To remove IPv6 router configuration as well clear the routing process, use the **clear ipv6 router eigrp** command. This command will remove all the IPv6 route as well interface commands.

clear ipv6 router eigrp *as_number*

Syntax Description

as_number	The autonomous system number. This must be the same as the autonomous system number of your EIGRP routing process.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
9.20(1)	This command was added.

Examples

```
ciscoasa# clear ipv6 route eigrp 1
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on an interface.
show ipv6 eigrp	Displays information about interfaces configured with IPv6 EIGRP.

clear ipv6 mld traffic

To clear the IPv6 Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

clear ipv6 mld traffic

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)	This command was added.

Usage Guidelines

The **clear ipv6 mld traffic** command allows you to reset all the MLD traffic counters.

Examples

The following example shows how to clear the traffic counters for IPv6 MLD:

```
ciscoasa# clear ipv6 mld traffic
ciscoasa#
```

Related Commands

Command	Description
debug ipv6 mld	Displays all debugging messages for MLD.
show debug ipv6 mld	Displays the MLD commands for IPv6 in the current configuration.

clear ipv6 neighbors

To clear the IPv6 neighbor discovery cache, use the **clear ipv6 neighbors** command in privileged EXEC mode.

clear ipv6 neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command deletes all discovered IPv6 neighbor from the cache; it does not remove static entries.

Examples

The following example deletes all entries, except static entries, in the IPv6 neighbor discovery cache:

```
ciscoasa# clear ipv6 neighbors
ciscoasa#
```

Related Commands

Command	Description
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

clear ipv6 ospf

To clear OSPFv3 routing parameters, use the **clear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 [*process_id*] [**counters**] [**events**] [**force-spf**] [**process**] [**redistribution**] [**traffic**]

Syntax Description

counters	Resets the OSPF process counters.
events	Clears the OSPF event log.
force-ospf	Clears the SPF for OSPF processes.
process	Resets the OSPFv3 process.
process_id	Clears the process ID number. Valid values range from 1 to 65535.
redistribution	Clears OSPFv3 route redistribution.
traffic	Clears traffic-related statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command removes all OSPFv3 routing parameters.

Examples

The following example shows how to clear all OSPFv3 route redistribution:

```
ciscoasa# clear ipv6 ospf
            redistribution
ciscoasa#
```

Related Commands

Command	Description
show running-config ipv6 router	Shows the running configuration of OSPFv3 processes.
clear configure ipv6 router	Clears OSPFv3 routing processes.

clear ipv6 prefix-list

To clear routing prefix-lists, use the **clear ipv6 prefix-list** command in privileged EXEC mode.

clear ipv6 prefix-list [*name*]

Syntax Description

name	Clears the named prefix-list created by the **ipv6 prefix-list** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

This command removes IPv6 prefix-lists.

Examples

The following example shows how to clear the list1 IPv6 prefix-list:

```
ciscoasa# clear ipv6 prefix-list list1
ciscoasa#
```

Related Commands

Command	Description
show running-config ipv6 prefix-list	Shows the running configuration of IPv6 prefix-lists.
clear configure ipv6 prefix-list	Clears the IPv6 prefix-lost configuration.

clear ipv6 route

To delete routes from the IPv6 routing table, use the clear ipv6 route command in privileged EXEC mode.

clear ipv6 route [**management-only**] { **all** | *ipv6-prefix / prefix-length* }

Syntax Description

management-only	Clears only the IPv6 management routing table.
ipv6-prefix/prefix-length	Clears routed for the IPv6 prefix.
all	Clears all IPv6 routes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

The **clear ipv6 route** command is similar to the **clear ip route** command, except that it is IPv6-specific. The per-destination maximum transmission unit (MTU) cache is also cleared.

Examples

The following example deletes the IPv6 route for 2001:0DB8::/35:

```
ciscoasa# clear ipv6 route 2001:0DB8::/35
```

Related Commands

Command	Description
show ipv6 route	Displays IPv6 routes.

clear ipv6 traffic

To reset the IPv6 traffic counters, use the **clear ipv6 traffic** command in privileged EXEC mode.

clear ipv6 traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Using this command resets the counters in the output from the **show ipv6 traffic** command.

Examples

The following example resets the IPv6 traffic counters. The output from the **ipv6 traffic** command shows that the counters have been reset:

```
ciscoasa# clear ipv6 traffic
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output
TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Related Commands

Command	Description
show ipv6 traffic	Displays IPv6 traffic statistics.

clear ip verify statistics

To clear the unicast RPF statistics, use the **clear ip verify statistics** command in privileged EXEC mode.

clear ip verify statistics [**interface** *interface_name*]

Syntax Description

interface *interface_name*	Sets the interface on which you want to clear unicast RPF statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

See the ip verify reverse-path command to enable unicast RPF.

Examples

The following example clears the unicast RPF statistics:

```
ciscoasa# clear ip verify statistics
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the ip verify reverse-path configuration.
ip verify reverse-path	Enables the unicast RPF feature to prevent IP spoofing.
show ip verify statistics	Shows the unicast RPF statistics.
show running-config ip verify reverse-path	Shows the ip verify reverse-path configuration.

clear isakmp sa

To remove all of the IKEv1 and IKEv2 runtime SA database, use the **clear isakmp sa** command in privileged EXEC mode.

clear isakmp sa

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The **clear isakmp sa** command was changed to **clear crypto isakmp sa**.
9.0(1)	Support for multiple context mode was added.

Examples

The following example removes the IKE runtime SA database from the configuration:

```
ciscoasa# clear isakmp sa
ciscoasa#
```

Related Commands

Command	Description
clear isakmp	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active ISAKMP configuration.

clear isis

To clear the IS-IS data structures, use the **clear isis** command.

clear isis { ***** | **lspfull** | **rib redistribution** [**level-1** | **level-2**] [*network_prefix*] [*network_mask*] }

Syntax Description

*****	Clears all IS-IS data structures.
level-1	(Optional) Clears Level 1 IS-IS redistributed prefixes from the redistribution cache.
level-2	(Optional) Clears Level 2 IS-IS redistributed prefixes from the redistribution cache.
lspfull	Clears the IS-IS LSPFULL state.
network_mask	(Optional) The network ID in the A.B.C.D format for the network mask for the specific network prefix you want to clear from the RIB. If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.
network_prefix	(Optional) The network ID in the A.B.C.D format for the specific network prefix you want to clear from the redistribution Routing Information Base (RIB). If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.
rib redistribution	Clears prefixes in the IS-IS redistribution cache.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If the link-state PDU (LSP) becomes full because too many routes are redistributed, use the **clear isis lspfull** command to clear the state after the problem has been resolved.

We recommend that you use the **clear isis rib** command in a troubleshooting situation only when a Cisco Technical Assistance Center representative requests you to do so following a software error.

Examples

The following example clears the LSPFULL state:

```
ciscoasa# clear isis lspfull
```

The following example clears the network prefix 10.1.0.0 from the IP local redistribution cache:

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.

Command	Description
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).

Command	Description
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.



clear l – clear z

- clear lisp eid, on page 681
- clear local-host (Deprecated), on page 683
- clear logging asdm, on page 685
- clear logging buffer, on page 686
- clear logging counter, on page 687
- clear logging queue bufferwrap, on page 688
- clear mac-address-table, on page 689
- clear memory appcache-threshold, on page 690
- clear memory delayed-free-poisoner, on page 691
- clear memory profile, on page 692
- clear mfib counters, on page 693
- clear module, on page 694
- clear nac-policy, on page 696
- clear nat counters, on page 697
- clear nve, on page 698
- clear object, on page 699
- clear object-group, on page 700
- clear ospf, on page 701
- clear path-monitoring, on page 703
- clear pclu, on page 704
- clear phone-proxy secure-phones, on page 705
- clear pim counters, on page 706
- clear pim group-map, on page 707
- clear pim reset, on page 709
- clear pim topology, on page 710
- clear priority-queue statistics, on page 711
- clear process, on page 712
- clear resource usage, on page 713
- clear route, on page 715
- clear service-policy, on page 717
- clear service-policy inspect gtp, on page 719
- clear service-policy inspect m3ua, on page 721
- clear service-policy inspect radius-accounting, on page 723

- clear session, on page 724
- clear shared license, on page 726
- clear shun, on page 728
- clear snmp-server statistics, on page 729
- clear ssl, on page 730
- clear startup-config errors, on page 732
- clear sunrpc-server active, on page 733
- clear terminal, on page 734
- clear threat-detection rate, on page 735
- clear threat-detection scanning-threat, on page 736
- clear threat-detection service, on page 738
- clear threat-detection shun, on page 740
- clear threat-detection statistics, on page 742
- clear traffic, on page 744
- clear uauth, on page 745
- clear uc-ime, on page 747
- clear url-block block statistics, on page 749
- clear url-cache statistics, on page 751
- clear url-server, on page 753
- clear user-identity active-user-database, on page 754
- clear user-identity ad-agent statistics, on page 756
- clear user-identity statistics, on page 758
- clear user-identity user-not-found, on page 760
- clear user-identity user no-policy-activated, on page 762
- clear vpn cluster stats internal, on page 763
- clear vpn-sessiondb statistics, on page 764
- clear wccp, on page 767
- clear webvpn sso-server statistics, on page 768
- clear xlate, on page 769

clear lisp eid

To clear the ASA EID table, use the **clear lisp eid** command in privileged EXEC mode.

clear lisp eid [*ip_address*]

Syntax Description

ip_address	Removes the specified IP address from the EID table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	We introduced this command.

Usage Guidelines

The ASA maintains an EID table that correlates the EID and the site ID. The **clear lisp eid** command clears EID entries in the table.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.
3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.

4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

clear local-host (Deprecated)

To reinitalize per-client run-time states such as connection limits and embryonic limits, use the **clear local-host** command in privileged EXEC mode.

clear local-host [*ip_address*] [**all**] [**zone** [*zone_name*]]

Syntax Description

all	(Optional) Clears all connections, including to-the-box traffic. Without the **all** keyword, only through-the-box traffic is cleared.
ip_address	(Optional) Specifies the local host IP address.
zone [*zone_name*]	(Optional) Specifies zone connections.

Command Default

Clears all through-the-box run-time states.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.3(2)	The **zone** keyword was added.
9.16(1)	This command was deprecated. Use the **clear conn address** command to clear connections to local addresses.

Usage Guidelines

When you make security policy changes to the configuration, all *new* connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy using the **clear local-host** command. You can alternatively use the **clear conn** command for more granular connection clearing, or the **clear xlate** command for connections that use dynamic NAT.

The **clear local-host** command releases the hosts from the host license limit. You can see the number of hosts that are counted toward the license limit by entering the **show local-host** command.

Examples

The following example clears the run-time state and assocaited connections for the host 10.1.1.15:

```
ciscoasa# clear local-host 10.1.1.15
```

Related Commands

Command	Description
clear conn	Terminates connections in any state.
clear xlate	Clears a dynamic NAT session, and any connections using NAT.
show local-host	Displays the network states of local hosts.

clear logging asdm

To clear the ASDM logging buffer, use the **clear logging asdm** command in privileged EXEC mode.

clear logging asdm

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from the **clear pdm logging** command to the **clear asdm log** command.

Usage Guidelines

ASDM system log messages are stored in a separate buffer from the ASA system log messages. Clearing the ASDM logging buffer only clears the ASDM system log messages; it does not clear the ASA system log messages. To view the ASDM system log messages, use the **show asdm log** command.

Examples

The following example clears the ASDM logging buffer:

```
ciscoasa(config)# clear logging asdm
ciscoasa(config)#
```

Related Commands

Command	Description
show asdm log_sessions	Displays the contents of the ASDM logging buffer.

clear logging buffer

To clear the log buffer, use the **clear logging buffer** command in privileged EXEC mode.

clear logging buffer

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

This example shows how to clear the contents of the log buffer:

```
ciscoasa
#
clear logging buffer
```

Related Commands

Command	Description
logging buffered	Configures the log buffer.
show logging	Displays logging information.

clear logging counter

To clear the logged counters and statistics, use the **clear logging counter** command in privileged EXEC mode.

clear logging counter { **all** | **console** | **monitor** | **buffer** | **trap** | **asdm** | **mail** }

Syntax Description

counter	Clears the counters and statistics for the specified logging destination. Specify **all** to clear statistics for all logging destinations. Optionally, you can specify the destination that you want to clear the statistics for—**console**, **monitor**, **buffer**, **trap**, **asdm**, **mail**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.14(1)	This command was added.

Usage Guidelines

The **show logging** command provides statistics of messages logged for each logging category configured on the ASA. In order to clear these statistics/counters, use the **clear logging counter** command.

Examples

This example shows how to clear the counters of the logged messages:

```
ciscoasa
#
clear logging counter all
```

Related Commands

Command	Description
show logging	Displays logging information.

clear logging queue bufferwrap

To clear the saved log buffers (ASDM, internal, FTP, and flash), use the **clear logging queue bufferwrap** command in privileged EXEC mode.

clear logging queue bufferwrap

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following example shows how to clear the contents of the saved log buffers:

```
ciscoasa
#
clear logging queue bufferwrap
```

Related Commands

Command	Description
logging buffered	Configures the log buffer.
show logging	Displays logging information.

clear mac-address-table

To clear dynamic MAC address table entries, use the **clear mac-address-table** command in privileged EXEC mode.

clear mac-address-table [*interface_name*]

Syntax Description

interface_name	(Optional) Clears the MAC address table entries for the selected interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	—	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears the dynamic MAC address table entries:

```
ciscoasa# clear mac-address-table
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows MAC address table entries.

clear memory appcache-threshold

To clear the hit count of memory appcache-threshold, use the **clear memory appcache-threshold** command in privileged EXEC mode.

clear memory appcache-threshold

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

Whenever the application cache threshold is hit, the counter increments by 1. The **clear memory appcache-threshold** command clears the hit count of memory application cache threshold and resets to 0.

Examples

The following example clears the hit count of memory appcache-threshold:

```
ciscoasa# clear memory appcache-threshold
```

Related Commands

Command	Description
memory appcache-threshold enable	Enable memory appcache-threshold to restrict application cache allocations after reaching certain memory threshold
show memory appcache-threshold	Show the status and hit count of memory appcache-threshold

clear memory delayed-free-poisoner

To clear the delayed free-memory poisoner tool queue and statistics, use the **clear memory delayed-free-poisoner** command in privileged EXEC mode.

clear memory delayed-free-poisoner

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear memory delayed-free-poisoner** command returns all memory held in the delayed free-memory poisoner tool queue to the system without validation and clears the related statistical counters.

Examples

The following example clears the delayed free-memory poisoner tool queue and statistics:

```
ciscoasa# clear memory delayed-free-poisoner
```

Related Commands

Command	Description
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

clear memory profile

To clear the memory buffers held by the memory profiling function, use the **clear memory profile** command in privileged EXEC mode.

clear memory profile [**peak**]

Syntax Description

peak	(Optional) Clears the contents of the peak memory buffer.

Command Default

Clears the current "in use" profile buffer by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear memory profile** command releases the memory buffers held by the profiling function, and therefore requires that profiling stop before it is cleared.

Examples

The following example clears the memory buffers held by the profiling function:

```
ciscoasa# clear memory profile
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a text range of memory to profile.
show memory profile	Displays information about the memory usage (profiling) of the ASA.

clear mfib counters

To clear MFIB router packet counters, use the **clear mfib counters** command in privileged EXEC mode.

clear mfib counters [*group* [*source*]]

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

Command Default

When this command is used with no arguments, route counters for all routes are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears all MFIB router packet counters:

```
ciscoasa# clear mfib counters
```

Related Commands

Command	Description
show mfib count	Displays MFIB route and packet count data.

clear module

To clear information about the SSM on the ASAs, information about the SSC on the ASA 5505, information about the SSP installed on the ASA 5585-X, information about the IPS SSP installed on the ASA 5585-X, information about the ASA Services Module, and system information, use the **clear module** command in privileged EXEC mode.

clear module [*mod_id* | *slot*] [**all** | [**details** | **recover** | **log** [**console**]]]

Syntax Description

all	(Default) Clears all SSM information.
console	(Optional) Clears console log information for the module.
details	(Optional) Clears additional information, including remote management configuration for SSMs (for example, ASA-SSM-*x* 0).
log	(Optional) Clears log information for the module.
mod_id	Clears the module name used for software modules, such as IPS.
recover	(Optional) For SSMs, clears the settings for the **hw-module module recover** command. **Note** The **recover** keyword is valid only when you have created a recovery configuration for the SSM by using the **configure** keyword with the **hw-module module recover** command. (Optional) For an IPS module installed on the ASA 5512-X, 5515-X, 5525-X, 5545-X, or 5555-X, clears the settings for the **sw-module module** *mod_id* **recover configure image** *image_location* command.
slot	Clears the module slot number, which can be 0 or 1.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for the SSC was added.

Release	Modification
8.2(5)	Support for the ASA 5585-X and the IPS SSP on the ASA 5585-X was added.
8.4(2)	Support for a dual SSP installation was added.
8.5(1)	Support for the ASASM was added.
8.6(1)	Support for the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X was added.

Usage Guidelines

This command clears information about the SSC, SSM, ASASM, IPS SSP, and device and built-in interfaces.

Examples

The following example clears the recovery settings for an SSM:

```
ciscoasa# clear module 1 recover
```

Related Commands

Command	Description
hw-module module recover	Recovers an SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

clear nac-policy

To reset NAC policy usage statistics, use the **clear nac-policy** command in global configuration mode.

clear nac-policy [*nac-policy-name*]

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to reset usage statistics.

Command Default

If you do not specify a name, the CLI resets the usage statistics for all NAC policies.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example resets the usage statistics for the NAC policy named framework1:

```
ciscoasa
(config)#

clear nac-policy framework1
```

The following example resets all NAC policy usage statistics:

```
ciscoasa
(config)#

clear nac-policy
```

Related Commands

Command	Description
show nac-policy	Displays NAC policy usage statistics on the ASA.
show vpn-session_summary.db	Displays the number of IPsec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

clear nat counters

To clear NAT policy counters, use the **clear nat counters** command in global configuration mode.

clear nat counters [*src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

Syntax Description

dst_ifc	(Optional) Specifies destination interface to filter.
dst_ip	(Optional) Specifies destination IP address to filter.
dst_mask	(Optional) Specifies mask for destination IP address.
src_ifc	(Optional) Specifies source interface to filter.
src_ip	(Optional) Specifies source IP address to filter.
src_mask	(Optional) Specifies mask for source IP address.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(4)	This command was added.

Examples

This example shows how to clear the NAT policy counters:

```
ciscoasa(config)# clear nat counters
```

Related Commands

Command	Description
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
nat-control	Enables or disables NAT configuration requirements.
show nat counters	Displays the protocol stack counters.

clear nve

To clear NVE source interface statistics, use the **clear nve** command in privileged EXEC mode.

clear nve 1

Syntax Description

1	Specifies the NVE instance, which is always 1.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

This command clears the parameters, status and statistics of a NVE interface, status of its carrier interface, IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

Examples

The following example clears the NVE interface statistics:

```
ciscoasa# clear nve 1
```

Related Commands

Command	Description
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

clear object

To clear the hit counts of network-service objects, use the **clear object** command in privileged EXEC mode..

clear object [**id** *object_name* | **network-service**]

Syntax Description

id *name*	(Optional) Clear the counter of the specified network-service object. Capitalization matters. For example “object-name” does not match “Object-Name.”
network-service	(Optional.) Clear the counters of all network-service objects. This action is the same as you would get by specifying no parameters on the command.

Command Default

Without parameters, all objects hit counts are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was added.

Example

The following example clears the hit counts of all objects.

```
ciscoasa# clear object
```

Related Commands

Command	Description
show object	Shows network-service objects and their hit counts.

clear object-group

To clear the hit counts of objects in a network object group, use the **clear object-group** command in privileged EXEC mode.

clear object-group [**id** *object_group_name* | **network-service**]

Syntax Description

object_group_name	The name of the object group whose counters should be cleared. If you do not specify a name, counters for all object groups are cleared.
network-service	(Optional.) Clear the counters of all network-service object groups.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.17(1)	This command was extended to work with network-service objects.
9.24(1)	The **network-service** keyword was added.

Examples

The following example shows how to clear the network object hit count for the network object group named “Anet”:

```
ciscoasa# clear object-group id Anet
```

Related Commands

Command	Description
show object-group	Shows object group information and hit counts.

clear ospf

To clear OSPF process information, use the **clear ospf** command in privileged EXEC mode.

clear ospf [*pid*] { **process counters** }

Syntax Description

counters	Clears the OSPF counters.
pid	(Optional) Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
process	Restarts the OSPF routing process.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command does not remove any part of the configuration. Use the **no** form of the configuration commands to clear specific commands from the configuration or use the **clear configure router ospf** command to remove all global OSPF commands from the configuration.

Note The **clear configure router ospf** command does not clear OSPF commands entered in interface configuration mode.

Examples

The following example shows how to clear the OSPF neighbor counters:

```
ciscoasa# clear ospf counters
```

Related Commands

Command	Description
clear configure router	Clears all global router commands from the running configuration.

clear path-monitoring

To clear path monitoring settings on the interface, use the **clear path-monitoring** command.

clear path-monitoring [**interface** *name*]

Syntax Description

Interface *name*	Removes the path-monitoring settings configured on the specified interface.

Command History

Release	Modification
9.18(1)	This command was introduced.

Examples

The following example clears the path monitoring settings on the *outside1* interface:

```
> clear path-montoring outside1
```

Related Commands

Command	Description
show path-monitoring	Shows path-monitoring metric information.

clear pclu

To clear PC logical update statistics, use the **clear pclu** command in privileged EXEC mode.

clear pclu

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example clears PC information:

```
ciscoasa# clear pclu
```

clear phone-proxy secure-phones

To clear the secure phone entries in the phone proxy database, use the **clear phone-proxy secure-phones** command in privileged EXEC mode.

clear phone-proxy secure-phones [*mac_address* | **noconfirm**]

Syntax Description

mac_address	Removes the IP phone from the phone proxy database with the specified MAC address.
noconfirm	Removes all the secure phone entries in the phone proxy database without prompting for confirmation. If you do not specify the **noconfirm** keyword, you are prompted to confirm whether to remove all the secure phone entries.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Because secure phones always request a CTL file upon bootup, the phone proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout (via the **timeout secure-phones** command). Alternatively, you can use the **clear phone-proxy secure-phones** command to clear the phone proxy database without waiting for the configured timeout.

Examples

The following example clears secure entries in the phone proxy database:

```
ciscoasa# clear phone-proxy secure-phones 001c.587a.4000
```

Related Commands

Command	Description
timeout secure-phones	Configures the idle timeout after which the secure phone entry is removed from the phone proxy database.

clear pim counters

To clear the PIM traffic counters, use the **clear pim counters** command in privileged EXEC mode.

clear pim counters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command only clears the traffic counters. To clear the PIM topology table, use the **clear pim topology** command.

Examples

The following example clears the PIM traffic counters:

```
ciscoasa# clear pim counters
```

Related Commands

Command	Description
clear pim reset	Forces MRIB synchronization through reset.
clear pim topology	Clears the PIM topology table.
show pim traffic	Displays the PIM traffic counters.

clear pim group-map

To delete group-to-rendezvous point (RP) mapping entries from the RP mapping cache, use the clear pim group-map command.

clear pim group-map [*rp-address*]

Syntax Description

rp-address	Rendezvous point mapping address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was introduced.

Examples

The following example deletes group-RP mapping entries at the 23.23.23.2 RP address:

```
ciscoasa(config)# sh pim group-map
Group Range         Proto Client Groups RP address      Info

224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    BSR    0      23.23.23.2      RPF: Gi0/3,23.23.23.2
ciscoasa(config)# clear pim group-map 23.23.23.2
ciscoasa(config)# sh pim group-map
Group Range         Proto Client Groups RP address      Info

224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    static 0      0.0.0.0         RPF: ,0.0.0.0
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears PIM traffic counters.

clear pim reset

To force MRIB synchronization through reset, use the **clear pim reset** command in privileged EXEC mode.

clear pim reset

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

All information from the topology table is cleared, and the MRIB connection is reset. This command can be used to synchronize states between the PIM topology table and the MRIB database.

Examples

The following example clears the topology table and resets the MRIB connection:

```
ciscoasa# clear pim reset
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears PIM traffic counters.

clear pim topology

To clear the PIM topology table, use the **clear pim topology** command in privileged EXEC mode.

clear pim topology [*group*]

Syntax Description

group	(Optional) Specifies the multicast group address or name to be deleted from the topology table.

Command Default

Without the optional *group* argument, all entries are cleared from the topology table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command clears existing PIM routes from the PIM topology table. Information obtained from the MRIB table, such as IGMP local membership, is retained. If a multicast group is specified, only those group entries are cleared.

Examples

The following example clears the PIM topology table:

```
ciscoasa# clear pim topology
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim reset	Forces MRIB synchronization through reset.
clear pim counters	Clears PIM traffic counters.

clear priority-queue statistics

To clear the priority-queue statistics counters for an interface or for all configured interfaces, use the **clear priority-queue statistics** command in either global configuration or privileged EXEC mode.

clear priority-queue statistics [*interface-name*]

Syntax Description

interface-name	(Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Command Default

If you omit the interface name, this command clears the priority-queue statistics for all configured interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows the use of the **clear priority-queue statistics** command in privileged EXEC mode to remove the priority queue statistics for the interface named “test”:

```
ciscoasa# clear priority-queue statistics test
ciscoasa#
```

Related Commands

Command	Description
clear configure priority queue	Removes the priority-queue configuration from the named interface.
priority-queue	Configures priority queueing on an interface.
show priority-queue statistics	Shows the priority queue statistics for a specified interface or for all interfaces.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

clear process

To clear statistics for specified processes running on the ASA, use the **clear process** command in privileged EXEC mode.

clear process [**cpu-hog** | **internals**]

Syntax Description

cpu-hog	Clears CPU hogging statistics.
internals	Clears process internal statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to clear CPU hogging statistics:

```
ciscoasa# clear process cpu-hog
ciscoasa#
```

Related Commands

Command	Description
cpu hog granular-detection	Triggers real-time CPU hog detection information.
show processes	Displays a list of the processes that are running on the ASA.

clear resource usage

To clear resource usage statistics, use the **clear resource usage** command in privileged EXEC mode.

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** { [**rate**] *resource_name* | **all** }]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to clear statistics. Specify **all** (the default) for all contexts.
resource [**rate**] *resource_name*	Clears the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to clear the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm**—ASDM management sessions. • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects**—Application inspections. • **hosts**—Hosts that can connect through the ASA. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **ssh**—SSH sessions. • **syslogs**—Syslog messages. • **telnet**—Telnet sessions. • (Multiple mode only) **VPN Other**—Site-to-site VPN sessions. • (Multiple mode only) **VPN Burst Other**—Site-to-site VPN burst sessions. • **xlates**—NAT translations.
summary	(Multiple mode only) Clears the combined context statistics.
system	(Multiple mode only) Clears the system-wide (global) usage statistics.

Command Default

For multiple context mode, the default context is **all**, which clears resource usage for every context. For single mode, the context name is ignored and all resource statistics are cleared.

The default resource name is **all**, which clears all resource types.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example clears all resource usage statistics for all contexts, but not the system-wide usage statistics:

```
ciscoasa# clear resource usage
```

The following example clears the system-wide usage statistics:

```
ciscoasa# clear resource usage system
```

Related Commands

Command	Description
context	Adds a security context.
show resource types	Shows a list of resource types.
show resource usage	Shows the resource usage of the ASA.

clear route

To remove dynamically learned routes from the routing table, use the **clear route** command in privileged EXEC mode.

clear route [**management-only**] [*ip_address* [*ip_mask*]]

Syntax Description

ip_address [*ip_mask*]	Specifies the destination IP address and, optionally, subnet mask of the route to be removed. If you omit this keyword, all dynamic routes are deleted.
management-only	Clears the IPv4 management routing table. If you omit this keyword, the route is removed from the data interface routing table.

Command Default

All dynamically learned routes are removed from the data interface routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.5(1)	The **management-only** keyword was added.
9.17(1)	Starting with version 9.17, for units that are part of a high availability group or cluster, this command is available on the active or control unit only. The command clears routes from all units in the HA group or cluster. In previous releases, the command clears routes on the unit on which it is run only.

Usage Guidelines

Use the **clear route** command to recover any missing routes. Whenever this command is executed, all routes from global RIB are deleted. All routes (dynamic or static) are pushed to global RIB by the respective modules (protocols).

On the other hand, when the best route is installed on the global RIB, the same is redistributed to peers and NP table. This process runs sequentially on multiple threads. The time taken to complete a cycle depends on the number of routes on the global RIB.

Thus, if you are using the **clear route** command consecutively, ensure to follow a minimum time interval of 30 seconds and a maximum time interval of 120 seconds. If this command is executed multiple times without following the recommended time interval, there is a chance of the distributed routes getting deleted, resulting in losing the routes from the RIB.

Examples

The following example shows how to remove all dynamically learned routes:

```
ciscoasa# clear route
```

The following example shows how to remove dynamically learned routes for a specific address.

```
ciscoasa# clear route 10.118.86.3
```

Related Commands

Command	Description
show route	Displays route information.
show running-config route	Displays configured routes.

clear service-policy

To clear operational data or statistics (if any) for enabled policies, use the **clear service-policy** command in privileged EXEC mode.

clear service-policy [**global** | **interface** *intf*] [**user-statistics**]

Syntax Description

global	(Optional) Clears the statistics of the global service policy.
interface *intf*	(Optional) Clears the service policy statistics of a specific interface.
user-statistics	(Optional) Clears the global counters for user statistics but does not clear the per-user statistics. Per-user or per-user-group statistics can still be seen using **show user-identity statistics** command. When the **accounting** keyword for the **user-statistics** command is specified, all global counters for sent packets, received packets, and sent dropped packets are cleared. When the **scanning** keyword **user-statistics** command is specified, the global counter for sent dropped packets is cleared. For the ASA to collect these user statistics, you must configure a policy map to collect user statistics. See the **user-statistics** command in this guide.

Command Default

By default, this command clears all the statistics for all enabled service policies.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Some inspection engines let you selectively clear statistics. See the **clear service-policy inspect** commands.

Examples

The following example shows how to clear service policy statistics for the outside interface.

```
ciscoasa# clear service-policy interface outside
```

Related Commands

Command	Description
clear service-policy inspect gtp	Clears service policy statistics for the GTP inspection engine.
clear service-policy inspect radius-accounting	Clears service policy statistics for the RADIUS accounting inspection engine.
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.
clear configure service-policy	Clears service policy configurations.
service-policy	Configures service policies.

clear service-policy inspect gtp

To clear GTP inspection statistics, use the **clear service-policy inspect gtp** command in privileged EXEC mode.

clear service-policy inspect gtp { **pdp-context** { **all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num* } | **requests** [*name* | **map** *name* | **version** *version_num*] | **statistics** [**gsn** *IP_address* | *IP_address*] }

Syntax Description

pdp-context { **all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num* }	Clears Packet Data Protocol (PDP) or bearer context information. You can specify the contexts to clear using the following keywords: • **all** —Clear all contexts. • **apn** *ap_name* —Clear contexts for the specified access point name. • **imsi** *IMSI_value* —Clear contexts for the specified IMSI hexadecimal number. • **ms-addr** *IP_address* —Clear contexts for the specified mobile subscriber (MS) IP address. • **tid** *tunnel_ID* —Clear contexts for the specified GTP tunnel ID, a hexadecimal number. • **version** *version_num* —Clear contexts for the specified GTP version (0-255).
requests [*name* | **map** *name* | **version** *version_num*	Clears GTP requests. You can optionally limit the requests to clear using the following parameters: • *name* —Clears requests associated with the specified GTP inspection policy map. This option is not available starting with 9.5(1). • **map** *name* —(9.5(1)+.) Clears requests associated with the specified GTP inspection policy map. • **version** *version_num* —(9.5(1)+.) Clears requests for the specified GTP version (0-255).
statistics [**gsn** *IP_address* | *IP_address*]	Clears GTP statistics for the **inspect gtp** command. You can clear the statistics for a specific endpoint by specifying the endpoint's address on the **gsn** keyword. Starting with 9.5(1), specify the address only, do not include the **gsn** keyword.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(1)	The following changes were made: • The **gsn** keyword on the **statistics** option was removed. To clear statistics for an endpoint, simply specify the endpoint IP address. • The **version** keyword was added to the **requests** option. The **map** keyword was added for the policy map name, replacing the ability to enter the map name directly after the **requests** option. • Support for IPv6 addresses.

Usage Guidelines

Use this command to clear statistics from GTP inspection. Use the **show** version of this command to view the statistics.

Examples

The following example clears GTP statistics:

```
ciscoasa# clear service-policy inspect gtp statistics
```

Related Commands

Commands	Description
inspect gtp	Enables GTP inspection.
show service-policy inspect gtp	Displays GTP statistics.

clear service-policy inspect m3ua

To clear M3UA inspection statistics, use the **clear service-policy inspect m3ua** command in privileged EXEC mode.

clear service-policy inspect m3ua { **drops** | **endpoint** [*ip_address*] | **session** [[**assocID** *hex_number*] }

Syntax Description

drops	Clears M3UA drop statistics.
endpoint [*ip_address*]	Clears M3UA endpoint statistics. You can optionally include the IP address of an endpoint to clear only the statistics for that endpoint.
session [**assocID** *hex_number*]	Clears all M3UA sessions, which are tracked if you enable strict application server process (ASP) state validation. If you want to clear a specific section, add the **assocID** keyword with the hexadecimal session number. Use the **show service-policy inspect m3ua session** command to see the current sessions and their association IDs.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.
9.7(1)	The **session** keyword was added.

Usage Guidelines

Use this command to clear statistics or sessions from M3UA inspection. Use the **show** version of this command to view the statistics and sessions.

Examples

The following example clears M3UA endpoint statistics:

```
ciscoasa# clear service-policy inspect m3ua endpoint
```

The following example clears a specific M3UA session:

```
ciscoasa(config)# show service-policy inspect m3ua session

1 in use, 1 most used
Flags: d - double exchange      , s - single exchange
AssocID: c0bbe629 in Down state, idle:0:00:06, timeout:0:30:00, s
ciscoasa(config)# clear service-policy inspect m3ua session assocID c0bbe629
```

Related Commands

Commands	Description
inspect m3ua	Enables M3UA inspection.
show service-policy inspect m3ua	Displays the M3UA statistics.
strict-asp-state	Enables strict M3UA ASP state validation.

clear service-policy inspect radius-accounting

To clear RADIUS accounting users, use the **clear service-policy inspect radius-accounting** command in privileged EXEC mode.

clear service-policy inspect radius-accounting users { **all** | *ip_address* | *policy_map* }

Syntax Description

all	Clears all users.
ip_address	Clears a user with this IP address.
policy_map	Clears users associated with this policy map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example clears all RADIUS accounting users:

```
ciscoasa# clear service-policy inspect radius-accounting users all
```

clear session

To delete the contents of a configuration session or to reset its access flag, use the **clear session** command in global configuration mode.

clear session *session_name* { **access** | **configuration** }

Syntax Description

session_name	The name of an existing configuration session. Use the **show configuration session** command for a list of current sessions.
access	Clears the access flag. The flag indicates that a session is being edited. Clear this flag only if you know the edit session was abandoned and you need to get into the session to complete the changes.
configuration	Clears the configuration changes made within the session without deleting the session.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Use this command in conjunction with the **configure session** command, which creates isolated sessions for editing ACLs and their objects.

The primary use of this command is to reset the access flag. When you open a session, the flag marks it as being edited. If you then break your connection to the ASA without cleanly exiting the session, the flag stays set, and this can prevent you from opening the session again. If you are certain no one is actually editing the session, you can reset the flag to regain access.

You can also use this command to empty the session of changes without deleting the session. If you decide you no longer need a session you created, and you do not want to commit the changes defined in the session, use the **clear configuration session** command to delete the session and the changes it contains.

Examples

The following example resets the access flag on my-session:

```
ciscoasa(config)# clear session my-session access
```

Related Commands

Command	Description
clear configuration session	Deletes a configuration session and its contents.
configure session	Creates or opens a session.
show configuration session	Shows the changes made in each current session.

clear shared license

To reset shared license statistics, shared license client statistics, and shared license backup server statistics to zero, use the **clear shared license** command in privileged EXEC mode.

clear shared license [**all** | **backup** | **client** [*hostname*]]

Syntax Description

all	(Optional) Clears all statistics. This is the default setting.
backup	(Optional) Clears statistics for the backup server.
client	(Optional) Clears statistics for all participants.
hostname	(Optional) Clears statistics for a particular participant.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The shared license counters include statistical data as well as error data.

Examples

The following example shows how to reset all shared license counters:

```
ciscoasa# clear shared license all
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.

Command	Description
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

clear shun

To disable all the shuns that are currently enabled and clear the shun statistics, use the **clear shun** command in privileged EXEC mode.

clear shun [**statistics**]

Syntax Description

statistics	(Optional) Clears the interface counters only.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to disable all the shuns that are currently enabled and clear the shun statistics:

```
ciscoasa(config)# clear shun
```

Related Commands

Command	Description
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.
show shun	Displays the shun information.

clear snmp-server statistics

To clear SNMP server statistics (SNMP packet input and output counters), use the **clear snmp-server statistics** command in privileged EXEC mode.

clear snmp-server statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to clear SNMP server statistics:

```
ciscoasa
#
clear snmp-server statistics
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show snmp-server statistics	Displays SNMP server configuration information.

clear ssl

To clear SSL information for debugging purposes, use the **clear ssl** command in privileged EXEC mode.

clear ssl { **cache** [**all** | **errors** | **mib** | **objects** }

Syntax Description

all	Clears all sessions and statistics in SSL session cache.
cache	Clears expired sessions in SSL session cache.
errors	Clears ssl errors.
mib	Clears SSL MIB statistics.
objects	Clears SSL object statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.5(2)	Support for multiple context mode was added.

Usage Guidelines

DTLS cache is never cleared because it would impact Secure Client functionality.

Examples

The following example shows clearing ssl cache and clearing all sessions and statistics in SSL session cache.

```
ciscoasa# clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
ciscoasa# clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
```

```
No SSLDEV session cache
DLTS caches are not cleared
```

clear startup-config errors

To clear configuration error messages from memory, use the **clear startup-config errors** command in privileged EXEC mode.

clear startup-config errors

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To view configuration errors generated when the ASA loaded the startup configuration, use the **show startup-config errors** command.

Examples

The following example clears all configuration errors from memory:

```
ciscoasa# clear startup-config errors
```

Related Commands

Command	Description
show startup-config errors	Shows configuration errors generated when the ASA loaded the startup configuration.

clear sunrpc-server active

To clear the pinholes opened by Sun RPC application inspection, use the **clear sunrpc-server active** command in privileged EXEC mode.

clear sunrpc-server active

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **clear sunrpc-server active** command to clear the pinholes opened by Sun RPC application inspection that allow service traffic, such as NFS or NIS, to pass through the ASA.

Examples

The following example shows how to clear the SunRPC services table:

```
ciscoasa# clear
 sunrpc-server
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the ASA.
inspect sunrpc	Enables or disables Sun RPC application inspection and configures the port used.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.
show sunrpc-server active	Displays information about active Sun RPC services.

clear terminal

To clear the terminal settings for the current CLI session and use the defaults, use the **clear terminal** command in privileged EXEC mode.

clear terminal { **interactive** | **pager** [[**lines**] *number*] }

Syntax Description

interactive	Clears the interactive help setting (when you enter **?** at the CLI). The default is enabled.
pager [[**lines**] *number*]]	Clears the setting for the number of lines in a page before the ---more--- prompt appears. The default is 24.

Command Default

The default terminal behavior is:

- **interactive**—Enabled
- **pager**—24 lines

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to clear the pager setting:

```
ciscoasa# clear
 terminal pager
```

Related Commands

Command	Description
terminal pager	Sets the number of lines on a page before the “---More---” prompt appears.
terminal interactive	Enables or disables help when you enter ? at the CLI.

clear threat-detection rate

To clear statistics when you enable basic threat detection using the **threat-detection basic-threat** command, use the **clear threat detection rate** command in privileged EXEC mode.

clear threat-detection rate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example clears the rate statistics:

```
ciscoasa# clear threat-detection rate
```

Related Commands

Command	Description
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection scanning-threat

To clear the attackers and targets after you enable scanning threat detection with the **threat-detection scanning-threat** command, use the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection scanning-threat [**attacker** [*ip_address* [*mask*]] | **target** [*ip_address* [*mask*]]

Syntax Description

attacker	(Optional) Clears only attackers.
ip_address	(Optional) Clears a specific IP address.
mask	(Optional) Sets the subnet mask.
target	(Optional) Clears only targets.

Command Default

If you do not specify an IP address, all hosts are released.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

To view current attackers and targets, use the **show threat-detection scanning-threat** command.

Examples

The following example shows targets and attackers with the **show threat-detection scanning-threat** command, and then clears all targets:

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
```

```
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
ciscoasa# clear threat-detection scanning-threat target
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection service

To remove tracked entries and statistics for Threat Detection for VPN Services, use the **clear threat-detection service** command in privileged EXEC mode.

clear threat-detection service [*service*] [**statistics** | **entries**]

Syntax Description

entries	(Optional.) Clear only the entries being tracked but keep the statistics. For example, clear the list of the IP addresses that have had failed authentication attempts.
service	(Optional.) Clear information for the specified service only. Enter one of the following: • **remote-access-authentication** • **remote-access-client-initiations** • **invalid-vpn-access**
statistics	(Optional.) Clear the statistics but not the entries being tracked.

Command Default

If you specify no options, the command clears all the tracked entries and resets the statistics for all services.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	Yes	—

Command History

Release	Modification
9.16(4), 9.20(3)	This command was introduced.

Usage Guidelines

This command does not remove any shuns applied by the services. To remove all shuns, use **clear shun** command. To remove individual shuns, use the **no shun** *ip_address* [**interface** *if_name*] command.

Example

The following example clears statistics and entries for all services.

```
ciscoasa# clear threat-detection service
```

Related Commands

Command	Description
clear shun	Removes all shuns.
show threat-detection service	Shows threat detection service entries and statistics.
[no]shun	Shuns an address, or clears the shun on a specific address.
threat-detection service	Configures Threat Detection for VPN Services.

clear threat-detection shun

To release the currently shunned hosts after you enable scanning threat detection with the **threat-detection scanning-threat** command and automatically shunning attacking hosts, use the **clear threat-detection shun** command in privileged EXEC mode.

clear threat-detection shun [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Releases a specific IP address from being shunned. The address can be IPv4 or IPv6 (with optional prefix length).
mask	(Optional) Sets the subnet mask for the shunned host IP address.

Command Default

If you do not specify an IP address, all hosts are released.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.20(1)	Support for IPv6 addresses was added.

Usage Guidelines

To view currently shunned hosts, use the **show threat-detection shun** command.

Examples

The following example views currently shunned hosts with the **show threat-detection shun** command, and then releases host 10.1.1.6 from being shunned:

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
ciscoasa# clear threat-detection shun 10.1.1.6 255.255.255.255
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.

Command	Description
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection statistics

To clear the statistics after you enable TCP Intercept statistics with the **threat-detection statistics tcp-intercept** command, use the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection statistics [**tcp-intercept**]

Syntax Description

tcp-intercept	(Optional) Clears TCP Intercept statistics.

Command Default

Clears TCP Intercept statistics.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

To view TCP Intercept statistics, enter the **show threat-detection statistics top** command.

Examples

The following example shows TCP Intercept statistics with the **show threat-detection statistics top tcp-intercept** command, and then clears all statistics:

```
ciscoasa# show threat-detection statistics top tcp-intercept
Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
ciscoasa# clear threat-detection statistics
```

Related Commands

Command	Description
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection statistics	Enables threat detection statistics.

clear traffic

To reset the counters for transmit and receive activity, use the **clear traffic** command in privileged EXEC mode.

clear traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The clear traffic command resets the counters for transmit and receive activity that is displayed with the **show traffic** command. The counters indicate the number of packets and bytes moving through each interface since the last clear traffic command was entered or since the ASA came online. And the number of seconds indicate the duration the ASA has been online since the last reboot.

Examples

The following example shows the **clear traffic** command:

```
ciscoasa# clear
 traffic
```

Related Commands

Command	Description
show traffic	Displays the counters for transmit and receive activity.

clear uauth

To delete all the cached authentication and authorization information for a user or for all users, use the **clear uauth** command in privileged EXEC mode.

clear uauth [*username*]

Syntax Description

username	(Optional) Specifies the user authentication information to remove by username.

Command Default

Omitting the *username* argument deletes the authentication and authorization information for all users.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear uauth** command deletes the AAA authorization and authentication caches for one user or for all users, which forces the user or users to reauthenticate the next time that they create a connection.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. If the user attempts to access a service that has been cached from the correct host, the ASA considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The cache allows up to 16 address and service pairs for each user host.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPsec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see the AAA commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

The following example shows how to cause the user to reauthenticate:

```
ciscoasa(config)# clear uauth user
```

Related Commands

Command	Description
aaa authentication	Enables, disables, or views LOCAL, TACACS+ or RADIUS user authentication (on a server designated by the aaa-server command).
aaa authorization	Enables, disables, or views TACACS+ or RADIUS user authorization (on a server designated by the aaa-server command).
show uauth	Displays current user authentication and authorization information.
timeout	Sets the maximum idle time duration.

clear uc-ime

To clear the counters used to display statistics about the Cisco Intercompany Media Engine proxy, use the **clear uc-ime** command in privileged EXEC mode.

clear uc-ime [[**mapping-service-sessions** | **signaling-sessions** | **fallback-notification**] **statistics**]

Syntax Description

fallback-notification	(Optional) Clears the counters for fallback notification statistics.
mapping-service-sessions	(Optional) Clears the counters for mapping-service-session statistics.
signaling-sessions	(Optional) Clears the counters for signaling-session statistics.
statistics	(Optional) The keyword to configure which counters to clear for the Cisco Intercompany Media Engine proxy.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Examples

The following example clears the counters which are used to display signaling-sessions statistics:

```
ciscoasa# clear configure signaling-sessions statistics
```

Related Commands

Command	Description
clear configure uc-ime	Clears the running configuration for the Cisco Intercompany Media Engine proxy on the ASA.
show running-config uc-ime	Shows the running configuration of the Cisco Intercompany Media Engine proxy.
show uc-ime	Displays statistical or detailed information about fallback notifications, mapping-service sessions, and signaling sessions.

Command	Description
uc-imc	Creates the Cisco Intercompany Media Engine proxy instance on the ASA.

clear url-block block statistics

To clear the block buffer usage counters, use the clear **url-block block statistics** command in privileged EXEC mode.

clear url-block block statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear url-block block statistics** command clears the block buffer usage counters, except for the Current number of packets held (global) counter.

Examples

The following example clears the URL block statistics and displays the status of the counters after they have been cleared:

```
ciscoasa# clear url-block block statistics
ciscoasa# show url-block block statistics
URL Pending Packet Buffer Stats with max block  0
--------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
 | exceeding url-block buffer limit: | 0
 | HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.

Commands	Description
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear url-cache statistics

To remove **url-cache** command statements from the configuration, use the clear **url-cache** command in privileged EXEC mode.

clear url-cache statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear url-cache** command removes URL cache statistics from the configuration.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enter the **url-cache** command to increase throughput. Accounting logs are updated for Websense protocol Version 4 and for N2H2 URL filtering while using the **url-cache** command.

Examples

The following example clears the URL cache statistics:

```
ciscoasa# clear url-cache statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.

Commands	Description
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear url-server

To clear URL filtering server statistics, use the clear **url-server** command in privileged EXEC mode.

clear url-server statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear url-server** command removes URL filtering server statistics from the configuration.

Examples

The following example clears the URL server statistics:

```
ciscoasa# clear url-server statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear user-identity active-user-database

To set the status of specified users to logged out for the Identity Firewall, use the **clear user-identity active-user-database** command in privileged EXEC mode.

clear user-identity active-user-database [**user** [*domain_nickname*\ ] *use_rname*] | **user-group** [*domain_nickname*\\ ] *user_group_name*]

Syntax Description

*domain_nickname**user_group_name*	Specifies a user group for which to clear statistics. The *group_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain _NetBIOS_name \group _name* contains a space, you must enclose the domain name and user name in quotation marks.
domain_nickname \use_rname	Specifies a user for which to clear statistics. The *user_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain_NetBIOS_name\user _name* contains a space, you must enclose the domain name and user name in quotation marks.
user	Specifies to clear statistics for users.
user-group	Specifies to clear statistics for user groups.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command sets the status of the specified user, all users belong to the specified user group, or all users to logged out.

When you specify the **user-group** keyword, the status of all users belong to the specified user group are set to logged out. When you do not specify the *domain_nickname* argument with the **user-group** keyword, users in the groups with *user_group_name* in default domain are given the logged out status.

When you specify the **user** keyword, the status of the specified user is set to logged out. When you do not specify the *domain_nickname* argument with the **user** keyword, the user with *user_name* in default domain receives a logged out status.

When you do not specify either the **user** or **user-group** keywords, all users have their status set to logged out.

Examples

The following example sets the status of all users in user group users1 in the SAMPLE domain to logged out:

```
ciscoasa# clear user-identity active-user-database user-group SAMPLE\users1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity user active	Displays the active users for the Identify Firewall.

clear user-identity ad-agent statistics

To clear the AD Agent statistics for the Identity Firewall, use the **clear user-identity ad-agent statistics** command in privileged EXEC mode.

clear user-identity ad-agent statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The ASA maintains the following information about the primary and secondary AD Agents:

- Status of the AD Agents
- Status of the domains
- Statistics for the AD Agents

Use the **clear user-identity ad-agent statistics** command to clear the statistics data of AD Agents.

Examples

The following example clears the AD Agent statistics for the Identity Firewall:

```
ciscoasa# clear user-identity ad-agent statistics
ciscoasa# show user-identity ad-agent statistics
 Primary AD Agent               Total  Last Activity
 -------------------------  ----------  ------------------------
 Input packets:                     0  N/A
 Output packets:                    0  N/A
 Send updates:                      0  N/A
 Recv updates:                      0  N/A
 Keepalive failed:                  0  N/A
 Send update failed:                0  N/A
 Query failed:                      0  N/A
 Secondary AD Agent             Total  Last Activity
 -------------------------  ----------  ------------------------
```

```
Input packets:                  0  N/A
Output packets:                 0  N/A
Send updates:                   0  N/A
Recv updates:                   0  N/A
Keepalive failed:               0  N/A
Send update failed:             0  N/A
Query failed:                   0  N/A
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity ad-agent [**statistics**]	Displays statistical information about the AD Agent for the Identity Firewall.

clear user-identity statistics

To clear the counters used to display statistics about the Identity Firewall, use the **clear user-identity statistics** command in privileged EXEC mode.

clear user-identity statistics [**user** [*domain_nickname*\ ] *use_rname*] | **user-group** [*domain_nickname*\\ ] *user_group-name*]

Syntax Description

*domain_nickname**user_group_name*	Specifies a user group for which to clear statistics. The *group_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain _NetBIOS_name \group _name* contains a space, you must enclose the domain name and user name in quotation marks.
domain_nickname *use_rname*	Specifies a user for which to clear statistics. The *user_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If *domain_NetBIOS_name**user _name* contains a space, you must enclose the domain name and user name in quotation marks.
user	Specifies to clear statistics for users.
user-group	Specifies to clear statistics for user groups.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

When *domain_nickname* is not specified before *user_group_name*, the ASA removes the Identity Firewall statistics for the group with *user_group_name* in the default domain.

When *domain_nickname* is not specified before *user_name*, the ASA removes the Identity Firewall statistics for the user with *user_name* in the default domain.

Examples

The following example clears the counters which are used to display statistics for a user group:

```
ciscoasa# clear user-identity statistics user-group SAMPLE\users1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity statistics	Displays statistics for a user or user group for the Identify Firewall.

clear user-identity user-not-found

To clear the ASA local user-not-found database for the Identity Firewall, use the **clear user-identity user-not-found** command in privileged EXEC mode.

clear user-identity user-not-found

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The ASA maintains a local user-not-found database of the IP addresses not found in Microsoft Active Directory. The ASA keeps only the last 1024 packets (contiguous packets from the same source IP address are treated as one packet) of the user-not-found list and not the entire list in the database.

User the **clear user-identity user-not-found** command to clear the local database on the ASA.

Tip Use the **show user-identity user-not-found** command to display the IP addresses of the users who are not found in Microsoft Active Directory.

Examples

The following example clears the local user-not-found database for the Identity Firewall:

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
ciscoasa# clear user-identity user-not-found
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity user-not-found	Displays the IP addresses of the Active Directory users not found in the ASA user-not-found database.

clear user-identity user no-policy-activated

To clear the local records on the ASA of users who are not activated for the Identity Firewall, use the **clear user-identity user no-policy-activated** command in privileged EXEC mode.

clear user-identity user no-policy-activated

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Use the **clear user-identity user no-policy-activated** to clear the local records of users not activated by any security policy, meaning the user is not part of an activated user group or not referenced in an access list or service policy configuration.

The **clear user-identity user no-policy-activated** command also clears the IP addresses of users who are active but not activated.

When you create a user group for the Identity Firewall, it must be activated, meaning the group is an import user group (defined as a user group in an access list or service policy configuration) or a local user group (defined in an object-group user).

Examples

The following example clears the local records on the ASA for users who are not activated:

```
ciscoasa# clear user-identity user no-policy-activated
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.
show user-identity group	Displays the list of activated user groups for the Identity Firewall.

clear vpn cluster stats internal

To clear the internal counters for VPN clustering, use this command in global configuration or privileged EXEC mode.

clear vpn cluster stats internal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.9(1)	Command added.

Related Commands

Command	Description
show vpn cluster stats internal	Clear all VPN cluster counters.

clear vpn-sessiondb statistics

To clear information about VPN sessions, including all statistics or specific sessions or protocols, use the clear **vpn-sessiondb statistics** command in privileged EXEC mode.

clear vpn-sessiondb { **all** | **anyconnect** | **failover** | **email-proxy** | **global** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *name* | **vpn-lb** | **webvpn** }

Syntax Description

all	Clears statistics for all sessions.
anyconnect	**Clears statistics for AnyConnect VPN client sessions.**
failover	Clears statistics for failover IPsec sessions.
email-proxy	(Deprecated) Clears **statistics for** e-mail proxy sessions.
global	Clears **statistics for** global session data.
index *indexnumber*	Clears statistics of a single session by index number. The output of the show vpn-sessiondb detail command displays index numbers for each session.
ipaddress *IPaddr*	Clears statistics for sessions of the IP address that you specify.
l2l	Clears stastistics for VPN LAN-to-LAN sessions.

protocol protocol	Clears **statistics for the following protocols:** • ikev1—Sessions using the IKEv1 protocol. • ikev2—Sessions using theIKEv2 protocol. • ipsec—IPsec sessions using either IKEv1 or IKEv2. • ipseclan2lan—IPsec LAN-to-LAN sessions. • ipseclan2lanovernatt—IPsec LAN-to-LAN over NAT-T sessions. • ipsecovernatt—IPsec over NAT-T sessions. • ipsecovertcp—IPsec over TCP sessions. • ipsecoverudp—IPsec over UDP sessions. • l2tpOverIpSec—L2TP over IPsec sessions. • l2tpOverIpsecOverNatT—L2TP over IPsec over NAT-T sessions. • ospfv3—OSPFv3 over IPsec sessions. • webvpn—Clientless SSL VPN sessions. • imap4s—IMAP4 sessions. • pop3s—POP3 sessions. • smtps—SMTP sessions. • anyconnectParent—Secure Client sessions, regardless of the protocol used for the session (terminates AnyConnect IPsec IKEv2 and SSL sessions). • ssltunnel—SSL VPN sessions, including Secure Client sessions using SSL and clientless SSL VPN sessions. • dtlstunnel—Secure Client sessions with DTLS enabled.
ra-ikev1-ipsec	Clears statistics for IPsec IKEv1 and L2TP sessions.
ra-ikev2-ipsec	Clears statistics for IPsec IKEv2 sessions.
tunnel-group *groupname*	Clears statistics for sessions for the tunnel group (connection profile) that you specify.
vpn-lb	Clears statistics for VPN load balancing management sessions.
webvpn	Clears statistics for clientless SSL VPN sessions.

Usage Guidelines

Note Executing `clear vpn-sessiondb statistics all` resets all VPN session statistics, including the received and sent octet counters. Because RADIUS interim and stop accounting messages report these same octet counts, their values are reset as well when the command runs.

Command Default

There is no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.3(2)	The **ra-ikev2-ipsec** keyword was added.
9.8(1)	The email-proxy option was deprecated.
9.0(1)	The OSPFv3 session type and multiple context mode was added.

clear wccp

To reset WCCP information, use the **clear wccp** command in privileged EXEC mode.

clear wccp [**web-cache** | *service_number*]

Syntax Description

web-cache	Specifies the web-cache service.
service-number	A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the **web-cache** keyword.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to reset the WCCP information for the web-cache service:

```
ciscoasa# clear wccp web-cache
```

Related Commands

Command	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

clear webvpn sso-server statistics

To reset the statistics from the WebVPN Single Sign-On (SSO) server, use the **clear webvpn sso-server statistics** command in privileged EXEC mode.

clear webvpn sso-server statistics *servername*

Syntax Description

servername	Specifies the name of the SSO server to be reset.

Command Default

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command does not reset the "pending requests" statistic.

Examples

The following example displays crypto accelerator statistics:

```
ciscoasa # clear webvpn sso-server statistics
ciscoasa #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

clear xlate

To clear current dynamic translation and connection information, use the **clear xlate** command in privileged EXEC mode.

clear xlate [**global** *ip1* [- *ip2*] [**netmask** *mask*]] [**local** *ip1* [- *ip2*] [**netmask** *mask*]] [**gport** *port1* [- *port2*]] [**interface** *if_name*] [**state** *state*]

Syntax Description

global *ip1* [- *ip2*]	(Optional) Clears the active translations by global IP address or range of addresses.
gport *port1* [-*port2*]	(Optional) Clears the active translations by the global port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local *ip1* [- *ip2*]	(Optional) Clears the active translations by local IP address or range of addresses.
lport *port1* [-*port2*]	(Optional) Clears the active translations by local port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state *state*	(Optional) Clears the active translations by state. You can enter one or more of the following states: • **static** —Specifies **static** translations. • **portmap** —Specifies PAT global translations. • **norandomseq** —Specifies a **nat** or **static** translation with the **norondomseq** setting. • **identity** —Specifies **nat 0** identity address translations. When specifying more than one state, separate the states with a space.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **clear xlate** command clears the contents of the translation slots ("xlate" refers to the translation slot). Translation slots can persist after key changes have been made. Always use the clear xlate command after adding, changing, or removing the global or nat commands in your configuration.

An xlate describes a NAT or PAT session. These sessions can be viewed with the **show xlate** command with the **detail** option. There are two types of xlates: static and dynamic.

A static xlate is a persistent xlate that is created using the **static** command. The **clear xlate** command does not clear for a host in a static entry. Static xlates can only be removed by removing the **static** command from the configuration; the **clear xlate** command does not remove the static translation rule. If you remove a static command from the configuration, preexisting connections that use the static rule can still forward traffic. Use the **clear local-host** or **clear conn** command to deactivate these connections.

A dynamic xlate is an xlate that is created on demand with traffic processing (through the **nat** or **global** command). The **clear xlate** command removes dynamic xlates and their associated connections. You can also use the **clear local-host** or **clear conn** command to clear the xlate and associated connections. If you remove a **nat** or a **global** command from the configuration, the dynamic xlate and associated connections may remain active. Use the **clear xlate** command to remove these connections.

Examples

The following example shows how to clear the current translation and connection slot information:

```
ciscoasa# clear xlate global
```

Related Commands

Command	Description
clear local-host	Clears local host network information.
clear uauth	Clears cached user authentication and authorization information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.
show xlate	Displays the current translation information.



clf - crx

- client (ctl-provider), on page 773
- client (tls-proxy), on page 775
- client-access-rule, on page 778
- client-bypass-protocol, on page 780
- client-firewall, on page 782
- client-types (crypto ca trustpoint), on page 785
- client-update, on page 787
- clock set, on page 792
- clock summer-time, on page 794
- clock timezone, on page 796
- clu-keepalive-interval, on page 798
- cluster-ctl-file (Deprecated), on page 800
- cluster encryption, on page 801
- cluster exec, on page 803
- cluster flow-mobility lisp, on page 805
- cluster group, on page 807
- cluster-interface, on page 810
- cluster interface-mode, on page 812
- cluster ip address, on page 815
- cluster key, on page 817
- cluster control-node, on page 819
- cluster-member-limit, on page 821
- cluster-mode (Deprecated), on page 822
- cluster port, on page 824
- cluster redistribute vpn-sessiondb, on page 826
- cluster remove unit, on page 828
- cluster replication delay, on page 830
- cn-id, on page 831
- command-alias, on page 833
- command-queue, on page 835
- commercial-security, on page 837
- community-list, on page 839
- compatible rfc1583, on page 842

- compression, on page 843
- config-register, on page 845
- config-replicate-parallel, on page 851
- configure factory-default, on page 852
- configure http, on page 856
- configure memory, on page 858
- configure net, on page 860
- configure session, on page 863
- configure terminal, on page 865
- config-url, on page 866
- connect fxos, on page 869
- conn data-rate, on page 871
- conn-rebalance, on page 873
- consent-token generate-challenge, on page 875
- consent-token accept-response, on page 876
- console-replicate, on page 877
- console timeout, on page 879
- content-length, on page 881
- context, on page 883
- copy, on page 885
- cpu hog granular-detection, on page 891
- cpu profile activate, on page 893
- coredump enable, on page 895
- crashinfo console disable, on page 899
- crashinfo force kernel-dump, on page 901
- crashinfo force, on page 903
- crashinfo save disable, on page 905
- crashinfo test, on page 907
- crl (Deprecated), on page 909
- crl cache-time, on page 911
- crl configure, on page 912
- crl enforcenextupdate, on page 913

client (ctl-provider)

To specify clients allowed to connect to the Certificate Trust List provider, or to specify a username and password for client authentication, use the **client** command in ctl provider configuration mode. To remove the configuration, use the **no** form of this command.

client { [**interface** *if_name*] *ipv4_addr* | **username** *user_name* **password** *password* [**encrypted**] }
no client { [**interface** *if_name*] *ipv4_addr* | **username** *user_name* **password** *password* [**encrypted**] }

Syntax Description

encrypted	Specifies encryption for the password.
interface *if_name*	Specifies the interface allowed to connect.
ipv4_addr	Specifies the IP address of the client.
password *password*	Specifies the password for client authentication.
username *user_name*	Specifies the username for client authentication.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl provider configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **client** command in ctl provider configuration mode to specify the clients allowed to connect to the CTL provider, and to set the username and password for client authentication. More than one command may be issued to define multiple clients. The username and password must match the CCM Administrator's username and password for the CallManager cluster.

Examples

The following example shows how to create a CTL provider instance:

```
ciscoasa(config)# ctl-provider my_ctl

ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
```

```
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl	Parses the CTL file from the CTL client and installs trustpoints.
ctl-provider	Configures a CTL provider instance in ctl provider configuration mode.
export	Specifies the certificate to be exported to the client
service	Specifies the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

client (tls-proxy)

To configure trustpoints, keypairs, and cipher suites for a TLS proxy, use the **client** command in tls proxy configuration mode. To remove the configuration, use the **no** form of this command.

client { **cipher-suite** *cipher_list* | **ldc** { **issuer** *ca_tp_name* | **key-pair** *key_label* } | **trust-point** *proxy_trustpoint* | **clear-text** }

no client { **cipher-suite** *cipher_list* | **ldc** { **issuer** *ca_tp_name* | **key-pair** *key_label* } | **trust-point** *proxy_trustpoint* | **clear-text** }

Syntax Description

cipher-suite *cipher_list*	Specifies the cipher suite. To see the available options for your platform, enter ? for the cipher list.
clear-text	Specifies that communication between the ASA and the TLS server should be in clear text (not encrypted).
ldc issuer *ca_tp_name*	Specifies the local CA trustpoint to issue client local dynamic certificates.
ldc keypair *key_label*	Specifies the RSA keypair to be used by client local dynamic certificates.
trust-point *proxy_trustpoint*	Specifies a trustpoint that uses a static certificate as opposed to issuing local dynamic certificates.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tls proxy configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)	The **trust-point** keyword was added.
9.6(1)	The **clear-text** keyword was added.

Usage Guidelines

TLS proxy is used by some protocol inspection engines to decrypt encrypted traffic so that it can be inspected. After inspection, the proxy re-encrypts the traffic and sends it to the destination.

Use the **client** command in tls proxy configuration mode to control the TLS handshake parameters for the ASA when it acts in the TLS client role in TLS proxy.

You have the following options for the client trustpoint:

- Use the **client ldc** commands to identify a local dynamic certificate issuer. Use this option when you need unique certificates per client. For example, for Cisco IP phones in SIP/SCCP inspection. Use the **ldc issuer** command to identify the local CA that issues client dynamic certificates (defined by the **crypto ca trustpoint** command). The trustpoint must have the **proxy-ldc-issuer** command configured, or be the default local CA server (LOCAL-CA-SERVER).

Use the **ldc key-pair** command to identify the keypair generated with the **crypto key generate** command.

- Use the **client trust-point** command to identify a trustpoint that uses a static certificate. For example, for Cisco Unified Presence Server (CUPS) in SIP/SCCP inspection, The certificate must be owned by the ASA (identity certificate). The certificate can be self-signed, enrolled with a certificate authority, or from an imported credential.
- Use the **client clear-text** command to use unencrypted communication with the TLS server. You can use this option if the ASA and TLS server are in the same data center and you can be certain the communication is secure. This configuration is intended for Diameter inspection.

You can also set a different cipher suite for the TLS proxy using **client cipher-suite**. If you do not define the ciphers the TLS proxy can use, the proxy uses the cipher suite defined by the **ssl encryption** command. If that command is not defined, all available ciphers are used. Specify this command only if you want to use a different suite than the one generally available on the ASA. You can use this command to achieve different ciphers between the two TLS sessions. You should use AES ciphers with the CallManager server.

Examples

The following example shows how to create a TLS proxy using a local dynamic certificate issuer:

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client ldc issuer ldc_server
ciscoasa(config-tlsp)# client ldc keypair phone_common
```

The following example shows how to create a TLS proxy using a trustpoint with a static certificate.

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client trust-point ent_y_proxy
```

The following example shows how to create a TLS proxy for Diameter inspection that uses clear text communication between the ASA and Diameter server.

```
ciscoasa(config)# tls-proxy diameter-tls-offload-proxy

ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp

ciscoasa(config-tlsp)# client clear-text
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters ctl provider configuration mode.

Commands	Description
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum number of sessions.

client-access-rule

To configure rules that limit the remote access client types and versions that can connect via IPsec through the ASA, use the **client-access-rule** command in group-policy configuration mode. To delete a rule, use the **no** form of this command.

client-access-rule *priority* { **permit | deny** } **type** *type* **version** *version* | **none**

no client-access-rule *priority* [{ **permit | deny** } **type** *type* **version** *version*]

Syntax Description

deny	Denies connections for devices of a particular type and/or version.
none	Allows no client access rules. Sets **client-access-rule** to a null value, thereby allowing no restriction. Prevents inheriting a value from a default or specified group policy.
permit	Permits connections for devices of a particular type and/or version.
priority	Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the ASA ignores it.
type *type*	Identifies device types via free-form strings, for example VPN 3002. A string must match exactly its appearance in the **show vpn-sessiondb remote** command output, except that you can use the * character as a wildcard.
version *version*	Identifies the device version via free-form strings, for example 7.0. A string must match exactly its appearance in the **show vpn-sessiondb remote** command output, except that you can use the * character as a wildcard.

Command Default

By default, there are no access rules.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To delete all rules, use the **no client-access-rule** command with only the *priority* argument. This deletes all configured rules, including a null rule created by issuing the **client-access-rule none** command.

When there are no client access rules, users inherit any rules that exist in the default group policy. To prevent users from inheriting client access rules, use the **client-access-rule none** command. The result of doing so is that all client types and versions can connect.

Construct rules according to these caveats:

- If you do not define any rules, the ASA permits all connection types.
- When a client matches none of the rules, the ASA denies the connection. This means that if you define a deny rule, you must also define at least one permit rule, or the ASA denies all connections.
- For both software and hardware clients, type and version must match exactly their appearance in the **show vpn-sessiondb remote** command output.
- The * character is a wildcard, which you can use multiple times in each rule. For example, **client-access-rule 3 deny type * version 3.*** createsa priority 3 client access rule that denies all client types running release versions 3.x software.
- You can construct a maximum of 25 rules per group policy.
- There is a limit of 255 characters for an entire set of rules.
- You can use n/a for clients that do not send client type and/or version.

Examples

The following example shows how to create client access rules for the group policy named FirstGroup. These rules permit VPN Clients running software version 4.1, while denying all VPN 3002 hardware clients:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-access-rule 1 d t VPN3002 v *
ciscoasa(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-bypass-protocol

To configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic, use the **client-bypass-protocol** command in group-policy configuration mode. To clear the client bypass protocol setting, use the **no** form of this command.

client-bypass-protocol { **enable** | **disable** }

no client-bypass-protocol { **enable** | **disable** }

Syntax Description

enable	If Client Bypass Protocol is enabled, the IP traffic for which the ASA did not assign an IP address type is sent from the client in the clear through the client's normal, non-VPN gateway.
disable	If Client Bypass Protocol is disabled, the IPv6 traffic for which the ASA did not assign an IP address type is dropped.

Command Default

Client Bypass Protocol is disabled by default in the DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The Client Bypass Protocol feature allows you to configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

When the Secure Client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the Secure Client connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or “in the clear.”

For example, assume that the ASA assigns only an IPv4 address to an Secure Client connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

Examples

The following example enables client bypass protocol:

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

The following example disables client bypass protocol:

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

The following example clears the client bypass protocol setting:

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

client-firewall

To set personal firewall policies that the ASA pushes to the VPN client during IKE tunnel negotiation, use the **client-firewall** command in group-policy configuration mode. To delete a firewall policy, use the **no** form of this command.

client-firewall none
no client-firewall { **opt req** } **custom vendor-id** *num* **product-id** *num* **policy** { **AYT** | **CPP acl-in** *acl* **acl-out** *acl*] [**description** *string*]
client-firewall { **opt** | **req** } **zonelabs-integrity**

Note When the firewall type is **zonelabs-integrity** , do not include arguments. The Zone Labs Integrity Server determines the policies.

client-firewall { **opt** | **req** } **zonelabs-zonealarm policy** { **AYT** | **CPP acl-in** *acl* **acl-out** *acl* }
client-firewall { **opt** | **req** } **zonelabs-zonealarmorpro policy** { **AYT** | **CPP acl-in** *acl* **acl-out** *acl* }
client-firewall { **opt** | **req** } **zonelabs-zonealarmpro policy** { **AYT** | **CPP acl-in** *acl* **acl-out** *acl* }
client-firewall { **opt** | **req** } **cisco-integrated acl-in** *acl* **acl-out** *acl* }
client-firewall { **opt** | **req** } **sygate-personal**
client-firewall { **opt** | **req** } **sygate-personal-pro**
client-firewall { **opt** | **req** } **sygate-personal-agent**
client-firewall { **opt** | **req** } **networkice-blackice**
client-firewall { **opt** | **req** } **cisco-security-agent**

Syntax Description

acl-in *acl*	Provides the policy the client uses for inbound traffic.
acl-out *acl*	Provides the policy the client uses for outbound traffic.
AYT	Specifies that the client PC firewall application controls the firewall policy. The ASA checks to make sure the firewall is running. It asks, “Are You There?” If there is no response, the ASA tears down the tunnel.
cisco-integrated	Specifies the Cisco Integrated firewall type.
cisco-security-agent	Specifies the Cisco Intrusion Prevention Security Agent firewall type.
CPP	Specifies Policy Pushed as source of the VPN Client firewall policy.
custom	Specifies the Custom firewall type.
description *string*	Describes the firewall.
networkice-blackice	Specifies the Network ICE Black ICE firewall type.
none	Indicates that there is no client firewall policy. Sets a firewall policy with a null value, thereby disallowing one. Prevents inheriting a firewall policy from a default or specified group policy.

opt	Indicates an optional firewall type.
product-id	Identifies the firewall product.
req	Indicates a required firewall type.
sygate-personal	Specifies the Sygate Personal firewall type.
sygate-personal-pro	Specifies the Sygate Personal Pro firewall type.
sygate-security-agent	Specifies the Sygate Security Agent firewall type.
vendor-id	Identifies the firewall vendor.
zonelabs-integrity	Specifies the Zone Labs Integrity Server firewall type.
zonelabs-zonealarm	Specifies the Zone Labs Zone Alarm firewall type.
zonelabs-zonealarmorpro policy	Specifies the Zone Labs Zone Alarm or Pro firewall type.
zonelabs-zonealarmpro policy	Specifies the Zone Labs Zone Alarm Pro firewall type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The **zonelabs-integrity** firewall type was added.

Usage Guidelines

Only one instance of this command can be configured.

To delete all firewall policies, use the **no client-firewall** command without arguments. This command deletes all configured firewall policies, including a null policy created by issuing the **client-firewall none** command.

When there are no firewall policies, users inherit any that exist in the default or other group policy. To prevent users from inheriting such firewall policies, use the **client-firewall none** command.

Examples

The following example shows how to set a client firewall policy that requires Cisco Intrusion Prevention Security Agent for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-firewall
             req cisco-security-agent
```

client-types (crypto ca trustpoint)

To specify the client connection types for which this trustpoint can be used to validate the certificates associated with a user connection, use the **client-types** command in crypto ca trustpoint configuration mode.

[**no**] **client-types** { **ssl** | **ipsec** }

Syntax Description

ipsec	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate IPsec connections.
ssl	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate SSL connections.

Command Default

No default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

When there are multiple trustpoints associated with the same CA certificate, only one of the trustpoints can be configured for a specific client type. However one of the trustpoints can be configured for one client type and the other trustpoint with another client-type.

If there is a trustpoint associated with the same CA certificate that is already configured with a client type, the new trustpoint is not allowed to be configured with the same client-type setting. The no form of the command clears the setting so that trustpoint cannot be used for any client validation.

Remote-access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPsec), or both, depending on deployment requirements, to permit access to virtually any network application or resource.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint, central, and designates it an SSL trustpoint:

```
hostname(config)# crypto ca trustpoint central
```

```
hostname(config-ca-trustpoint)# client-types ssl
hostname(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for trustpoint, checkin 1, and designated it as an IPsec trustpoint.

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# client-types ipsec
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
id-usage	Specifies how the enrolled identity of a trustpoint can be used.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

client-update

To issue a client-update for all active remote VPN software and hardware clients and ASAs configured as Auto Update clients, on all tunnel-groups or for a particular tunnel group, use the **client-update** command in privileged EXEC mode.

To configure and change client-update parameters at the global level, including VPN software and hardware clients and ASAs configured as Auto Update clients, use the **client-update** command in global configuration mode.

To configure and change client-update tunnel-group IPsec-attributes parameters for VPN software and hardware clients, use the **client-update** command in tunnel-group ipsec-attributes configuration mode.

To disable a client update, use the **no** form of this command.

Global configuration mode command:

client-update { **enable** | **component** { **asdm** | **image** } | **device_id** *dev_string* | **family** *family_name* | **type** *type* } **url** *url-string* **rev-nums** *rev-nums* }
no client-update { **enable** | **component** { **asdm** | **image** } | **device_id** *dev_string* | **family** *family_name* | **type** *type* } **url** *url-string* **rev-nums** *rev-nums* }

Tunnel-group ipsec-attributes configuration mode command:

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*
no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

Privileged EXEC mode command:

client-update { **all** | *tunnel-group* }
no client-update *tunnel-group*

Syntax Description

all	(Available only in privileged EXEC mode.) Applies the action to all active remote clients in all tunnel groups. You cannot use the keyword **all** with the **no** form of the command.
component {**asdm** | **image**}	The software component for ASAs configured as Auto Update clients.
device-id *dev_string*	If the Auto Update client is configured to identify itself with a unique string, specify the same string that the client uses. The maximum length is 63 characters.
enable	(Available only in global configuration mode). Enables remote client software updates.
family *family_name*	If the Auto Update client is configured to identify itself by device family, specify the same device family that the client uses. It can be asa, pix, or a text string with a maximum length of 7 characters.
rev-nums *rev-nums*	(Not available in privileged EXEC mode.) Specifies the software or firmware images for this client. For Windows, WIN9X, WinNT, and VPN3002 clients, enter up to 4, in any order, separated by commas. For ASAs, only one is allowed. The maximum length of the string is 127 characters.

tunnel-group	(Available only in privileged EXEC mode.) Specifies the name of a valid tunnel-group for remote client update.
type *type*	(Not available in privileged EXEC mode.) Specifies the operating systems of remote PCs or the type of ASAs (configured as Auto Update clients) to notify of a client update. The list is the following: • asa5505: Cisco 5505 Adaptive Security Appliance • asa5510: Cisco 5510 Adaptive Security Appliance • asa5520: Cisco 5520 Adaptive Security Appliance • asa5540: Cisco 5540 Adaptive Security Appliance • linux: A Linux client • mac: MAC OS X client • pix-515: Cisco PIX 515 Firewall • pix-515e: Cisco PIX 515E Firewall • pix-525: Cisco PIX 525 Firewall • pix-535: Cisco PIX 535 Firewall • Windows: all windows-based platforms • WIN9X: Windows 95, Windows 98, and Windows ME platforms • WinNT: Windows NT 4.0, Windows 2000, and Windows XP platforms • vpn3002: VPN 3002 hardware client • A text string of up to 15 characters
url *url-string*	(Not available in privileged EXEC mode.) Specifies the URL for the software/firmware image. This URL must point to a file appropriate for this client. The maximum string length is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The tunnel-group ipsec-attributes configuration mode was added.
7.2(1)	The **component**, **device-id**, and **family** keywords and their arguments were added to support the ASA configured as an Auto Update Server.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

In tunnel-group ipsec-attributes configuration mode, you can apply this attribute only to the IPsec remote-access tunnel-group type.

The **client-update** command lets you enable the update; specify the types and revision numbers of clients to which the update applies; provide a URL or IP address from which to get the update; and, in the case of Windows clients, optionally notify users that they should update their VPN client version. If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update.

For Windows clients, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. When the client type is another ASA, this ASA acts as an Auto Update server.



Note For all Windows clients and Auto Update clients, you must use the protocol “http://” or “https://” as the prefix for the URL. For the VPN 3002 hardware client, you must specify protocol “tftp://” instead.

Alternatively, for Windows clients and VPN 3002 hardware clients, you can configure client update just for individual tunnel-groups, rather than for all clients of a particular type.



Note You can have the browser automatically start an application by including the application name at the end of the URL; for example: https://support/updates/vpnclient.exe.

After you have enabled client update, you can define a set of client-update parameters for a particular IPsec-remote access tunnel group. To do this, in tunnel-group ipsec-attributes mode, specify the tunnel-group name and its type, and the URL or IP address from which to get the updated image. In addition, you must specify a revision number. If the user client revision number matches one of the specified revision numbers, there is no need to update the client; for example, to issue a client update for all Windows clients.

Optionally, you can send a notice to active users with outdated Windows clients that their VPN client needs updating. For these users, a dialog box appears, offering the opportunity to launch a browser and download the updated software from the site specified in the URL. The only part of this message that you can configure is the URL. Users who are not active get a notification message the next time they log in. You can send this notice to all active clients on all tunnel groups, or you can send it to clients on a particular tunnel group.

If the user client revision number matches one of the specified revision numbers, there is no need to update the client, and users receive no notification message. VPN 3002 clients update without user intervention, and users receive no notification message.



Note If you specify the client-update type as **windows** (specifying all Windows-based platforms) and later want to enter a client-update type of **win9x** or **winnt** for the same entity, you must first remove the windows client type with the **no** form of the command, then use new **client-update** commands to specify the new client types.

Examples

The following example, entered in global configuration mode, enables client update for all active remote clients on all tunnel groups:

```
ciscoasa(config)# client-update enable
ciscoasa#
```

The following example applies only to Windows (Win9x, WinNT). Entered in global configuration mode, it configures client update parameters for all Windows-based clients, including the revision number, 4.7 and the URL for retrieving the update, https://support/updates.

```
ciscoasa(config)# client-update type windows url https://support/updates/ rev-nums 4.7
ciscoasa(config)#
```

The following example applies only to VPN 3002 hardware clients. Entered in tunnel-group ipsec-attributes configuration mode, it configures client update parameters for the IPsec remote-access tunnel-group “salesgrp”. It designates the revision number, 4.7 and uses the TFTP protocol for retrieving the updated software from the site with the IP address 192.168.1.1:

```
ciscoasa(config)# tunnel-group salesgrp type ipsec-ra
ciscoasa(config)# tunnel-group salesgrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# client-update type vpn3002
url tftp:192.168.1.1 rev-nums 4.7
ciscoasa(config-tunnel-ipsec)#
```

The following example shows how to issue a client update for clients that are Cisco 5520 ASAs configured as Auto Update clients:

```
ciscoasa(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

The following example, entered in privileged EXEC mode, sends a client-update notification to all connected remote clients in the tunnel group named “remotegrp” that need to update their client software. Clients in other groups do not get an update notification.

```
ciscoasa# client-update remotegrp
ciscoasa#
The following example, entered in privileged EXEC mode, notifies all active clients on all
 tunnel groups:
```

```
ciscoasa# client-update all
ciscoasa#
```

Related Commands

Command	Description
clear configure client-update	Clears the entire client-update configuration.
show running-config client-update	Shows the current client-update configuration.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

clock set

To manually set the clock on the ASA, use the **clock set** command in privileged EXEC mode.

clock set *hh :mm: ss* { *month day* | *day month* } *year*

Syntax Description

day	Sets the day of the month, from 1 to 31. You can enter the day and month as **april 1** or as **1 april**, for example, depending on your standard date format.
hh:*mm*:*ss*	Sets the hour, minutes, and seconds in 24-hour time. For example, set **20:54:00** for 8:54 pm.
month	Sets the month. Depending on your standard date format, you can enter the day and month as **april 1** or as **1 april**.
year	Sets the year using four digits, for example, **2004**. The year range is 1993 to 2035.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you have not entered any **clock** configuration commands, the default time zone for the **clock set** command is UTC. If you change the time zone after you enter the **clock set** command using the **clock timezone** command, the time automatically adjusts to the new time zone. However, if you enter the **clock set** command after you establish the time zone with the **clock timezone** command, then enter the time appropriate for the new time zone and not for UTC. Similarly, if you enter the clock summer-time command after the **clock set** command, the time adjusts for daylight saving. If you enter the **clock set** command after the **clock summer-time** command, enter the correct time for daylight saving.

This command sets the time in the hardware chip, and does not save the time in the configuration file. This time endures reboots. Unlike the other **clock** commands, this command is a privileged EXEC command. To reset the clock, you need to set a new time for the **clock set** command.

Examples

The following example sets the time zone to MST, the daylight saving time to the default period in the U.S., and the current time for MDT to 1:15 p.m. on July 27, 2004:

```
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa(config)# exit
ciscoasa# clock set 13:15:0 jul 27 2004
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

The following example sets the clock to 8:15 on July 27, 2004 in the UTC time zone, and then sets the time zone to MST and the daylight saving time to the default period in the U.S. The end time (1:15 in MDT) is the same as the previous example.

```
ciscoasa# clock set 20:15:0 jul 27 2004
ciscoasa# configure terminal
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

Related Commands

Command	Description
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
show clock	Shows the current time.

clock summer-time

To set the date range for daylight saving time for the display of the ASA time, use the **clock summer-time** command in global configuration mode. To disable the daylight saving time dates, use the **no** form of this command.

clock summer-time *zone* **recurring** [*week weekday month hh: mm week weekday month hh: mm*] [*offset*]
no clock summer-time [*zone* **recurring** [*week weekday month hh: mm week weekday month hh: mm*] [*offset*]
clock summer-time *zone* **date** { *day month* | *month day* } *year hh: mm* { *day month* | *month day* } *year hh: mm* [*offset*]
no clock summer-time [*zone* **date** { *day month* | *month day* } *year hh: mm* { *day month* | *month day* } *year hh: mm* [*offset*]]

Note This command is not supported on the Firepower 1000 or Firepower 2100 in Appliance mode.

Syntax Description

date	Specifies the start and end dates for daylight saving time as a specific date in a specific year. If you use this keyword, you need to reset the dates each year.
day	Sets the day of the month, from 1 to 31. You can enter the day and month as **April 1** or as **1 April**, for example, depending on your standard date format.
hh:mm	Sets the hour and minutes in 24-hour time.
month	Sets the month as a string. For the **date** command, you can enter the day and month as **April 1** or as **1 April**, for example, depending on your standard date format.
offset	(Optional) Sets the number of minutes to change the time for daylight saving time. By default, the value is 60 minutes.
recurring	Specifies the start and end dates for daylight saving time, in the form of a day and time of the month, and not a specific date in a year. This keyword lets you set a recurring date range that you do not need to alter yearly. If you do not specify any dates, the ASA uses the default date range for the United States: from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.
week	(Optional) Specifies the week of the month as an integer between 1 and 4 or as the words **first** or **last**. For example, if the day might fall in the partial fifth week, then specify **last**.
weekday	(Optional) Specifies the day of the week: **Monday**, **Tuesday**, **Wednesday**, and so on.
year	Sets the year using four digits, for example, **2004**. The year range is 1993 to 2035.
zone	Specifies the time zone as a string, for example, **PDT** for Pacific Daylight Time. When the ASA shows the daylight saving time according to the date range you set with this command, the time zone changes to the value you set here. See the **clock timezone** command to set the base time zone to a zone other than UTC.

Command Default

The default offset is 60 minutes.

The default recurring date range is from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.0(2)	The default recurring date range was changed to 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

Usage Guidelines

For the Southern Hemisphere, the ASA accepts the start month to be later in the year than the end month, for example, from October to March.

Examples

The following example sets the daylight saving date range for Australia:

```
ciscoasa(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday March
 2:00
```

Some countries start daylight saving on a specific date. In the following example, daylight saving time is configured to start on April 1, 2008, at 3 a.m. and end on October 1, 2008, at 4 a.m.

```
ciscoasa(config)# clock summer-time UTC date 1 April 2008 3:00 1 October 2008 4:00
```

Related Commands

Command	Description
clock set	Manually sets the clock on the ASA.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show clock	Shows the current time.

clock timezone

To set the time zone for the ASA clock, use the **clock timezone** command in global configuration mode. To set the time zone back to the default of UTC, use the **no** form of this command.

For Firepower 1000 and 2100 in Appliance mode:

clock timezone *zone*
no clock timezone [*zone*]

For all other models:

clock timezone *zone* [**-**] *hours* [*minutes*]
no clock timezone [*zone* [**-**] *hours* [*minutes*]]

Syntax Description

[-]*hours*	Sets the number of hours of offset from UTC. For example, PST is -8 hours.
minutes	(Optional) Sets the number of minutes of offset from UTC.
zone	Specifies the time zone as a string, for example, PST for Pacific Standard Time. For the Firepower 1000 and 2100 in Appliance mode, Enter the **clock timezone ?** command to see a list of acceptable time zone names.

Command Default

The default time zone is UTC.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	This command was updated for the Firepower 1000 and 2100 in Appliance mode.

Usage Guidelines

To set daylight saving time, see the **clock summer-time** command (not supported for the Firepower 1000 or 2100).

The **clock set** command or the time derived from an NTP server sets the time in UTC. You must set the time zone as an offset of UTC using this command.

Examples

For the Firepower 1000 and 2100 in Appliance mode, the following example sets the time zone to Mountain Standard Time:

```
ciscoasa(config)# clock timezone ?
Available timezones:
CET
CST6CDT
Cuba
EET
Egypt
Eire
EST
EST5EDT
Factory
GB
GB-Eire
GMT
GMT0
GMT-0
GMT+0
Greenwich
Hongkong
HST
Iceland
Iran
Israel
Jamaica
Japan
[...]
ciscoasa(config)# clock timezone US/?

configure mode commands/options:
  US/Alaska          US/Aleutian    US/Arizona    US/Central
  US/East-Indiana    US/Eastern     US/Hawaii     US/Indiana-Starke
  US/Michigan        US/Mountain    US/Pacific
ciscoasa(config)# clock timezone US/Mountain
```

The following example sets the time zone to Pacific Standard Time, which is -8 hours from UTC:

```
ciscoasa(config)# clock timezone PST -8
```

Related Commands

Command	Description
clock set	Manually sets the clock on the ASA.
clock summer-time	Sets the date range to show daylight saving time.
ntp server	Identifies an NTP server.
show clock	Shows the current time.

clu-keepalive-interval

To set the keepalive interval for flow state refresh messages (clu_keepalive and clu_update messages) from the flow owner to the director and backup owner, use the **clu-keepalive-interval** command in cluster group configuration mode. To use the default setting, use the **no** form of this command.

clu-keepalive-interval *seconds*
no clu-keepalive-interval

Syntax Description

seconds	15 to 55. The default is 15.

Command Default

The default is 15 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.20(1)	This command was added.

Usage Guidelines

The flow owner sends keepalives (clu_keepalive messages) and updates (clu_update messages) to the director and backup owner to refresh the flow state. You can now set the keepalive interval. The default is 15 seconds, and you can set the interval between 15 and 55 seconds. You may want to set the interval to be longer to reduce the amount of traffic on the cluster control link.

This command is not part of the bootstrap configuration, and is replicated from the control node to the data nodes.

Examples

The following example sets the keepalive interval to 30 seconds:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# clu-keepalive-interval 30
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.

Command	Description
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

cluster-ctl-file (Deprecated)

To use trustpoints that are already created from an existing CTL file stored in flash memory, use the **cluster-ctl-file** command in ctl file configuration mode. To remove the CTL file configuration so that you can create a new CTL file, use the **no** form of this command.

cluster-ctl-file*filename_path*
no cluster-ctl-file *filename_path*

Syntax Description

filename_path	Specifies the path and filename of the CTL file stored on disk or stored in flash memory.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl-file configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

When this command is configured, the Phone Proxy parses the CTL file stored in flash memory and installs the trustpoints from that CTL file, then uses that file from flash in the creation of the new CTL file.

Examples

The following example parses the CTL file stored in flash memory to install the trustpoints from that file:

```
ciscoasa(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

cluster encryption

To enable encryption for messages exchanged on the virtual load-balancing cluster, use the **cluster encryption** command in vpn load-balancing configuration mode. To disable encryption, use the **no** form of this command.

clusterencryption
noclusterencryption

Note VPN load balancing requires an active 3DES/AES license. The ASA checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the ASA prevents the enabling of load balancing and prevents internal configuration of 3DES by the load balancing system, unless the license permits this usage.

Syntax Description

This command has no arguments or keywords.

Command Default

Encryption is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Vpn load-balancing configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command turns encryption on or off for messages exchanged on the virtual load-balancing cluster.

Before configuring the **cluster encryption** command, you must have first used the **vpn load-balancing** command to enter vpn load-balancing configuration mode. You must also use the **cluster key** command to configure the cluster shared secret key before enabling cluster encryption.

Note When using encryption, you must first configure the command **isakmp enable** *inside*, where *inside* designates the load-balancing inside interface. If ISAKMP is not enabled on the load-balancing inside interface, an error message appears when you try to configure cluster encryption.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **cluster encryption** command to enable encryption for the virtual load-balancing cluster:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
cluster key	Specifies the shared-secret key for the cluster.
vpn load-balancing	Enters vpn load-balancing configuration mode.

cluster exec

To execute a command on all units in the cluster, or on a specific member, use the **cluster exec** command in privileged EXEC mode.

cluster exec [**unit** *unit_name*] *command*

Syntax Description

unit *unit_name*	(Optional) Performs the command on a specific unit. To view member names, enter **cluster exec unit ?** (to see all names except the current unit), or enter the **show cluster info** command.
command	Specifies the command you want to execute.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Sending a **show** command to all members collects all output and displays it on the console of the current unit. Other commands, such as **capture** and **copy**, can also take advantage of cluster-wide execution.

Examples

To copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the following command on the master unit:

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as capture1_asa1.pcap, capture1_asa2.pcap, and so on. In this example, asa1 and asa2 are cluster unit names.

The following sample output for the **cluster exec show port-channel** summary command shows EtherChannel information for each member in the cluster:

```
ciscoasa# cluster exec show port-channel summary
primary(LOCAL):*********************************************************
 Number of channel-groups in use: 2
```

```
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-------------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 secondary:*****************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-------------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

Related Commands

Command	Description
cluster group	Enters cluster group configuration mode.
show cluster info	Shows cluster information.

cluster flow-mobility lisp

To enable flow mobility for a traffic class, use the **cluster flow-mobility lisp** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map** command. To disable flow mobility, use the **no** form of this command.

cluster flow-mobility lisp
no cluster flow-mobility lisp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.

3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.
4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following example enables flow mobility for all inside traffic going to a server on 10.10.10.0/24 using HTTPS:

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

cluster group

To configure the cluster bootstrap parameters and other cluster settings, use the **cluster group** command in global configuration mode. To clear the cluster configuration, use the **no** form of this command.

cluster group *name*
no cluster group *name*

Syntax Description

name Specifies the cluster name as an ASCII string from 1 to 38 characters. You can only configure one cluster group per unit. All members of the cluster must use the same name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Each unit in the cluster requires a bootstrap configuration to join the cluster. Typically, the first unit you configure to join the cluster will be the master unit. After you enable clustering, after an election period, the cluster elects a master unit. With only one unit in the cluster initially, that unit will become the master unit. Subsequent units that you add to the cluster will be slave units.

Before you configure clustering, you need to set the cluster interface mode using the **cluster interface-mode** command.

You must use the console port or ASDM to enable or disable clustering. You cannot use Telnet or SSH.

Examples

The following example configures a management interface, configures a device-local EtherChannel for the cluster control link, disables the health check (temporarily), and then enables clustering for the ASA called “unit1,” which will become the master unit because it is added to the cluster first:

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
interface management 0/0
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
```

```
management-only
no shutdown
interface tengigabitethernet 0/6
channel-group 1 mode active
no shutdown
interface tengigabitethernet 0/7
channel-group 1 mode active
no shutdown
cluster group pod1
local-unit unit1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
no health-check
enable noconfirm
```

The following example includes the configuration for a slave unit, unit2:

```
interface tengigabitethernet 0/6
channel-group 1 mode active
no shutdown
interface tengigabitethernet 0/7
channel-group 1 mode active
no shutdown
cluster group pod1
local-unit unit2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
no health-check
enable as-slave
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
health-check auto-rejoin	Customizes the auto-rejoin cluster settings after a health check failure.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.

Command	Description
priority (cluster group)	Sets the priority of this unit for master unit elections.
site-id	Sets the site ID to avoid MAC address flapping in inter-site clustering.

cluster-interface

To specify the cluster control link physical interface and IP address, use the **cluster-interface** command in cluster group configuration mode. To remove the cluster interface, use the **no** form of this command.

cluster-interface*interface_id***ip***ip_addressmask*
no cluster-interface [*interface_id* **ip** *ip_address mask*]

Syntax Description

interface_id	For hardware platforms: Specifies a physical interface, an EtherChannel, or a redundant interface. Subinterfaces and Management interfaces are not allowed. For the ASA Virtual: Specify a VNI interface. This interface cannot have a **nameif** configured. For the ASA 5585-X with an IPS module, you cannot use the IPS module interfaces for the cluster control link.
ip *ip_address mask*	Specify an IPv4 address for the IP address; IPv6 is not supported for this interface. For each unit, specify a different IP address on the same network.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.17(1)	We added support for VNI interfaces for the ASA Virtual.

Usage Guidelines

You need to enable the cluster control link interface before you join the cluster.

For the ASA Virtual: Each unit must dedicate one interface as a VXLAN (VTEP) interface for the cluster control link.

For hardware platforms: We recommend that you combine multiple cluster control link interfaces into an EtherChannel if you have enough interfaces. The EtherChannel is local to the ASA, and is not a spanned EtherChannel. We recommend that you use a Ten Gigabit Ethernet interface for the cluster control link. We recommend using the On mode for EtherChannel member interfaces to reduce unnecessary traffic on the cluster control link. The cluster control link does not need the overhead of LACP traffic because it is an isolated, stable network.

The cluster control link interface configuration is not replicated from the control node to data nodes; however, you must use the same configuration on each node. Because this configuration is not replicated, you must configure the cluster control link interfaces separately on each node.

See the configuration guide for more information about the cluster control link.

Examples

The following example creates an EtherChannel, Port-channel 2, for TenGigabitEthernet 0/6 and TenGigabitEthernet 0/7, and then assigns the port channel as the cluster control link. The port-channel interface is created automatically when you assign an interface to the channel group.

```
interface tengigabitethernet 0/6
channel-group 2 mode on
no shutdown
interface tengigabitethernet 0/7
channel-group 2 mode on
no shutdown
cluster group cluster1
cluster-interface port-channel2 ip 10.1.1.1 255.255.255.0
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

cluster interface-mode

To specify the cluster interface mode on each cluster unit, use the **cluster interface-mode** command in global configuration mode.To disable cluster interface mode, enter the **no** form of this command.

cluster interface-mode { **individual** | **spanned** } [**check-details** | **force**]
no cluster-interface [*interface_id* **ip** *ip_address mask*]

Syntax Description

individual	Sets the mode to Individual interface mode (routed mode; ASA hardware models only).
spanned	Sets the mode to Spanned EtherChannel mode.
check-details	Shows any incompatible configuration so that you can force the interface mode and fix your configuration later; the mode is not changed with this command.
force	Changes the mode without checking your configuration for incompatible settings. You need to manually fix any configuration issues after you change the mode. Because any interface configuration can only be fixed after you set the mode, we recommend using the **force** option so that you can at least start from the existing configuration. You can re-run the **check-details** option after you set the mode for more guidance. Without the **force** option, if there is any incompatible configuration, you are prompted to clear your configuration and reload, thus requiring you to connect to the console port to reconfigure your management access. If your configuration is compatible (rare), the mode is changed and the configuration is preserved. If you do not want to clear your configuration, you can exit the command by typing **n**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You can only configure one type of interface for clustering: Spanned EtherChannels or Individual interfaces; you cannot mix interface types in a cluster. If you have not set the mode, you cannot enable clustering. After you set the mode, even if you have not enabled clustering, your interfaces must comply with clustering interface requirements.

See the following guidelines:

- You must set the mode separately on each ASA that you want to add to the cluster.
- You can always configure the management-only interface as an Individual interface (recommended), even in Spanned EtherChannel mode. The management interface can be an Individual interface even in transparent firewall mode.
- In Spanned EtherChannel mode, if you configure the management interface as an Individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.
- In multiple context mode, you must choose one interface type for all contexts. For example, if you have a mix of transparent and routed mode contexts, you must use Spanned EtherChannel mode for all contexts because that is the only interface type allowed for transparent mode.

Examples

The following example checks the current interface compatibility for Spanned EtherChannel mode:

```
ciscoasa(config)# cluster interface-mode spanned check-details
ERROR: Please modify the following configuration elements that are incompatible with 'spanned'
 interface-mode.
 - Interface vni1 is not a span-cluster port-channel interface, vni1(vni1) cannot be used
as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/0 is not a span-cluster port-channel interface, Gi0/0(inside) cannot be
used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/1 is not a span-cluster port-channel interface, Gi0/1(test) cannot be used
 as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/1 is not a span-cluster port-channel interface, Gi0/1.1(vlan100) cannot
be used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/2 is not a span-cluster port-channel interface, Gi0/2(outside) cannot be
used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/5 is not a span-cluster port-channel interface, Gi0/5(bgmember1) cannot
be used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/5 is not a span-cluster port-channel interface, Gi0/5.2(vlan200) cannot
be used as data interface when cluster interface-mode is 'spanned'.
 - Interface BV1 is not a span-cluster port-channel interface, BV1(bvi1) cannot be used as
 data interface when cluster interface-mode is 'spanned'.
ciscoasa(config)#
```

The following example sets the mode to Spanned EtherChannel mode and does not clear the incompatible configuration:

```
ciscoasa(config)# cluster interface-mode spanned force
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.

Command	Description
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

cluster ip address

To set the IP address of the virtual load-balancing cluster, use the **cluster ip address** command in vpn load-balancing configuration mode. To remove the IP address specification, use the **no** form of this command.

cluster ip address *ip-address*
no cluster ip address [*ip-address*]

Syntax Description

ip-address	The IP address that you want to assign to the virtual load-balancing cluster.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Vpn load-balancing configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode and configure the interface to which the virtual cluster IP address refers.

The cluster IP address must be on the same subnet as the interface for which you are configuring the virtual cluster.

In the **no** form of the command, if you specify the optional *ip-address* value, it must match the existing cluster IP address before the **no cluster ip address** command can be completed.

Examples

The following example shows a VPN load-balancing command sequence that includes a **cluster ip address** command that sets the IP address of the virtual load-balancing cluster to 209.165.202.224:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
```

```
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
interface	Sets the interfaces of the device.
nameif	Assigns a name to an interface.
vpn load-balancing	Enters vpn load-balancing configuration mode.

cluster key

To set the shared secret for IPsec site-to-site tunnel exchanges on the virtual load-balancing cluster, use the **cluster key** command in vpn load-balancing configuration mode. To remove this specification, use the **no** form of this command.

cluster key [**0** | **8**] *shared-secret*
no cluster key [**0** | **8**] [*shared-secret*]

Syntax Description

[**0** | **8**]	Specify **0** if the password is unencrypted, or **8** if the password is already encrypted (for example, you copied it from another unit's configuration).
shared-secret	A 3- through 17-character string that defines the shared secret for the VPN load-balancing cluster. Special characters can appear in the string, but not spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Vpn load-balancing configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	We added support for encrypted passwords with the **0** and **8** keywords.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode. The shared secret defined in the **cluster key** command is also used for cluster encryption.

You must use the **cluster key** command to configure the shared secret before enabling cluster encryption.

If you specify a value for *shared-secret* in the **no cluster key** form of the command, the shared secret value must match the existing configuration.

Examples

The following example shows a VPN load-balancing command sequence that includes a **cluster key** command to set the shared secret of the virtual load-balancing cluster to 123456789:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
```

```
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enters vpn load-balancing configuration mode.

cluster control-node

To make the current node the control node of a cluster, or to set another node as the control node, use the **cluster control-node** command in privileged EXEC mode.

cluster control-node [**unit** *unit_name*]

Caution The best method to change the control node is to disable clustering on the control node (see the **no enable (cluster group)** command), waiting for a new control node election, and then re-enabling clustering. If you must specify the exact unit you want to become the control node, use the **cluster control-node unit** command. Note, however, that for centralized features, if you force a control node change using this command, then all connections are dropped, and you have to re-establish the connections on the new control node.

Syntax Description

unit *unit_name*	(Optional) Specifies the local unit name to be the new control node. To view node names, enter **cluster control-node unit ?** (to see all names except the current unit), or enter the **show cluster info** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.19(1)	This command was changed from **cluster master** to **cluster control-node**.

Usage Guidelines

You will need to reconnect to the main cluster IP address.

Examples

The following example sets asa2 as the control node:

```
ciscoasa# cluster control-node unit asa2
```

Related Commands

Command	Description
cluster exec	Sends a command to all cluster members.
cluster group	Configures a cluster.
cluster remove unit	Removes the unit from the cluster.

cluster-member-limit

To configure the maximum number of cluster members, use the **cluster-member-limit** command in cluster group configuration mode. To restore the default, use the **no** form of this command.

cluster-member-limit *number*

no cluster-member-limit

Syntax Description

number	Sets the maximum number of cluster members between 2 and 16. The default is 16

Command Default

The default is 16 members.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.16(1)	This command was added.

Usage Guidelines

If you know that your cluster will be fewer than the maximum of 16 units, then we recommend that you set the actual planned number of units. Setting the maximum units lets the cluster manage resources better. For example, if you use port address translation (PAT), then the control unit can allocate port blocks to the planned number of members, and it will not have to reserve ports for extra units you don't plan to use.

If you change the cluster limit, and you are using port address translation (PAT) rules, ensure that you clear xlates or reboot the devices so that PAT pools can be appropriately reallocated to the cluster units.

Examples

The following example sets the maximum cluster members to 6:

```
ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# cluster-member-limit 6
```

Related Commands

Command	Description
cluster group	Configures the cluster group settings.

cluster-mode (Deprecated)

To specify the security mode of the cluster, use the **cluster-mode** command in phone-proxy configuration mode. To set the security mode of the cluster to the default mode, use the **no** form of this command.

cluster-mode [**mixed** | **nonsecure**]
no cluster-mode [**mixed** | **nonsecure**]

Syntax Description

mixed	Specifies the cluster mode to be in mixed mode when configuring the Phone Proxy feature.
nonsecure	Specifies the cluster mode to be in nonsecure mode when configuring the Phone Proxy feature.

Command Default

The default cluster mode is nonsecure.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

When you are configuring the Phone Proxy to run in mixed-mode clusters (both secure and nonsecure modes), you must also configure the LDC issuer in case some phones are configured to be in authenticated or encrypted mode:

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Examples

The following example sets the security mode of the Phone Proxy to mixed (the IP phones will operate in secure and nonsecure modes):

```
ciscoasa
(config-phone-proxy)# cluster-mode mixed
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
tls-proxy	Configures the TLS Proxy instance.

cluster port

To set the UDP port for the virtual load-balancing cluster, use the **cluster port** command in vpn load-balancing configuration mode. To remove the port specification, use the **no** form of this command.

cluster port *port*
no cluster port [*port*]

Syntax Description

port	The UDP port that you want to assign to the virtual load-balancing cluster.

Command Default

The default cluster port is 9023.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Vpn load-balancing configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode.

You can specify any valid UDP port number. The range is 1-65535.

If you specify a value for *port* in the **no cluster port** form of the command, the port number specified must match the existing configured port number.

Examples

The following example sets the UDP port for the virtual load-balancing cluster to 9023:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enters vpn load-balancing configuration mode.

cluster redistribute vpn-sessiondb

To re-balance active sessions on a Distributed VPN cluster, use this command in privileged EXEC mode.

cluster redistribute vpn-sessiondb

Syntax Description

This command has no arguments.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	• Yes

Command History

Release	Modification
9.9(1)	Command added for the Firepower 9300.
9.23(1)	Support added for the Secure Firewall 4200.

Usage Guidelines

This command executes in the background and will return to the CLI, no console message will be displayed to the user when the operation is complete.

To monitor progress, use the **show cluster vpn-sessiondb distribution** command, or enable syslogs

The ASR operation must be performed on the master node, the orchestrator of the VPN sessions. The orchestrator is responsible for calculating which sessions will move and where. The orchestrator itself can move active sessions from itself to other nodes as well.

To reduce load on the cluster during this operation and to ensure a timely response time, a maximum of 100 sessions to be moved will be requested at any one time. If the calculated move was 1000 for one node, there would be 10 separate requests for that calculation.

The orchestrator will consider a move request complete for a node when all of the sessions have been moved, or if the owner member cannot move the requested number of sessions.

There are ways a redistribution operation will abort including if a node is unable to respond to the move request or there is a cluster topology change (member join/leave).

This is a best-effort operation. There is no guarantee that after the operation is complete that there will be a perfect distribution. Some nodes may have as much as 20% more/less sessions than average.

Examples

For example, if you have the following results from the show cluster vpn-sessiondb distribution:

```
Member 0 (unit-1-1): active: 229; backups at: 1(120), 2(109)
Member 1 (unit-1-3): active: 224; backups at: 0(117), 2(107)
Member 2 (unit-1-2): active: 0
After the ASR operation, the result looks like:
Member 0 (unit-1-1): active: 151; backups at: 1(120), 2(31)
Member 1 (unit-1-3): active: 151; backups at: 0(117), 2(34)
Member 2 (unit-1-2): active: 151; backups at: 0(72), 1(79)


Example of a successful initiation:
ciscoasa/master# cluster redistribute vpn-sessiondb
Session redistribution initiated.
Use 'show cluster vpn-sessiondb distribution' to view distribution.
Initiation when redistribution is already in progress:
ciscoasa/master# cluster redistribute vpn-sessiondb
Redistribution already in progress
Use 'show cluster vpn-sessiondb distribution' to view distribution.
When executed on a slave node

ciscoasa/slave# cluster redistribute vpn-sessiondb
ERROR: This command is only allowed on the cluster master
```

Related Commands

Command	Description
vpn-mode	Enable distributed VPN

cluster remove unit

To remove the unit from the ASA cluster, use the cluster remove unit command in privileged EXEC mode.

cluster remove unit *unit_name*

Syntax Description

unit_name	Specifies the local unit name to removes from the cluster. To view member names, enter **cluster remove unit ?**, or enter the **show cluster info** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The bootstrap configuration remains intact, as well as the last configuration synced from the master unit, so you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master unit is elected.

Examples

The following example checks for unit names, and then removes asa2 from the cluster:

```
ciscoasa(config)# cluster remove unit ?
Current active units in the cluster:
asa2
ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Related Commands

Command	Description
cluster exec	Sends a command to all cluster members.
cluster group	Configures a cluster.
cluster master unit	Sets a new unit as the master unit of an ASA cluster.

Command	Description
cluster remove unit	Removes the unit from the cluster.

cluster replication delay

To enable the cluster replication delay for TCP connections, use the **cluster replication delay** command in cluster group configuration mode. To disable the delay, use the **no** form of this command.

cluster replication delay *seconds* { **http** | **match tcp** { **host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6** } [{ **eq** | **lt** | **gt** } **port**] { **host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6** } [{ **eq** | **lt** | **gt** } *port*] }

no cluster replication delay *seconds* { **http** | **match tcp** { **host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6** } [{ **eq** | **lt** | **gt** } **port**] { **host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6** } [{ **eq** | **lt** | **gt** } *port*] }

Syntax Description

seconds	Sets the delay between 1 and 15 seconds.
http	Sets the delay for all HTTP traffic. The **http** delay is enabled by default for 5 seconds.

Command Default

The **http** delay is enabled by default for 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.4(1.152)	This command was added.

Usage Guidelines

This feature helps eliminate the “unnecessary work” related to short-lived flows by delaying the director/backup flow creation.

Examples

The following example sets the FTP delay to 15 seconds, and the HTTP delay to 15 seconds:

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

Related Commands

Command	Description
cluster group	Configures the cluster group settings.

cn-id

To configure a cn-id in a reference-identity object, use the **cn-id** command in ca-reference-identity mode. To delete a cn-id, use the **no** form of this command. You can access the *ca-reference-identity* mode by first entering the **crypto ca reference-identity** command to configure a reference-identity object..

cn-id*value*
no cn-id *value*

Syntax Description

value	Value of each reference-id.
cn-id	Common Name (CN), where the value matches the overall form of a domain name. The CN value cannot be free text. A CN-ID reference identifier does not identify an application service.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ca-reference-identity	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity.

The reference identifiers **cn-id** and **dns-id** MAY NOT contain information identifying the application service and MUST contain information identifying the DNS domain name.

Examples

The following example creates a reference-identity for a syslog server:

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Related Commands

Command	Description
crypto ca reference-identity	Configures a reference identity object.

Command	Description
dns-id	Configures and DNS domain name Identifier in a reference identity object.
srv-id	Configures a SRV-ID identifier in a reference identity object.
uri-id	Configures a URI identifier in a reference identity object.
logging host	Configures a logging server that can use a reference-identity object for a secure connection.
call-home profile destination address http	Configures a Smart Call Home server that can use a reference-identity object for a secure connection.

command-alias

To create an alias for a command, use the **command-alias** command in global configuration mode. To remove the alias, use the **no** form of this command.

command-alias mode *command_alias original_command*
no command-alias mode *command_alias original_command*

Syntax Description

command_alias	Specifies the new name for an existing command.
mode	Specifies the command mode in which you want to create the command alias, for example **exec** (for user and privileged EXEC modes), **configure**, or **interface**.
original_command	Specifies the existing command or command with its keywords for which you want to create the command alias.

Command Default

By default, the following user EXEC mode aliases are configured:

- **h** for **help**
- **lo** for **logout**
- **p** for **ping**
- **s** for **show**

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you enter the command alias, the original command is invoked. You might want to create command aliases to provide shortcuts for long commands, for example.

You can create an alias for the first part of any command and still enter the additional keywords and arguments as normal.

When you use CLI help, command aliases are indicated by an asterisk (*), and displayed in the following format:

```
*command-alias=original-command
```

For example, the **lo** command alias displays along with other privileged EXEC mode commands that start with “lo,” as follows:

```
ciscoasa# lo?
*lo=logout login  logout
```

You can use the same alias in different modes. For example, you can use “happy” in privileged EXEC mode and configuration mode to alias different commands, as follows:

```
ciscoasa(config)# happy?
configure mode commands/options:
*happy="username employee1 password test"
exec mode commands/options:
*happy=enable
```

To list only commands and omit aliases, begin your input line with a space. Also, to circumvent command aliases, use a space before entering the command. In the following example, the alias named “happy” is not shown, because there is a space before the happy? command.

```
ciscoasa(config)# alias exec test enable
ciscoasa(config)# exit
ciscoasa#   happy?
ERROR: % Unrecognized command
```

As with commands, you can use CLI help to display the arguments and keywords that can follow a command alias.

You must enter the complete command alias. Shortened aliases are not accepted. In the following example, the parser does not recognize the hap command as indicating the alias named “happy”:

```
ciscoasa# hap
% Ambiguous command: "hap"
```

Examples

The following example shows how to create a command alias named “**save**” for the **copy running-config startup-config** command:

```
ciscoasa(config)# command-alias exec save copy running-config startup-config
ciscoasa(config)# exit
ciscoasa# save
Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e
2209 bytes copied in 0.210 secs
ciscoasa#
```

Related Commands

Command	Description
clear configure command-alias	Clears all nondefault command aliases.
show running-config command-alias	Displays all nondefault command aliases configured.

command-queue

To specify the maximum number of MGCP commands that are queued while waiting for a response, use the **command-queue** command in mgcp-map configuration mode. To remove the configuration, use the **no** form of this command.

command-queue*limit*
no command-queue *limit*

Syntax Description

limit	Specifies the maximum number of commands to queue, from 1 to 2147483647.

Command Default

This command is disabled by default.

The default for the MGCP command queue is 200.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Mgcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **command-queue** command to specify the maximum number of MGCP commands that are queued while waiting for a response. The range of allowed values is from 1 to 4294967295. The default is 200. When the limit has been reached and a new command arrives, the command that has been in the queue for the longest time is removed.

Examples

The following example limits the MGCP command queue to 150 commands:

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)#command-queue 150
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debugging information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.

Commands	Description
show mgcp	Displays MGCP configuration and session information.
timeout	Configures the idle timeout after which an MGCP media or MGCP PAT xlate connection will be closed.

commercial-security

To define an action when the Commercial Security (CIPSO) option occurs in a packet header with IP Options inspection, use the **commercial-security** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

commercial-security action { **allow** | **clear** }
no commercial-security action { **allow clear** }

Syntax Description

allow	Allow packets containing the Commercial Security IP option.
clear	Remove the Commercial Security option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Commercial Security IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# commercial-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

community-list

To create or configure a Border Gateway Protocol (BGP) community list and to control access to it, use the community-list command in global configuration command. To delete the community list, use the no form of this command

StandardCommunityLists
community-list { *standard* | **standard** *list-name* } { **deny** | **permit** } [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**]
no community-list { *standard* | **standard** *list-name* }
ExpandedCommunityLists
community-list { *expanded* | **expanded** *list-name* } { **deny** | **permit** } *regexp*
no community-list { *expanded* | **expanded** *list-name* }

Syntax Description

standard	Configures a standard community list using a number from 1 to 99 to identify one or more permit or deny groups of communities.
standard list-name	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
community-number	(Optional) Specifies a community as a 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.
AA:NN	(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.
internet	(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).
no-export	(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.
local-AS	(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised to external peers or to other subautonomous systems within a confederation.
no-advertise	(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).
Expanded	Configures an expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.
expanded list-name	Configures a named expanded community list.

regexp	Configures a regular expression that is used to specify a pattern to match against an input string. **Note** Regular expressions can be used only with expanded community lists.

Command Default

BGP community exchange is not enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The community-list command is used to configure BGP community filtering. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the bgp-community new-format command is entered in global configuration mode. The new community format consists of a 4-byte value.

The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported. BGP community attribute exchange between BGP peers is enabled when the neighbor send-community command is configured for the specified neighbor. The BGP community attribute is defined in RFC 1997and RFC 1998.

BGP community exchange is not enabled by default. It is enabled on a per-neighbor basis with the neighbor send-community command. The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the set community command.

Once a permit value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it

will match the earliest part first. For more information about configuring regular expressions, see the "Regular Expressions" appendix of theCisco IOS Terminal Services Configuration Guide.

Community List Processing

When multiple values are configured in the same community list statement, a logical AND condition is created. All community values must match to satisfy an AND condition. When multiple values are configured in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

In the following example, a standard community list is configured that permits routes that from network 10 in autonomous system 50000:

```
ciscoasa(config)#  community-list 1 permit 50000:10
```

In the following example, a standard community list is configured that permits only routes from peers in the same autonomous system or from subautonomous system peers in the same confederation:

```
ciscoasa(config)#  community-list 1 permit no-export
```

In the following example, a standard community list is configured to deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
ciscoasa(config)#  community-list 2 deny 65534:40 65412:60
```

In the following example, a named standard community list is configured that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
ciscoasa(config)#  community-list standard RED permit local-AS
ciscoasa(config)#  community-list standard RED permit 40000:20
```

In the following example, an expanded community list is configured that will deny routes that carry communities from any private autonomous system:

```
ciscoasa(config)#  community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
```

In the following example, a named expanded community list configured that denies routes from network 1 through 99 in autonomous system 50000:

```
ciscoasa(config)#  community-list expanded BLUE deny 50000:[0-9][0-9]_
```

Related Commands

Commands	Description
bgp-community-new format	Configures BGP to display communities in the format AA:NN (autonomous system:community number/4-byte number).
neighbor send-community	Specifies that a communities attribute should be sent to a BGP neighbor
set community	Sets the BGP communities attribute.

compatible rfc1583

To restore the method that is used to calculate the summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583
no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl provider configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Only the **no** form of this command appears in the configuration.

Examples

The following example shows how to disable an RFC 1583-compatible route summary cost calculation:

```
ciscoasa(config-router)# no compatible rfc1583
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

compression

To enable compression for anyconnect-ssl connections and WebVPN connections, use the **compression** command in global configuration mode. To remove the command from the configuration, use the **no** form of the command.

compression { **all** | **anyconnect-ssl** | **http-comp** }
no compression { **all** | **anyconnect-ssl** | **http-comp** }

all	Specifies enabling all available compression techniques.
anyconnect-ssl	Specifies compression for anyconnect-ssl connections.
http-comp	Specifies compression for WebVPN connections.

Command Default

The default is *all* . All available box-wide compression techniques are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **compression** command configured in global configuration mode overrides the **compression** anyconnect-ssl command configured in group policy webvpn and username webvpn configuration modes.

For example, if you enter the **anyconnect-ssl compression** command for a certain group in group policy webvpn configuration mode, and then you enter the **no compression** command in global configuration mode, you override the **anyconnect-ssl compression** command settings that you have configured for the group.

Conversely, if you turn compression back on with the **compression** command in global configuration mode, any group settings take effect, and those settings ultimately determine the compression behavior.

If you disable compression with the **no compression** command, only new connections are affected. Active connections remain unaffected.

Examples

In the following example, compression is turned on for anyconnect-ssl connections:

```
hostname(config)# compression anyconnect-ssl
```

In the following example, compression is disabled for anyconnect-ssl and WebVPN connections:

```
hostname(config)# no
 compression anyconnect-ssl http-comp
```

Related Commands

Command	Description
show webvpn anyconnect-ssl	Displays information about the anyconnect-ssl installation.
anyconnect-ssl enable	Enables or requires the anyconnect-ssl for a specific group or user.
anyconnect-ssl compression	Enables compression of HTTP data over an anyconnect-ssl connection for a specific group or user.

config-register

To set the configuration register value that is used the next time you reload the ASA, use the **config-register** command in global configuration mode. To set the value back to the default, use the **no** form of this command.

config-register *hex_value*
no config-register

Syntax Description

hex_value	Sets the configuration register value as a hexadecimal number from 0x0 to 0xFFFFFFFF. This number represents 32 bits and each hexadecimal character represents 4 bits. Each bit controls a different characteristic. However, bits 32 through 20 are either reserved for future use, cannot be set by the user, or are not currently used by the ASA; therefore, you can ignore the three characters that represent those bits, because they are always set to 0. The relevent bits are represented by 5 hexadecimal characters: 0x*nnnnn* . You do not need to include preceding 0s. You do need to include trailing 0s. For example, 0x2001 is equivalent to 0x02001; but 0x10000 requires all the zeros. See <xref> for more information about available values for the relevant bits.

Command Default

The default value is 0x1, which boots from the local image and startup configuration.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl provider configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is only supported on the ASA 5500 series. The configuration register value determines which image to boot from as well as other boot parameters.

The five characters are numbered from 0 to 4 from right to left, which is standard for hexadecimal and binary numbers. You can select one value for each character, and mix and match values as appropriate. For example, you can select either 0 or 2 for character number 3. Some values take priority if they conflict with other values. For example, if you set 0x2011, which sets the ASA to both boot from the TFTP server and to boot from the local image, the ASA boots from the TFTP server. Because this value also stipulates that if the TFTP boot fails, the ASA should boot directly into ROMMON, then the action that specifies to boot from the default image is ignored.

A value of 0 means no action unless otherwise specified.

<xref> lists the actions associated with each hexadecimal character; choose one value for each character:

Table 5:

Prefix	Hexadecimal Character Numbers 4, 3, 2, 1, and 0				
0x	**0**	**0**	**0** [1]	**0** [2]	**0**
	1 Disables the 10 second ROMMON countdown during startup. Normally, you can press Escape during the countdown to enter ROMMON.	**2** If you set the ASA to boot from a TFTP server, and the boot fails, then this value boots directly into ROMMON.		**1** Boots from the TFTP server image as specified in the ROMMON Boot Parameters (which is the same as the **boot** *system tftp* command, if present). This value takes precedence over a value set for character 1.	**1** Boots the image specified by the first **boot** *system local_flash* command. If that image does not load, the ASA tries to boot each image specified by subsequent **boot** *system* commands until it boots successfully.
				4 [3] Ignores the startup configuration and loads the default configuration.	

Prefix	Hexadecimal Character Numbers 4, 3, 2, 1, and 0				
					2, 4, 6, 8 Boots the image specified by a particular **boot** *system local_flash* command. Value 3 boots the image specified in the first *boot system* command, value 5 boots the second image, and so on. If the image does not boot successfully, the ASA does not attempt to fall back to other **boot** *system* command images (this is the difference between using value 1 and value 3). However, the ASA has a failsafe feature that in the event of a boot failure attempts to boot from any image found in the root directory of internal Flash memory. If you do not want the failsafe feature to take effect, store your images in a different directory than root.

Prefix	Hexadecimal Character Numbers 4, 3, 2, 1, and 0				
				5 Performs both actions above.	**3, 5, 7, 9** From ROMMON, if you enter the **boot** command without any arguments, then the ASA boots the image specified by a particular boot *system local_flash* command. Value 3 boots the image specified in the first *boot system* command, value 5 boots the second image, and so on. This value does not automatically boot an image.

[1] Reserved for future use.
[2] If character numbers 0 and 1 are not set to automatically boot an image, then the ASA boots directly into ROMMON.
[3] If you disable password recovery using the **service password-recovery** command, then you cannot set the configuration register to ignore the startup configuration.

The configuration register value is not replicated to a standby unit, but the following warning is displayed when you set the configuration register on the active unit:

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

You can also set the configuration register value in ROMMON using the **confreg** command.

Examples

The following example sets the configuration register to boot from the default image:

```
ciscoasa(config)# config-register 0x1
```

Related Commands

Command	Description
boot	Sets the boot image and startup configuration.

Command	Description
service password-recovery	Enables or disables password recovery.

config-replicate-parallel

To sync configuration changes with slave units in parallel instead of sequentially, use the **config-replicate-parallel** command in cluster configuration mode. To disable this feature, use the **no** form of this command.

config-replicate-parallel
no config-replicate-parallel

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.14(1)	Command added.

Usage Guidelines

Parallel configuration syncing improves performance over sequential syncing.

Examples

The following example disables parallel syncing:

```
ciscoasa(config)# cluster cluster1
ciscoasa(cfg-cluster)# no config-replicate-parallel
```

Related Commands

Command	Description
cluster	Enters cluster configuration mode

configure factory-default

To restore the configuration to the factory default, use the **configure factory-default** command in global configuration mode.

configure factory-default [*ip_address* [*mask*]]

Syntax Description

ip_address	Sets the IP address of the management or inside interface, instead of using the default address, 192.168.1.1. See the "Usage Guidelines" sections for more information about which interface is configured for your model.
mask	Sets the subnet mask of the interface. If you do not set a mask, the ASA uses the mask appropriate for the IP address class.

Command Default

The default IP address and mask are 192.168.1.1 and 255.255.255.0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	A factory default configuration was added for the ASA 5505.

Usage Guidelines

The factory default configuration is the configuration applied by Cisco to new ASAs. This command is supported on all platforms except for the PIX 525 and PIX 535 ASAs.

For the PIX 515/515E and the ASA 5510 and higher ASAs, the factory default configuration automatically configures a management interface so you can connect to it using ASDM, with which you can then complete your configuration. For the ASA 5505, the factory default configuration automatically configures interfaces and NAT so that the ASA is ready to use in your network.

This command is available only for routed firewall mode; transparent mode does not support IP addresses for interfaces, and setting the interface IP address is one of the actions this command takes. This command is also only available in single context mode; an ASA with a cleared configuration does not have any defined contexts to automatically configure using this command.

This command clears the current running configuration and then configures several commands.

If you set the IP address in the **configure factory-default** command, then the **http** command uses the subnet that you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify.

After you restore the factory default configuration, save it to internal Flash memory using the **write memory** command. The **write memory** command saves the running configuration to the default location for the startup configuration, even if you previously configured the **boot config** command to set a different location; when the configuration was cleared, this path was also cleared.

Note This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external Flash memory card. The next time you reload the ASA after restoring the factory configuration, it boots from the first image in internal Flash memory; if you do not have an image in internal Flash memory, the ASA does not boot.

To configure additional settings that are useful for a full configuration, see the **setup** command.

ASA 5505 Configuration

The default factory configuration for the ASA 5505 configures the following:

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. If you did not set the IP address in the **configure factory-default** command, then the VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.
- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address using DHCP.
- The default route is also derived from DHCP.
- All inside IP addresses are translated when accessing the outside using interface PAT.
- By default, inside users can access the outside with an access list, and outside users are prevented from accessing the inside.
- The DHCP server is enabled on the ASA, so a PC connecting to the VLAN 1 interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
```

```
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 and Higher Configuration

The default factory configuration for the ASA 5510 and higher configures the following:

- The management Management 0/0 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the ASA, so a PC connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E Security Appliance Configuration

The default factory configuration for the PIX 515/515E security appliance configures the following:

- The inside Ethernet1 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the PIX security appliance, so a PC connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Examples

The following example resets the configuration to the factory default, assigns the IP address 10.1.1.1 to the interface, and then saves the new configuration as the startup configuration:

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
Begin to apply factory-default configuration:
Clear all configuration
...
ciscoasa(config)#
ciscoasa(config)# copy running-config startup-config
```

Related Commands

Command	Description
boot system	Sets the software image from which to boot.
clear configure	Clears the running configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
setup	Prompts you to configure basic settings for the ASA.
show running-config	Shows the running configuration.

configure http

To merge a configuration file from an HTTP(S) server with the running configuration, use the **configure http** command in global configuration mode.

configure [**interface** *name*] **http** [**s**] **://** [*user* [**:** *password*] **@**] *server* [*: port*] **/** [*path* **/**]] *filename*

Syntax Description

:password	(Optional) For HTTP(S) authentication, specifies the password.
:*port*	(Optional) Specifies the port. For HTTP, the default is 80. For HTTPS, the default is 443.
@	(Optional) If you enter a name and/or a password, precedes the server IP address with an at sign (@).
filename	Specifies the configuration filename.
http[**s**]	Specifies either HTTP or HTTPS.
interface *name*	(Optional) Specifies the interface name through which the configuration file will be copied. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
path	(Optional) Specifies a path to the filename.
server	Specifies the server IP address or name. For IPv6 server addresses, if you specify the port, then you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the port number. For example, enter the following address and port: `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	(Optional) For HTTP(S) authentication, specifies the username.

Command Default

For HTTP, the default port is 80. For HTTPS, the default port is 443.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5(1)	The **interface** *name* argument was added.

Usage Guidelines

This command supports IPv4 and IPv6 addresses. A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration, but are not set in the new configuration.

This command is the same as the copy **http running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure http** command is an alternative for use within a context.

If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table. Note that if you have a default route through a management-only interface, all **configure** traffic will match that route and never check the data routing table. In this scenario, always specify the interface if you need to copy through a data interface.

Examples

The following example copies a configuration file from an HTTPS server to the running configuration:

```
ciscoasa(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands that you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure memory

To merge the startup configuration with the running configuration, use the **configure memory** command in global configuration mode.

configure memory

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration, but are not set in the new configuration.

If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the ASA, and then enter the **configure memory** command to load the new configuration.

This command is equivalent to the **copy startup-config running-config** command.

For multiple context mode, a context startup configuration is at the location specified by the **config-url** command.

Examples

The following example copies the startup configuration to the running configuration:

```
ciscoasa(config)# configure memory
```

Related Commands

Command	Description
clear configure	Clears the running configuration.

Command	Description
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands that you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure net

To merge a configuration file from a TFTP server with the running configuration, use the **configure net** command in global configuration mode.

configure net [**interface** *name*] [*server* **:** [*filename*]] **:** *filename*]

Syntax Description

:*filename*	Specifies the path and filename. If you already set the filename using the **tftp-server** command, then this argument is optional. If you specify the filename in this command as well as a name in the **tftp-server** command, the ASA treats the **tftp-server** command filename as a directory, and adds the **configure net** command filename as a file under the directory. To override the **tftp-server** command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path. If you specified the TFTP server address using the **tftp-server** command, you can enter the filename alone preceded by a colon (:).
interface *name*	(Optional) Specifies the interface name through which the configuration file will be copied. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
*server***:**	Sets the TFTP server IP address or name. This address overrides the address you set in the **tftp-server** command, if present. For IPv6 server addresses, you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the filename. For example, enter the following address: [fe80::2e0:b6ff:fe01:3b7a] The default gateway interface is the highest security interface; however, you can set a different interface name using the **tftp-server** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5(1)	The **interface** *name* argument was added.

Usage Guidelines

This command supports IPv4 and IPv6 addresses. A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration, but are not set in the new configuration.

This command is the same as the **copy tftp running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure net** command is an alternative for use within a context.

If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table. Note that if you have a default route through a management-only interface, all **configure** traffic will match that route and never check the data routing table. In this scenario, always specify the interface if you need to copy through a data interface.

Examples

The following example sets the server and filename in the **tftp-server** command, and then overrides the server using the **configure net** command. The same filename is used.

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:
```

The following example overrides the server and the filename. The default path to the filename is /tftpboot/configs/config1. The /tftpboot/ part of the path is included by default when you do not lead the filename with a slash (/). Because you want to override this path, and the file is also in tftpboot, include the tftpboot path in the **configure net** command.

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

The following example sets the server only in the **tftp-server** command. The **configure net** command specifies only the filename.

```
ciscoasa(config)# tftp-server inside 10.1.1.1
ciscoasa(config)# configure net :configs/config1
```

Related Commands

Command	Description
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
show running-config	Shows the running configuration.

Command	Description
tftp-server	Sets a default TFTP server and path for use in other commands.
write net	Copies the running configuration to a TFTP server.

configure session

To create or open a configuration session, where you can edit ACLs and objects in isolation, use the **configure session** command in privileged EXEC mode.

configure session *session_name*

Syntax Description

session_name	The name of a configuration session. If the session already exists, you open that session. Otherwise, you are creating a new session. Use the **show configuration session** command for a list of current sessions.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

When you edit an ACL used for access rules or any other purpose, the change is immediately implemented and impacts traffic. With access rules, you can enable the transactional commit model to ensure that new rules become active only after rule compilation is complete, but the compilation happens after each ACE you edit.

If you want to further isolate the impact of editing ACLs, you can make your changes in a "configuration session," which is an isolated mode that allows you to edit several ACEs and objects before explicitly committing your changes. Thus, you can ensure that all of your intended changes are complete before you change device behavior.

Use the **configure session** command to create a new session or to open an existing one. You cannot open a session if someone else already has it open for editing. If you determine that the session is not actually being edited, you can reset the access flag using the **clear session** *session_name* **access** command, and then open it.

You can have up to three sessions defined at a time.

Within a session, you can use the following commands:

- Configuration commands—In uncommitted sessions, you can use the following basic commands with any of their parameters:
  - **access-list**

- **object**
- **object-group**

- Session management commands— The commands available depend on whether you have previously committed the session. Possible commands are:
  - **exit**—To simply exit the session without committing or discarding changes, so that you can return later.
  - **commit** [**noconfirm** [**revert-save** | **config-save**]]—(Uncommitted sessions only.) To commit your changes. You are asked if you want to save the session. You can save the revert session (**revert-save**), which lets you undo your changes using the **revert** command, or the configuration session (**config-save**), which includes all of the changes made in the session (allowing you to commit the same changes again if you would like to). If you save the revert or configuration session, the changes are committed, but the session remains active. You can open the session and revert or recommit the changes. You can avoid the prompt by including the **noconfirm** option and optionally, the desired save option.
  - **abort**—(Uncommitted sessions only.) To abandon your changes and delete the session. If you want to keep the session, exit the session and use the **clear session** *session_name* **configuration** command, which empties the session without deleting it.
  - **revert**—(Committed sessions only.) To undo your changes, returning the configuration back to what it was before you committed the session, and delete the session.
  - **show configuration session** [*session_name*]—To show the changes made in the session.

Examples

The following example opens my-session:

```
ciscoasa# configure session my-session access
ciscoasa(config-s)#
```

Related Commands

Command	Description
clear configuration session	Deletes a configuration session and its contents.
clear session	Clears the contents of a configuration session or resets its access flag.
forward-reference	Lets you refer to objects or ACLs in ACEs or access groups before they exist.
show configuration session	Shows the changes made in each current session.

configure terminal

To configure the running configuration at the command line, use the **configure terminal** command in privileged EXEC mode.

configure terminal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command enters global configuration mode, which lets you enter commands that change the configuration.

Examples

The following example enters global configuration mode:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
show running-config	Shows the running configuration.

config-url

To identify the URL from which the system downloads the context configuration, use the **config-url** command in context configuration mode.

config-url*url*

Syntax Description

url Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax:

- **disk0:**/[*path*/]*filename*

For the ASA 5500 series, this URL indicates the internal Flash memory. You can also use the **flash** command instead of the **disk0** command; they are aliased.

- **disk1:**/[*path*/]*filename*

For the ASA 5500 series, this URL indicates the external Flash memory card.

- **flash:**/[*path*/]*filename*

This URL indicates the internal Flash memory.

- **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]

The **type** can be one of the following keywords:

- **ap**—ASCII passive mode
- **an**—ASCII normal mode
- **ip**—(Default) Binary passive mode
- **in**—Binary normal mode
- **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*
- **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*]

Specify the interface name if you want to override the route to the server address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Context configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you add a context URL, the system immediately loads the context so that it is running.



Note Enter the **allocate-interface** command(s) before you enter the **config-url** command. The ASA must assign interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (**interface**, **nat**, **global**). If you enter the **config-url** command first, the ASA loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

The filename does not require a file extension, although we recommend using ".cfg."

The admin context file must be stored on the internal Flash memory.

If you download a context configuration from an HTTP or HTTPS server, you cannot save changes back to these servers using the **copy running-config startup-config** command. You can, however, use the **copy tftp** command to copy the running configuration to a TFTP server.

If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready for you to configure with the command-line interface.

To change the URL, reenter the **config-url** command with a new URL.

The ASA merges the new configuration with the current running configuration. Reentering the same URL also merges the saved configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used. If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

Examples

The following example sets the admin context to "administrator," creates a context called "administrator" on the internal Flash memory, and then adds two contexts from an FTP server:

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context
 administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
```

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url
 flash:/admin.cfg
ciscoasa(config-ctx)# context
 test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# context
 sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

Related Commands

Command	Description
allocate-interface	Allocates interfaces to a context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

connect fxos

To connect to FXOS from the ASA CLI on a Firepower 1000/2100, or Secure Firewall 4200, enter the **connect fxos** command in privileged EXEC mode.

connect fxos [**admin**]

Syntax Description

admin (Optional) For the Firepower 1000 or the Firepower 2100 in Appliance mode, specify **admin** for admin-level access. Without this option, users have read-only access. Note that no configuration commands are available even in admin mode.

This keyword is not available for the Firepower 2100 in Platform mode.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	We added this command.
9.13(1)	Added the **admin** keyword.

Usage Guidelines

Firepower 1000 and 2100 in Appliance Mode

The Firepower 1000 and 2100 Appliance mode console port connects you to the ASA CLI (unlike the Firepower 2100 Platform mode console, which connects you to the FXOS CLI). From the ASA CLI, you can then connect to the FXOS CLI using Telnet for troubleshooting purposes.

You are not prompted for user credentials. The current ASA username is passed through to FXOS, and no additional login is required. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Within FXOS, you can view user activity using the **scope security/show audit-logs** command.

Firepower 2100 in Platform Mode

If you SSH or Telnet to the ASA, connect to the FXOS CLI using this command. You are prompted to authenticate for FXOS; use the default username: **admin** and password: **Admin123**. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

If your initial connection is to FXOS (for example on the console port), you can use the **connect asa** command to connect to the ASA CLI. Do not use the **connect** commands to return to the original connection CLI; you must exit the connection instead.

Examples

The following connects to the FXOS CLI on the Firepower 1000 or 2100 in Appliance mode:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

The following connects to the FXOS CLI on the Firepower 2100 in Platform mode:

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
FXOS 2.2(2.32) kp2110
kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software
[...]
kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Related Commands

Command	Description
fxos permit	Allows FXOS management access on ASA data interfaces.
fxos port	Sets the FXOS management access port.
ip-client	Allows FXOS management traffic to egress the ASA data interface.

conn data-rate

To view the connections on the device that are passing heavy loads of data, use the **conn data-rate** command in privileged exec mode. This command displays per-flow data rate along with the existing connection information. To disable the collection of connections by data-rate, use the **no** form of the command.

conn data-rate
no conn data-rate

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.14(1)	This command was added.

Usage Guidelines

The **conn data-rate** command is most useful to determine which connections, and users, might be contributing the most to the overall load on the device.

When enabled, the conn data-rate feature tracks two statistics for all connections:

- The current (1-second) data rate in the forward and reverse direction of a connection.
- The maximum 1-second data rate in the forward and reverse direction of a connection.

Examples

The following example shows how to enable the connection data rate collection:

```
ciscoasa(config)#conn data-rate
ciscoasa(config)#
```

Related Commands

Command	Description
show conn data-rate	Displays the current state of the connection data rate tracking.
show conn detail	Displays filtered connections by data-rate value.

Command	Description
clear conn data-rate	Clears the current maximum data-rate value.

conn-rebalance

To enable connection rebalancing between members of a cluster, use the **conn-rebalance** command in cluster group configuration mode. To disable connection rebalancing, use the **no** form of this command.

conn-rebalance [**frequency** *seconds*]
no conn-rebalance [**frequency** *seconds*]

Syntax Description

frequency *seconds*	(Optional) Specifies how often the load information is exchanged, between 1 and 360 seconds. The default is 5 seconds.

Command Default

Connection rebalancing is disabled by default.

If enabled, the default frequency is 5 seconds

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If the load balancing capabilities of the upstream or downstream routers result in unbalanced flow distribution, you can configure overloaded units to redirect new flows to other units. No existing flows will be moved to other units. If enabled, ASAs exchange load information periodically, and offload new connections from more loaded devices to less loaded devices.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units.

Examples

The following example sets the connection rebalance frequency to 60 seconds:

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.

Command	Description
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables conn ection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

consent-token generate-challenge

To generate a one-time token for Linux root-level shell access, use the **consent-token generate-challenge** command in privileged EXEC mode. This command is available on the ASA Virtual and must be used under Cisco TAC supervision.

consent-token generate-challenge shell-access *minutes*

consent-token accept-response

To validate a response string and grant one-time access to the Linux root shell, use the **consent-token accept-response** command in privileged EXEC mode. This command is available on the ASA Virtual and must be used under Cisco TAC supervision.

consent-token accept-response shell-access

console-replicate

To enable console replication from slave units to the master unit in an ASA cluster, use the **console-replicate** command in cluster group configuration mode. To disable console replication, use the **no** form of this command.

console-replicate
noconsole-replicate

Syntax Description

This command has no arguments or keywords.

Command Default

Console replication is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The ASA prints out some messages directly to the console for certain critical events. If you enable console replication, slave units send the console messages to the master unit so you only need to monitor one console port for the cluster.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units.

Examples

The following example enables console replication:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# console-replicate
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.

Command	Description
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

console timeout

To set the inactivity timeout for an authenticated serial console session (**aaa authentication serial console**) so that a user is logged out of the console after the timeout, or for an authenticated enable session (**aaa authentication enable console**) where the user exits privileged EXEC mode and reverts to user EXEC mode after the timeout, use the **console timeout** command in global configuration mode. To disable the inactivity timeout for an authenticated serial console session, use the **no** form of this command.

console timeout [*number*]
no console timeout [*number*]

Syntax Description

number	Specifies the idle time in minutes (0 through 60) after which the console session ends. 0 means the console never times out.

Command Default

The default timeout is 0, which means the console session will not time out.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl provider configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **console timeout** command only applies to authenticated serial or enable connections. This command does not alter the Telnet, SSH, or HTTP timeouts; these access methods maintain their own timeout values. The command does not affect unauthenticated console connections.

The **no console timeout** command resets the console timeout value to the default timeout of 0, which means that the console will not time out.

Examples

The following example shows how to set the console timeout to 15 minutes:

```
ciscoasa(config)# console timeout 15
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
clear configure timeout	Restores the default idle time durations in the configuration.

Command	Description
show running-config console timeout	Displays the idle timeout for a console connection to the ASA.

content-length

To restrict HTTP traffic based on the length of the HTTP message body, use the **content-length** command in http-map configuration mode. To remove this command, use the **no** form of this command.

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** { **allow** | **reset** | **drop** } [**log**]
no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action	Specifies the action taken when a message fails this inspection.
allow	Allows the message.
bytes	Specifies the number of bytes. The permitted range is 1 to 65535 for the **min** option and 1 to 50000000 for the **max** option.
drop	Closes the connection.
log	(Optional) Generates a syslog.
max	(Optional) Specifies the maximum content length allowed.
min	Specifies the minimum content length allowed.
reset	Sends a TCP reset message to the client and server.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Http-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

After enabling the content-length command, the ASA only allows messages within the configured range and otherwise takes the specified action. Use the **action** keyword to cause the ASA to reset the TCP connection and create a syslog entry.

Examples

The following example restricts HTTP traffic to messages 100 bytes or larger and not exceeding 2000 bytes. If a message is outside this range, the ASA resets the TCP connection and creates a syslog entry.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# content-length min 100 max 2000 action reset log
ciscoasa(config-http-map)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

context

To create a security context in the system configuration and enter context configuration mode, use the **context** command in global configuration mode. To remove a context, use the **no** form of this command.

context*name*
no context *name* [**noconfirm**]

Syntax Description

name	Sets the name as a string up to 32 characters long. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. "System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.
noconfirm	(Optional) Removes the context without prompting you for confirmation. This option is useful for automated scripts.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

In context configuration mode, you can identify the configuration file URL and interfaces that a context can use. If you do not have an admin context (for example, if you clear the configuration), then the first context you add must be the admin context. To add an admin context, see the **admin-context** command. After you specify the admin context, you can enter the **context** command to configure the admin context.

You can only remove a context by editing the system configuration. You cannot remove the current admin context using the **no** form of this command; you can only remove it if you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to "administrator," creates a context called "administrator" on the internal Flash memory, and then adds two contexts from an FTP server:

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context
```

```
 administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url
 flash:/admin.cfg
ciscoasa(config-ctx)# context
 test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# context
 sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts and the system execution space.
config-url	Specifies the location of the context configuration.
join-failover-group	Assigns a context to a failover group.
show context	Shows context information.

copy

To copy a file to or from the ASA flash memory, use the **copy** command in privileged EXEC mode.

copy [**/noconfirm** | **/noverify**] [*interface_name*] [**/pcap**] { *url* | **running-config** | **startup-config** } { **running-config** | **startup-config** | *url* }

Syntax Description

/noconfirm	(Optional) Copies the file without a confirmation prompt.
interface_name	(Optional) Specifies the interface name through which the file will be copied. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
/pcap	(Optional) Specifies the raw packet capture dump of the **capture** command.
/noverify	(Optional) Skips the signature verification when copying development key signed images.
running-config	Specifies the running configuration stored in system memory.
startup-config	Specifies the startup configuration stored in flash memory. The startup configuration for single mode or for the system in multiple context mode is a hidden file in flash memory. From within a context, the location of the startup configuration is specified by the **config-url** command. For example, if you specify an HTTP server for the **config-url** command and then enter the **copy startup-config running-config** command, the ASA copies the startup configuration from the HTTP server using the admin context interface.

url Specifies the source or destination file to be copied between local and remote locations. (You cannot copy from a remote server to another remote server.)

In a context, you can access remote servers for the following cases:

- Copy the **running-config** , **startup-config**, or **capture:** to a TFTP or FTP server using the context interfaces. You cannot copy from a server to the running or startup configuration. See the **startup-config** keyword for other options. To download from a TFTP server to the running context configuration, use the **configure net** command.
- If you configure private storage (**storage-url private**) for the context, you can copy any files to and from external servers.
- In all cases, SCP within a context is not supported with the CiscoSSH stack.

Some URLs are only available as the source or as the destination. See the CLI help for exact usage. Use the following URL syntax for this command:

- **cache:**/[[*path*/]*filename*]—Indicates the cache memory in the file system.
- **capture:**/[[*context_name*/]*buffer_name*]—Indicates the output in the capture buffer.
- **cluster_trace:**—Indicates the cluster trace file system.
- **cluster:/**[[*path*/]*filename*]—Indicates the cluster file system.
- **disk***n***:/**[[*path*/]*filename*]—**disk0:** is the internal memory. Other drive numbers represent external storage such as a USB drive, SSD, or SD card.
- (Insecure, not recommended.) **smb:**/[[*path*/]*filename*]—Indicates a UNIX server local file system. Use Server Message Block file-system protocol in LAN managers and similar network systems to package data and exchange information with other systems.
- (Insecure, not recommended.) **ftp:**//[[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode).
- (Use HTTPS; HTTP is insecure, not recommended.) **http**[**s**]**:**//[[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*]
- **scp:**//[[*user* [**:***password*]**@**]*server* [*/path*]*/filename* [**;int=***interface_name*]]—The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.
- **system:/**[[*path*/]*filename*]—Represents the system memory.
- **system:text**—Represents the main ASA process as text that you can copy from the ASA for analysis.
- (Insecure, not recommended.) **tftp:**//[[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*[**;int=***interface_name*]]

  The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command. The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the TFTP server.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes [4]	• Yes

[4] Within a context, you can only copy the **running-config**, **startup-config**, or **capture:** to an external URL; or to and from private storage (**storage-url private**).

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	Added support for DNS names.
8.0(2)	Added the **smb** option.
9.1(5)	Added the **scp** option.
9.3(2)	Added the /**noverify** option.
9.5(1)	Added the *interface_name* argument.
9.6(2)	Added the **system:text** keyword.
9.16	If you include the password in an FTP URL, it is ignored. You must enter the password when prompted for it.
9.17(1)	If you use the CiscoSSH stack (the **ssh stack ciscossh** command), then if you want to use **copy** with SCP, you must allow SSH access for the SCP server IP address using the **ssh** command. The CiscoSSH stack does not support using SCP within a context.

Usage Guidelines

- When you copy a configuration to the running configuration, you merge the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.
- If an RSA key cannot be saved in NVRAM, the following error message appears:

```
ERROR: NV RAM does not have enough space to save keypair keypair name
```

- After you have performed a cluster-wide capture, you can simultaneously copy the same capture file from all units in the cluster to a TFTP server by entering the following command on the master unit:

```
hostname (config-cluster)# cluster exec copy
 /pcap capture
:
cap_name
tftp://
location/path/filename
.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as filename_A.pcap, filename_B.pcap, where A and B are cluster unit names.



Note A different destination name gets generated if you add the unit name at the end of the filename.

You can also copy the packet capture to a disk. However, ensure that the capture name is less than 63 characters for the copy operation to succeed.

- If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table. Note that if you have a default route through a management-only interface, all **copy** traffic will match that route and never check the data routing table. In this scenario, always specify the interface if you need to copy through a data interface.
- If you use the CiscoSSH stack (the **ssh stack ciscossh** command), then if you want to use **copy** with SCP, you must allow SSH access for the SCP server IP address using the **ssh** command.
- The CiscoSSH stack does not support using SCP within a context. This stack is the default in 9.19 and later. In 9.23 and later, this is the only SSH stack available.
- For FTP transfers, starting with 9.16 and some older point releases, the password is ignored if you include it in the URL. You must always enter the FTP password when prompted for it by the command.

Examples

The following example shows how to copy a file from the disk to an HTTPS server in the system execution space:

```
ciscoasa(config)# copy disk0:my_context/my_context.cfg
https://10.7.0.80/my_context/my_context.cfg
```

The following example shows how to copy a file from one location on the disk to another location on the disk. The name of the destination file can be either the name of the source file or a different name.

```
ciscoasa(config)# copy disk0:my_context.cfg disk0:my_context/my_context.cfg
```

The following example shows how to copy an ASDM file from am HTTPS server to the internal flash memory:

```
ciscoasa(config)# copy https://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

The following example shows how to copy the running configuration in a context to an HTTPS server:

```
ciscoasa(config)# copy running-config https://10.7.0.80/my_context/my_context.cfg
```

The **copy** command supports DNS names as well as IP addresses, as shown in this version of the preceding example:

```
ciscoasa(config)# copy running-config https://www.example.com/my_context/my_context.cfg
```

The following example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
ciscoasa(config)# copy capture:abc https
Address or name of remote host [209.165.200.224]?
Source file name [username/cdisk]?
copying capture to https://209.165.200.224/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

You can specify the full path as follows:

```
ciscoasa(config)# copy capture:abc tftp:209.165.200.224/tftpboot/abc.cap
```

If the TFTP server is already configured, the location or filename can be unspecified as follows:

```
ciscoasa
(co
nfig)# tftp-server outside 209.165.200.224 tftp/cdisk
ciscoasa
(config)#
copy capture:abc tftp:/tftp/abc.cap
```

The following example shows how to copy a development key signed image without verifying it:

```
ciscoasa(config)# copy /noverify lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

Related Commands

Command	Description
configure net	Copies a file from a TFTP server to the running configuration.
copy capture	Copies a capture file to a TFTP server.

Command	Description
tftp-server	Sets the default TFTP server.

cpu hog granular-detection

To provide real-time hog detection and set the CPU hog threshold in a short period of time, use the cpu hog granular-detection command in privileged EXEC mode.

cpu hog granular-detection [**count** *number*] [**threshold** *value*]

Syntax Description

count *number*	Specifies the number of code execution interruptions performed. Valid values are from 1-10000000. The default and recommended value is 1000.
threshold *value*	Ranges from 1 to 100. If not set, the default is used, which varies among platforms.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The **cpu hog granular-detection** command interrupts the current code execution every 10 milliseconds, and the total number of interruptions is the count. The interruption checks for CPU hogging. If there is any, it is logged. This command reduces the granularity of CPU hog detection in the data path.

Each scheduler-based hog is associated with up to 5 interrupt-based hog entries; each entry could have up to 3 tracebacks. The interrupt-based hog cannot be overwritten; if there is no space, the new one is discarded. The scheduler-based hog is still reused according to the LRU policy, and its associated interrupt-based hog is cleared by then.

Note Performance may be affected on the ASA 5585-X with small UDP packets.

Examples

The following example show how to trigger CPU hog detection:

```
ciscoasa# cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
```

```
under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

Related Commands

Command	Description
show process cpu-hog	Displays the processes that are hogging the CPU.
clear process cpu-hog	Clears the processes that are hogging the CPU.

cpu profile activate

To start CPU profiling, use the cpu profile activate command in privileged EXEC mode.

cpu profile-activate *n-samples* [**sample-process** *process-name*] [**trigger-cpu-usage** *cpu %* [*process-name*]]

Syntax Description

n-samples	Allocates memory for storing *n* number of samples. Valid values are from 1 to 100,000.
sample-process *process-name*	Samples only a specific process.
trigger cpu-usage *cpu %*	Prevents the profiler from starting until the global 5-second CPU percentage is greater and stops the profiler if the CPU percentage drops below this value.
trigger cpu-usage *cpu % process-name*	Uses the process 5-second CPU percentage as a trigger.

Command Default

The *n-samples* default value is 1000.

The *cpu %* default value is 0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.1(2)	The **sample-process** *process-name* , **trigger cpu-usage** *cpu %* , and **trigger cpu-usage** *cpu % process-name* options were added. The output format was updated.

Usage Guidelines

The CPU profiler can help you determine which process is using more CPU. Profiling the CPU captures the address of the process that was running on the CPU when the timer interrupt fired. This profiling occurs every 10 milliseconds, regardless of the CPU load. For example, if you take 5000 samples, the profiling takes exactly 50 seconds to complete. If the amount of CPU time that the CPU profiler uses is relatively low, the samples take longer to collect. The CPU profile records are sampled in a separate buffer.

Use the **show cpu profile** command in conjunction with the **cpu profile activate** command to display information that you can collect and that the TAC can use for troubleshooting CPU issues. The **show cpu profile dump** command output is in hexadecimal format.

If the CPU profiler is waiting for a starting condition to occur, the **show cpu profile** command displays the following output:

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

Examples

The following example activates the profiler and instructs it to store 1000 samples.

```
hostname# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump"
to interrupt profiling and display the incomplete results.
```

The following examples show the status of the profiing (in-progress and completed):

```
hostname# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete
or to interrupt profiling and display the incomplete results.
hostname# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2
Process virtual address map:
---------------------------
...
---------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

Related Commands

Command	Description
show cpu profile	Displays the CPU profiling progress.
show cpu profile dump	Displays incomplete or completed results for profiling.

coredump enable

To enable the coredump feature, enter the coredump **enable** command. To disable the command, use the no form of this command.

coredump enable [**filesystem disk** *n :* [**size** [**default** | *size*]]
no coredump enable [**filesystem disk** *n :* [**size** [**default** | *size*]]

Syntax Description

default	Specifies the default is the suggested value to use, because the ASA calculates what this value should be.
filesystem **disk*n*:**	Specifies the disk where the coredump file will be saved.
size	Defines the total size allocated for the coredump file system image on the ASA flash. When configuring coredump, if not enough space is available, an error message appears. It may be helpful to think of the **size** option as a container, which means that coredumps generated will never be allowed to exceed this size in disk space consumption.
size	Specifies that the ASA will override the default value and allocate the specified value in MB for the coredump filesystem (if the space is available).

Command Default

By default, coredumps are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Note For ASAs that are operating on 4100/9300 platforms, use the bootstrap CLI mode for working with coredumps.

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Enabling this feature provides significant troubleshooting information. Disabling this feature results in a coredump file not being generated on a system crash for all components. In addition, disabling this feature does not delete a previous coredump filesystem image and/or the coredump filesystem image contents. When you enable coredumps, you are prompted to allow the coredump filesystem to be created. The prompt is a

confirmation and includes the size (in MB) of the coredump filesystem to be created. It is important that you save your configuration after enabling or disabling coredumps.

Before enabling coredumps, you must be aware of the disk space that is currently available on your ASA device. Enable coredumps only if your ASA has sufficient disk space. The amount of disk space allocated for coredumps is currently based on the ASA platform and its typical memory configuration, such as:

- 60 MB for ASA5505, ASA5510, ASA552
- 100 MB for ASA5540
- 200 MB for ASA5550, ASA5580
- 300 MB for ASA5585

If the default coredump is too large to be stored in the available flash memory, ASA throws an error.

When coredumps are enabled, the following file elements get created. You should never manipulate these file elements explicitly.

- coredumpfsys – Directory that includes coredump images
- coredumpfsysimage.bin – Coredump filesystem image used to manage coredumps
- coredumpinfo – Directory that includes the coredump log



Note Disabling coredumps has no effect on crashinfo file generation.

Cisco TAC may request that you enable the coredump feature to troubleshoot application or system crashes on the ASA.



Note Make sure that you archive the coredump files, because it is possible a subsequent coredump may result in previous coredump(s) being removed to fit the current coredump. Coredump files are located on the configured filesystem (for example, “disk0:/coredumpfsys” or “disk1:/coredumpfsys”) and can be removed from the ASA.

To enable coredump, perform the following steps:

1. Make sure that you are in the /root directory. To verify your directory location on the console, enter the **pwd** command.
2. If necessary, change the directory by entering either the **cd disk0:**/ or **cd disk1:/** command.
3. Enter the **coredump enable** command.

When using the **coredump** command to troubleshoot crashes on the ASA, it is possible that no coredump file is saved after a crash. This can occur when the coredump feature has been enabled and a coredump filesystem with preallocated disk space has been created. This condition usually appears while troubleshooting crashes that occur after a few weeks on busy ASAs that have allocated a large amount of RAM.

In the output of the **show coredump** command, something similar to the following appears:

```
Coredump Aborted as the complete coredump could not be written to flash
   Filesystem full on 'disk0', current coredump size <size> bytes too big
   for allocated filesystem
```

To alleviate this issue, you need to have a coredump filesystem card that is large enough to contain the full memory and allocate corresponding space to the coredump filesystem.

Examples

Each bang (!) in these examples represents 1 MB of the coredump filesystem being written.

The following example uses default values and **disk0:** to create the coredump filesystem.

```
hostname(config)# coredump enable
Warning: Enabling coredump on an ASA5505 platform will delay the
reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceed with coredump filesystem allocation of 60 MB on 'disk0:'
(Note this may take a while) [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The following example shows how to specify the filesystem and size by creating a 120-MB coredump filesystem on **disk1:**

```
hostname(config)# coredump enable filesystem disk1: size 120
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceed with coredump filesystem allocation of 120 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The following example shows how to resize the coredump filesystem from 120 MB to 100 MB:

Note The contents of the 120-MB coredump filesystem are not preserved, so make sure that you archive previous coredumps before doing this.

```
hostname(config)# coredump enable filesystem disk1: size 100
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceeding with resizing to 100 MB results in
deletion of current 120 MB coredump filesystem and
its contents on 'disk1:', proceed ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
```

The following example enables coredump initially on **disk0:**, then on **disk1:**. Also note the use of the **default** keyword.

Note We do not allow two active coredump filesystems, so you must delete the previous coredump filesystem before proceeding.

```
hostname(config)# coredump enable filesystem disk1: size default
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Coredump is currently configured on 'disk0:', upon successful
configuration on 'disk1:', the coredump filesystem will be
deleted on 'disk0:', proceed ? [confirm]
Proceed with coredump filesystem allocation of 100 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
```

The following example shows how to disable the coredump filesystem. However, the current coredump filesystem image and its contents are not affected.

```
hostname(config)# no coredump enable
```

To reenable coredumps, reenter the command you originally used to configure the coredump filesystem.

The following examples disable and reenable coredumps:

- Using default values:

```
hostname(config)# coredump enable
hostname(config)# no coredump enable
hostname(config)# coredump enable
```

- Using explicit values:

```
hostname(config)# coredump enable filesystem disk1: size 200
hostname(config)# no coredump enable
hostname(config)# coredump enable filesystem disk1: size 200
```

Related Commands

Command	Description
clear configure coredump	Removes the coredump filesystem and its contents from your system. Also clears the coredump log.
clear coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log.
show coredump filesystem	Displays files on the coredump filesystem and indicates how full it might be.
show coredump log	Shows the coredump log.

crashinfo console disable

To suppress crash information from being output to the console, use the crashinfo console disable command in global configuration mode.

crashinfo console disable
no crashinfo console disable

Syntax Description

disable	Suppresses console output in the event of a crash.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(4)	This command was added.
	This command has been deprecated and might not be available in the software version you are running.

Usage Guidelines

This command lets you suppress crash information from being output to the console. The crash information may contain sensitive information that is not appropriate for viewing by all users connected to the device. In conjunction with this command, you should also ensure crash information is written to flash, which can be examined after the device reboots. This command affects output for crash information and checkheaps, which is saved to flash and should be sufficient for troubleshooting.

Examples

The following example shows how to suppress crash information from being output to the console:

```
hostname(config)# crashinfo console disable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
fips enable	Enables or disables policy checking to enforce FIPS compliance on the system or module.

Command	Description
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash information output to flash.
show running-config fips	Displays the FIPS configuration that is running on the ASA.

crashinfo force kernel-dump

To force crash dump of the primary kernel, enter the **crashinfo force kernel-dump** command in privileged EXEC mode.

crashinfo force kernel-dump

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	Yes	Yes	Yes	—	Yes

Command History

Release	Modification
9.24(1)	This command was added.

Usage Guidelines

A Secure Firewall product that experiences unexpected Linux kernel crashes or silent reboots does not provide information for debugging the root cause. To effectively capture, store, and facilitate the analysis of Linux kernel crash incidents in the system, use the **crashinfo force kernel-dump** command.

Upon execution, this command checks whether the secondary kernel is configured to support the Linux kernel crash dump. If disabled, the crash dump operation is halted. If enabled, the system prompts the user for confirmation to initiate a crash dump. Upon receiving confirmation, the primary Linux kernel is intentionally crashed, triggering the secondary kernel to boot and capture the incident details.

Examples

The following is a sample output of the **crashinfo force kernel-dump** command when the crash dump is not enabled in the kernels:

```
hostname# crashinfo force kernel-dump
System requests are not enabled. Aborting...

hostname# crashinfo force kernel-dump
Kernel crash dump is not enabled. Aborting...
```

The following is a sample output of the **crashinfo force kernel-dump** command when a user does not provide the confirmation for the dump:

```
hostname# crashinfo force kernel-dump
This will trigger a kernel crash dump and cause the system to reboot.
Are you sure you want to continue? (yes/no): [no]
User did not provide confirmation. Aborting...
```

The following is a sample output of the **crashinfo force kernel-dump** command when a user provides confirmation for the dump:

```
hostname# crashinfo force kernel-dump
This will trigger a kernel crash dump and cause the system to reboot.
Are you sure you want to continue? (yes/no): [yes]
Sending request to crash the kernel. Please wait for the system to restart...
[...]
```

Related Commands

Command	Description
kernel crash-dump	Enables the secondary crash dump kernel.
show kernel crash-dump	Displays the status of the secondary crash dump kernel.

crashinfo force

To force the ASA to crash, use the **crashinfo force** command in privileged EXEC mode.

crashinfo force [**page-fault** | **watchdog** | **dump** [**process** *name*]]

Syntax Description

page-fault	(Optional) Forces a crash of the ASA as a result of a page fault.
watchdog	(Optional) Forces a crash of the ASA as a result of watchdogging.
kernel-dump	Crashes the entire Linux kernel and generates a kernel core dump for analysis.
dump	(Optional) Collects the main ASA process ("lina") core dump and then crashes the system.
process*name*	(Optional) Collects the specified process core dump and then crashes the system. To view available processes, use the **show kernel process** command. If the given process is for a non-killable process, then the ASA issues an appropriate error message and does not kill the process.

Command Default

The ASA saves the crash information file to flash memory by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.24(1)	The **kernel-dump** keyword was introduced.

Usage Guidelines

You can use the **crashinfo force** command to test the crash output generation. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashinfo force page-fault** or **crashinfo force watchdog** command (because these are real crashes). The ASA reloads after the crash dump is complete.



Caution Do not use the **crashinfo force** command in a production environment. The **crashinfo force** command crashes the ASA and forces it to reload.

Examples

The following example shows the warning that displays when you enter the **crashinfo force page-fault** command:

```
ciscoasa# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
Do you wish to proceed? [confirm]:
```

If you enter a carriage return (by pressing the Return or Enter key on your keyboard), "Y," or "y," the ASA crashes and reloads; any of these responses are interpreted as confirmation. Any other character is interpreted as a no, and the ASA returns to the command-line prompt.

Related Commands

clear crashinfo	Clears the contents of the crash information file.
crashinfo save disable	Disables crash information from writing to flash memory.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo	Displays the contents of the crash information file.

crashinfo save disable

To disable crash information from writing to flash memory, use the **crashinfo save** command in global configuration mode. To allow the crash information to be written to flash memory and return to the default behavior, use the **no** form of this command.

crashinfo save disable
no crashinfo save disable

Syntax Description

This command has no arguments or keywords.

Command Default

The ASA saves the crash information file to flash memory by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	The **crashinfo save enable** command was deprecated. Use the **no crashinfo save disable** command instead.
	This command has been deprecated and might not be available in the software version you are running.

Usage Guidelines

Crash information writes to flash memory first, and then to the console.

Note If the ASA crashes during startup, the crash information file is not saved. The ASA must be fully initialized and running first before it can save crash information to flash memory.

Use the no crashinfo save disable command to reenable saving the crash information to flash memory.

Examples

The following example shows how to disable crash information from writing to flash memory:

```
ciscoasa(config)# crashinfo save disable
```

Related Commands

clear crashinfo	Clears the contents of the crash file.

crashinfo force	Forces a crash of the ASA.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo	Displays the contents of the crash file.

crashinfo test

To test the ability of the ASA to save crash information to a file in flash memory, use the **crashinfo test** command in privileged EXEC mode.

crashinfo test

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	The output was updated to display the user enabled crash information file in a new format.

Usage Guidelines

The user enabled crash information file is stored in crashinfo-test_YYYYMMDD_HHMMSS_UTC format. The command output does not display the real crash information. If a previous crash information file already exists in flash memory, that file is overwritten.

Note Entering the **crashinfo test** command does not crash the ASA.

Examples

The following example shows the output of a crash information file test.:

```
ciscoasa# crashinfo test
```

Related Commands

clear crashinfo	Deletes all the crash information files. the contents of the crash file.
crashinfo force	Forces the ASA to crash.
crashinfo save disable	Disables crash information from writing to flash memory.

show crashinfo	Displays the contents of the latest crash information file.
show crashinfo files	Displays the last five crash information files based on the date and timestamp.

crl (Deprecated)

To specify CRL configuration options, use the **crl** command in crypto ca trustpoint configuration mode.

crl { **required** | **optional** | **nocheck** }

Syntax Description

nocheck	Directs the ASA not to perform CRL checking.
optional	The ASA can still accept the peer certificate if the required CRL is not available.
required	The required CRL must be available for a peer certificate to be validated.

Command Default

The default value is **nocheck**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The following forms of the **revocation-check** command replace it. • **revocation-check crl none** replaces **crl optional** • **revocation-check crl** replaces **crl required** • **revocation-check none** replaces **crl nocheck**
9.13(1)	This command was removed.

Examples

The following example enters crypto ca trustpoint configuration mode for a trustpoint central, and requires that a CRL be available for a peer certificate to be validated for this trustpoint:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl required
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.
crl configure	Enters crl configuration mode.
url	Specifies a URL for the CRL retrieval.

crl cache-time

To configure the amount of time (minutes) that a trustpool CRL can remain in the CRL cache before the ASA refreshes it, use the **crl cache-time** command in ca-trustpool configuration mode. To accept the default value of 60 minutes, use the **no** form of this command.

crl cache-time
no crl cache-time

Syntax Description

cache-time	Value in minutes (1-1440).

Command Default

The default value is **60**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpool configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command is consistent with the version of this command supported in the trustpoint configuration mode.

Examples

```
ciscoasa(ca-trustpool)# crl
 cache-time
 30
```

Related Commands

Command	Description
crl enforcenextupdate	Specifies how to handle the NextUpdate CRL field.

crl configure

To enter CRL configuration mode, use the **crl configure** command in crypto ca trustpoint configuration mode.

crl configure

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crl configuration mode for a trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)#
```

crl enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **crl enforcenextupdate** command in ca-trustpool configuration mode. If enabled, CRLs are required to have a NextUpdate field that has not yet lapsed. To not enforce this restriction, use the **no** form of this command:

crl enforcenextupdate
no crl enforcenextupdate

Syntax Description

This command has no arguments or keywords.

Command Default

The default is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpool configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If enabled, CRLs are required to have a NextUpdate field that has not yet elapsed. This command is consistent with the version of this command supported in the trustpoint configuration mode.

Related Commands

Command	Description
crl cache-time	Configures how long a CRL can remain in the CRL cache before ASA refreshes it.



crypto a – crypto ir

- crypto am-disable, on page 917
- crypto ca alerts expiration, on page 918
- crypto ca authenticate, on page 920
- crypto ca certificate chain, on page 925
- crypto ca certificate map, on page 926
- crypto ca crl request, on page 928
- crypto ca enroll, on page 929
- crypto ca export, on page 933
- crypto ca import, on page 936
- crypto ca permit-weak-crypto, on page 938
- crypto ca reference-identity, on page 939
- crypto ca server (Deprecated), on page 942
- crypto ca server crl issue, on page 945
- crypto ca server revoke, on page 947
- crypto ca server unrevoke, on page 949
- crypto ca server user-db add, on page 951
- crypto ca server user-db allow, on page 953
- crypto ca server user-db email-otp, on page 955
- crypto ca server user-db remove, on page 957
- crypto ca server user-db show-otp, on page 959
- crypto ca server user-db write, on page 961
- crypto ca trustpoint, on page 963
- crypto ca trustpool export, on page 967
- crypto ca trustpool import, on page 968
- crypto ca trustpool policy, on page 970
- crypto ca trustpool remove, on page 972
- crypto dynamic-map match address, on page 973
- crypto dynamic-map set df-bit, on page 975
- crypto dynamic-map set ikev1 transform-set, on page 976
- crypto dynamic-map set ikev2 ipsec-proposal, on page 979
- crypto dynamic-map set nat-t-disable, on page 980
- crypto dynamic-map set peer, on page 981
- crypto dynamic-map set pfs, on page 982

- crypto dynamic-map set reverse route, on page 984
- crypto dynamic-map set security-association lifetime, on page 985
- crypto dynamic-map set tfc-packets, on page 987
- crypto dynamic-map set validate-icmp-errors, on page 988
- crypto engine accelerator-bias, on page 989
- crypto engine large-mod-accel, on page 990
- crypto ikev1 enable, on page 992
- crypto ikev1 limit max-in-negotiation-sa, on page 994
- crypto ikev1 policy, on page 996
- crypto ikev2 cookie-challenge, on page 998
- crypto ikev2 enable, on page 1000
- crypto ikev2 fragmentation, on page 1002
- crypto ikev2 limit max-in-negotiation-sa, on page 1004
- crypto ikev2 limit max-sa, on page 1006
- crypto ikev2 limit queue sa_init, on page 1008
- crypto ikev2 notify, on page 1010
- crypto ikev2 policy, on page 1011
- crypto ikev2 redirect, on page 1014
- crypto ikev2 remote-access trust-point, on page 1016
- crypto ipsec df-bit, on page 1018
- crypto ipsec fragmentation, on page 1020
- crypto ipsec ikev1 transform-set, on page 1022
- crypto ipsec ikev1 transform-set mode transport, on page 1025
- crypto ipsec ikev2 ipsec-proposal, on page 1027
- crypto ipsec ikev2 sa-strength-enforcement, on page 1029
- crypto ipsec inner-routing-lookup, on page 1031
- crypto ipsec profile, on page 1033
- crypto ipsec security-association lifetime, on page 1035
- crypto ipsec security-association pmtu-aging, on page 1037
- crypto ipsec security-association replay, on page 1038

crypto am-disable

To disable IPsec IKEv1 inbound aggressive mode connections, use the **crypto ikev1 am-disable** command in global configuration mode. To enable inbound aggressive mode connections, use the **no** form of this command.

crypto ikev1 am-disable
no crypto ikev1 am-disable

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **isakmp am-disable** command was added.
7.2.(1)	The **crypto isakmp am-disable** command replaces the **isakmp am-disable** command**.**
8.4(1)	The command name was changed from crypto isakmp **am-disable to crypto ikev1 am-disable.**

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
ciscoasa(config)# crypto ikev1 am-disable
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears the ISAKMP configuration.
clear configure crypto isakmp policy	Clears the ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays the active configuration.

crypto ca alerts expiration

Expiration checking for all installed certificates is enabled by default with the **crypto ca alerts expiration** command. To disable expiration checking, use the **no** form of this command:

crypto ca alerts expiration [**begin** < **days before expiration** > [**repeat** < **days** >]
[**no**] **crypto ca alerts expiration** [**begin** < **days before expiration** > [**repeat** < **days** >]

Syntax Description

begin <days before expiration>	Set the interval at which the reminders are sent by configuring the number of days before expiration at which the first alert will go out. The range is from 1 to 90 days.
repeat <*days*>	Configure the alert frequency if the certificate is not renewed. The range is 1 to 14 days.

Command Default

Expiration checking for all installed certificate is enabled by default.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command Modes

The following table shows the modes in which you can enter the command:

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Since the reminders are syslog messages, we do not anticipate a need for disabling. This command has little impact on performance because it is only checked once a day. By default we will send the first alert 60 days prior to expiration and once every week after that until the certificate is renewed and removed. In addition, an alert is sent on the day of the expiration and once every day after that. Irrespective of the alerts configuration, a reminder is sent every day during the last week of expiration.

Examples

```
100(config)# crypto ca ?
configure mode commands/options:
  alerts        Configure alerts
100(config)# crypto ca alerts ?
configure mode commands/options:
  expiration  Configure an alert for certificates nearing expiration
100(config)# crypto ca alerts expiration ?
configure mode commands/options:
  begin   Begin alert
  repeat  Repeat alert
  <cr>100(config)# crypto ca alerts expiration begin ?
```

```
configure mode commands/options:
  <1-90>  Days prior to expiration at which the first alert should be sent
100(config)# crypto ca alerts expiration begin 10 ?
configure mode commands/options:
  repeat  Repeat alert
  <cr>
100(config)# crypto ca alerts expiration begin 10 repeat ?
configure mode commands/options:
  <1-14>  Number of days at which the alert should be repeated after the prior
          alert
100(config)# crypto ca alerts expiration begin 10 repeat 1
100(config)# show run crypto ca ?
exec mode commands/options:
  alerts       Show alerts


   server    Show local certificate server configuration
 trustpoint     Show trustpoints
   trustpool    Show trustpool
  |            Output modifiers
  <cr>
100(config)# show run crypto ca alerts
crypto ca alerts expiration begin 10 repeat 1
100(config)# clear conf crypto ca ?
configure mode commands/options:
  alerts       Clear alerts
  certificate  Clear certificate map entries
  server       Clear Local CA server
  trustpoint   Clear trustpoints
  trustpool    Clear trustpool
100(config)# clear conf crypto ca alerts
```

Related Commands

Command	Description
clear conf crypto ca alerts	Clears the configured crypto ca alerts.
show run crypto ca alerts	Shows the configured crypto ca alerts.

crypto ca authenticate

To install and authenticate the CA certificates associated with a trustpoint, use the **crypto ca authenticate** command in global configuration mode.

crypto ca authenticate *trustpoint* [**allow-untrusted-connection**] [**fingerprint** *hexvalue*] [**nointeractive**]

Syntax Description

fingerprint	Specifies a hash value consisting of alphanumeric characters that the ASA uses to authenticate the CA certificate. If a fingerprint is provided, the ASA compares it to the computed fingerprint of the CA certificate and accepts the certificate only if the two values match. If there is no fingerprint, the ASA displays the computed fingerprint and asks whether to accept the certificate.
hexvalue	Identifies the hexadecimal value of the fingerprint.
allow-untrusted-connection	Allows the ASA to ignore EST server certificate validation failure. This option is available only for trustpoints that are configured with the EST enrollment protocol.
nointeractive	Obtains the CA certificate for this trustpoint using no interactive mode; intended for use by the device manager only. In this case, if there is no fingerprint, the ASA accepts the certificate without question.
trustpoint	Specifies the trustpoint from which to obtain the CA certificate. The maximum name length is 128 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.16(1)	The **allow-untrusted-connection** keyword was introduced to ignore EST server certificate validation failure.
9.22(3), 9.23(1)	Support to add ACME CA certificate was added.

Usage Guidelines

Use the **crypto ca authenticate** command to add a CA certificate to a trustpoint in the ASA configuration. When configured, the certificate is considered trusted.

If the trustpoint is configured for SCEP enrollment, the CA certificate is downloaded through SCEP. If not, the ASA prompts you to paste the base-64 formatted CA certificate into the terminal.

The **allow-untrusted-connection** keyword can be used to allow the ASA to ignore server certificate validation failure for EST trustpoints.

The invocations of this command do not become part of the running configuration.

Examples

The following example shows the ASA requesting the certificate of the CA. The CA sends its certificate and the ASA prompts the administrator to verify the certificate of the CA by checking the CA certificate fingerprint. The ASA administrator should verify the fingerprint value displayed with a known, correct value. If the fingerprint displayed by the ASA matches the correct value, you should accept the certificate as valid.

```
ciscoasa(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y
#
ciscoasa(config)#
```

The following example shows the trustpoint tp9 configured for terminal-based (manual) enrollment. The ASA prompts the administrator to paste the CA certificate into the terminal. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained.

```
ciscoasa(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=
Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]:
yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
ciscoasa(config)#
```

The following example shows successful certification validation when an EST trustpoint is configured without using **allow-untrusted-connection** and **nointeractive** keywords. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows successful certification validation when an EST trustpoint is configured with **nointeractive** keyword. After displaying the fingerprint of the certificate, the ASA does not prompt the administrator to confirm that the certificate should be retained:

```
   asa(config-ca-trustpoint)# crypto ca authenticate EST_TP nointeractive

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Trustpoint CA certificate accepted.
```

The following example shows successful certification validation when an EST trustpoint is configured with **allow-untrusted-connection**. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows successful certification validation when an EST trustpoint is configured with **allow-untrusted-connection** and **nointeractive** keywords. After displaying the fingerprint of the certificate, the ASA does not prompt the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection
nointeractive

TLS Connection to EST server https://est-server.example.com:8443 validated successfully by
 trust anchor.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when an EST trustpoint is configured without using **allow-untrusted-connection** and **nointeractive** keywords. ASA prompts the administrator to confirm if the TLS server certificate validation should be bypassed. If it is bypassed,

the fingerprint of the certificate is displayed and the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
Bypass TLS server certificate validation: [yes/no]: yes

INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when an EST trustpoint is configured with **nointeractive** keyword.

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP nointeractive

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
 ERROR: receiving Certificate Authority certificate: status = FAIL, cert length = 0
asa(config-ca-trustpoint)#
```

The following example shows failed certification validation when an EST trustpoint is configured with **allow-untrusted-connection** keyword. ASA bypasses the TLS server certificate validation. After displaying the fingerprint of the certificate, the ASA prompts the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when an EST trustpoint is configured with **allow-untrusted-connection** and **nointeractive** keywords. ASA bypasses the TLS server certificate validation. After displaying the fingerprint of the certificate, the ASA does not prompt the administrator to confirm that the certificate should be retained:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP allow-untrusted-connection
nointeractive

TLS Connection to EST server https://est-server.example.com:8443 could not be validated.
INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d

Trustpoint CA certificate accepted.
```

The following example shows failed certification validation when there is a fingerprint mismatch:

```
asa(config-ca-trustpoint)# crypto ca authenticate EST_TP fingerprint 87654321 1212121212
11111111 12345678

INFO: Certificate has the following attributes:
Fingerprint:     a76027e8 0518a06c d0710845 b104303d
Fingerprint mismatch

Trustpoint CA certificate NOT accepted.
```

The following example shows how to use the **crypto ca authenticate** command to add an ACME CA certificate to the trustpoint. This command is optional when trust is already established for the signing path of the certificate to be issued.

```
ciscoasa(config)# crypto ca authenticate my_acme_tp
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
<----snipped--->
-----END CERTIFICATE-----
quit
INFO: Certificate has the following attributes:
Fingerprint:     7e589f83 386c48fa 740bcfeb b7643dba
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca enroll	Starts enrollment with a CA.
crypto ca import certificate	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca certificate chain

To enter certificate chain configuration mode for the indicated trustpoint, use the **crypto ca certificate chain** command in global configuration mode.

crypto ca certificate chain *trustpoint*

Syntax Description

trustpoint	Specifies the trustpoint for configuring the certificate chain.

Command Default

No default values or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters certificate chain configuration mode for the trustpoint, central:

```
ciscoasa
(config)#
crypto ca certificate chain central
ciscoasa
(config-cert-chain)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.

crypto ca certificate map

To maintain a prioritized list of certificate mapping rules, use the **crypto ca certificate map** command in global configuration mode. To remove a crypto CA configuration map rule, use the **no** form of the command.

crypto ca certificate map { *sequence-number* | *map-name sequence-number* }
no crypto ca certificate map { *sequence-number* | *map-name sequence-number* }

Syntax Description

map-name	Specifies a name for a certificate-to-group map.
sequence-number	Specifies a number for the certificate map rule that you are creating. The range is 1 through 65535. You can use this number when creating a tunnel group map, which maps a tunnel group to a certificate map rule.

Command Default

The default value for *map-name* is DefaultCertificateMap.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The *map-name* option was added.

Usage Guidelines

Entering this command places the ASA in ca certificate map configuration mode, where you can configure rules based on the issuer and subject distinguished names (DNs) of the certificate. The sequence number orders the mapping rules. The general form of these rules is as follows:

- *DN match-criteria match-value*
- *DN* is either *subject-name* or *issuer-name*. DNs are defined in the ITU-T X.509 standard.
- *match-criteria* comprise the following expressions or operators:

attr *tag*	Limits the comparison to a specific DN attribute, such as common name (CN).
co	Contains
eq	Equal

nc	Does not contain
ne	Not equal

The DN matching expressions are case insensitive.

Examples

The following example enters ca certificate map mode with a map named example-map and a sequence number of 1 (rule # 1), and specifies that the common name (CN) attribute of the subject-name must match Example1:

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name attr cn eq Example1
ciscoasa(ca-certificate-map)#
```

The following example enters ca certificate map mode with a map named example-map and a sequence number of 1, and specifies that the subject-name contain the value cisco anywhere within it:

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name co cisco
ciscoasa(ca-certificate-map)#
```

Related Commands

Command	Description
issuer-name	Indicates that rule entry is applied to the issuer DN of the IPsec peer certificate.
subject-name (crypto ca certificate map)	Indicates that rule entry is applied to the subject DN of the IPsec peer certificate.
tunnel-group-map enable	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

crypto ca crl request

To request a CRL based on the configuration parameters of the specified trustpoint, use the **crypto ca crl request** command in crypto ca trustpoint configuration mode.

crypto ca crl request *trustpoint*

Syntax Description

trustpoint	Specifies the trustpoint. The maximum number of characters allowed is 128.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Invocations of this command do not become part of the running configuration.

Examples

The following example requests a CRL based on the trustpoint named central:

```
ciscoasa(config)# crypto ca crl request central
ciscoasa(config)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.

crypto ca enroll

To start the certificate enrollment process with the CA, use the **crypto ca enroll** command in global configuration mode.

crypto ca enroll *trustpoint* [**est-username** *name* **est-password** *password*] [**regenerate**] [**shared-secret** < **value** > | **signing-certificate** < **value** >] [**noconfirm**]

Syntax Description

noconfirm	(Optional) Suppresses all prompts. Enrollment options that might have been prompted for must be preconfigured in the trustpoint. This option is for use in scripts, ASDM, or other noninteractive needs.
regenerate	Indicates whether or not a new key pair should be generated prior to building the enrollment request.
shared-secret	A value provided out-of-band by the CA that is used to confirm the authenticity and integrity of the messages exchanged with ASA..
signing-certificate	The name of the trustpoint with a previously-issued device certificate used for signing the cmp enrollment request.
trustpoint	Specifies the name of the trustpoint to enroll with. The maximum number of characters allowed is 128.
est-username *user*	The EST username used for initial enrollment. This keyword is available only for trustpoints that are configured with the EST enrollment protocol.
est-password *password*	The EST password used for initial enrollment. This keyword is available only for trustpoints that are configured with the EST enrollment protocol.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	The option to regenerate was added, and the shared-secret and signing-certificate keywords were added.

Release	Modification
9.16(1)	The provision to enroll an EST certificate was added.
9.22(3), 9.23(1)	The provision to enroll an ACME certificate was added.

Usage Guidelines

Use **crypto ca enroll** command to initiate a certificate enrollment or re-enrollment with a CA.

When the trustpoint is configured for SCEP enrollment, the ASA displays a CLI prompt immediately and status messages appear on the console asynchronously. When the trustpoint is configured for manual enrollment, the ASA writes a base-64-encoded PKCS10 certificate request to the console and then the CLI prompt appears.

This command generates interactive prompts that vary, depending on the configured state of the referenced trustpoint. For this command to run successfully, the trustpoint must have been configured correctly.

When a trustpoint is configured for CMP, either a shared secret value (ir) or the name of the trustpoint that contains the cert that will sign the request (cr) can be specified, but not both. The shared-secret or signing-certificate keywords are available only when the trustpoint enrollment protocol is set to CMP.

This command supports certificate enrollment using EST. You can provide the username and password credentials to authenticate the device to the EST server when issuing the enrollment request. Use this command regardless of whether a certificate has already been issued. If you do not provide the username and password credentials, the device uses the pre-existing device certificate to authenticate the device to the server. If a device certificate is not present, the command becomes invalid.

Examples

The following example requests enrollment for an identity certificate with trustpoint tp1 using SCEP enrollment. The ASA prompts for information not stored in the trustpoint configuration.

```
ciscoasa(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
ciscoasa(config)#
```

The following example shows manual enrollment of a CA certificate:

ciscoasa(config)# **crypto ca enroll tp1**

```
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
```

```
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
ciscoasa(config)#
```

Examples

The following example requests enrollment for an identity certificate with trustpoint EST_TP using EST enrollment, when the http credentials are provided:

```
asa(config-ca-trustpoint)# crypto ca enroll EST_TP ?
configure mode commands/options:
  est-username       Specify EST username for HTTP authentication
  <CR>

asa(config)# crypto ca enroll EST_TP username ?

configure mode commands/options:
  WORD < 32 char username required for initial EST enrollment.
asa(config)# crypto ca enroll EST_TP username ESTUSER ?

configure mode commands/options:
 est-password         Specify EST password for HTTP authentication
asa(config)# crypto ca enroll EST_TP user ESTUSER password ?

configure mode commands/options:
  WORD < 32 char password required for initial EST enrollment

asa(config)# crypto ca enroll EST_TP est-username ESTUSER est-password ESTPASSWORD ?

configure mode commands/options:
  noconfirm  Specify this keyword to suppress all interactive prompting.

asa(config)# crypto ca enroll EST_TP est-username ESTUSER est-password ESTPASSWORD
%
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: asa.cisco.com

% The serial number in the certificate will be: FCH1814JT76

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
asa(config)# The certificate has been granted by CA!
```

The following example shows re-enrollment using device certificates:

```
asa(config-ca-trustpoint)# crypto ca enroll EST_TP
%
WARNING: Trustpoint EST_TP has already enrolled and has
a device cert issued to it.
If you successfully re-enroll this trustpoint,
the existing certificate will be replaced.
```

```
Do you want to continue with re-enrollment? [yes/no]: yes
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: asa.cisco.com

% The serial number in the certificate will be: FCH1814JT76

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
asa(config)# The certificate has been granted by CA!
```

Examples

The following example shows how to use the **crypto ca enroll** command to request ACME enrollment to the *my_acme_tp* trustpoint when regenerate (generate a new key while renewing certificate) is opted:

```
ciscoasa(config)#
ciscoasa(config)# crypto ca enroll my_acme_tp
Would you like to continue with this enrollment? [yes/no]: yes
% Start certificate enrollment ..
% The subject name in the certificate will be: cn=test-asav20.bxb-vpn.com
% The fully-qualified domain name in the certificate will be: test-asav20.bxb-vpn.com
Request certificate from CA? [yes/no]: yes
ciscoasa(config)# SUCCESS: The certificate has been granted by CA!
```

Related Commands

Command	Description
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca import pkcs12	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca export

To export the ASA trustpoint configuration with all associated keys and certificates in PKCS12 format, or to export the device identity certificate in PEM format, use the **crypto ca export** command in global configuration mode.

crypto ca export *trustpoint* **identity-certificate**

Syntax Description

identity-certificate	Specifies that the enrolled certificate associated with the named trustpoint is to be displayed on the console.
trustpoint	Specifies the name of the trustpoint whose certificate is to be displayed. The maximum number of characters allowed for a trustpoint name is 128.

Command Default

No default values or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	This command was changed to accommodate certificate exporting in PEM format.

Usage Guidelines

Invocations of this command do not become part of the active configuration. The PEM or PKCS12 data is written to the console.

Web browsers use the PKCS12 format to store private keys with accompanying public key certificates protected with a password-based symmetric key. The ASA exports the certificates and keys associated with a trustpoint in base64-encoded PKCS12 format. This feature can be used to move certificates and keys between ASAs.

PEM encoding of a certificate is a base64 encoding of an X.509 certificate enclosed by PEM headers. This encoding provides a standard method for text-based transfer of certificates between ASAs. PEM encoding can be used to export the *proxy-ldc-issuer* certificate using an SSL/TLS protocol proxy when the ASA is acting as a client.

Examples

The following example exports the PEM-formatted certificate for trustpoint 222 as a console display:

```
ciscoasa
```

```
 (config)#
crypto ca export 222 identity-certificate
Exported 222 follows:
```

-----BEGIN CERTIFICATE-----

MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt

```
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----

ciscoasa
 (config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca enroll	Starts enrollment with a CA.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca import

To install a certificate received from a CA in response to a manual enrollment request or to import the certificate and key pair for a trustpoint using PKCS12 data, use the **crypto ca import** command in global configuration mode.

crypto ca import *trustpoint* **certificate** [**nointeractive**]
crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

Syntax Description

certificate	Tells the ASA to import a certificate from the CA represented by the trustpoint.
nointeractive	(Optional) Imports a certificate using nointeractive mode, which suppresses all prompts. This option is for use in scripts, ASDM, or other noninteractive needs.
passphrase	Specifies the passphrase used to decrypt the PKCS12 data.
pkcs12	Tells the ASA to import a certificate and key pair for a trustpoint, using PKCS12 format.
trustpoint	Specifies the trustpoint with which to associate the import action. The maximum number of characters allowed is 128. If you import PKCS12 data and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example manually imports a certificate for the trustpoint Main:

```
ciscoasa
 (config)#
crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself[ certificate data omitted ]quit
INFO: Certificate successfully imported
```

```
ciscoasa
 (config)#
```

The following example manually imports PKCS12 data to a trustpoint central:

```
ciscoasa
 (config)#
crypto ca import central pkcs12 ?
configure mode commands/options:
 WORD Passphrase used to protect the pkcs12 data
Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:[ PKCS12 data omitted ]quit
INFO: Import PKCS12 operation completed successfully
ciscoasa
 (config)#
```

The following example, entered in global configuration mode with passphrase *Wh0ist*, generates a warning message because there is not enough space in NVRAM to save the RSA keypair:

```
ciscoasa(config)# crypto ca import central pkcs12 Wh0ist

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
INFO: The name for the keys will be: central
Keypair generation process begin. Please wait...
NV RAM will not have enough space to save keypair central. Remove any unnecessary keypairs
 and save the running config before using this keypair.
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca export	Exports a trustpoint certificate and key pair in PKCS12 format.
crypto ca authenticate	Obtains the CA certificate for a trustpoint.
crypto ca enroll	Starts enrollment with a CA.
crypto ca trustpoint	Enters the crypto ca trustpoint configuration mode for the indicated trustpoint.

crypto ca permit-weak-crypto

ASA does not support CA certificates with the SHA-1 with RSA encryption algorithm and RSA key sizes smaller than 2048 bits. You can use the **crypto ca permit-weak-crypto** command to override certification restrictions. We do not recommend you to use this option, because the certificates generated with weak ciphers and key sizes are not as secure as the certificates with bigger key sizes and strong ciphers.

[no] crypto ca permit-weak-crypto

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.16(1)	This command was added.

Usage Guidelines

When you enable **permit-weak-crypto**, ASA allows the following options when validating certificates:

- SHA-1 with RSA encryption algorithm.
- RSA key sizes smaller than 2048 bits.

If the **permit-weak-crypto** option is not enabled, the certificate validation operations fail when these attributes are present.

Examples

The following example enables weak-crypto on the ASA:

```
asa(config)# crypto ca ?

configure mode commands/options:
permit-weak-crypto (Not Recommended) permit weak key sizes and hash algorithms
```

crypto ca reference-identity

To configure a reference-identity object, use the **crypto ca reference-identity** command in configuration mode. To delete a reference-identity object, use the **no** form of this command.

crypto ca reference-identity *reference_identity_name*
no crypto ca reference-identity *reference_identity_name*

Enter the **crypto ca reference-identity** command in global configuration mode to place the ASA in ca-reference-identity mode. Enter the following reference-ids while in ca-reference-identity mode. Multiple reference-ids of any type may be added. Use the no form of each command to remove reference-ids.

[**no**] **cn-id** *value*
[**no**] **dns-id** *value*
[**no**] **srv-id** *value*
[**no**] **uri-id** *value*

Syntax Description

reference-identity-name	Name of the reference-identity object.
value	Value of each reference-id.
cn-id	Common Name (CN), where the value matches the overall form of a domain name. The CN value cannot be free text. A CN-ID reference identifier does not identify an application service.
dns-id	A subjectAltName entry of type dNSName. This is a DNS domain name. A DNS-ID reference identifier does not identify an application service.
srv-id	A subjectAltName entry of type otherName whose name form is SRVName as defined in RFC 4985. A SRV-ID identifier may contain both a domain name and an application service type. For example, a SRV-ID of "_imaps.example.net" would be split into a DNS domain name portion of "example.net" and an application service type portion of "imaps."
uri-id	A subjectAltName entry of type uniformResourceIdentifier whose value includes both (i) a "scheme" and (ii) a "host" component (or its equivalent) that matches the "reg-name" rule specified in RFC 3986. A URI-ID identifier must contain the DNS domain name, not the IP address, and not just the hostname. For example, a URI-ID of "sip:voice.example.edu" would be split into a DNS domain name portion of "voice.example.edu" and an application service type of "sip."

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Enter the **crypto ca reference-identity** command in global configuration mode to place the ASA in ca-reference-identity mode. Enter the following reference-ids while in ca-reference-identity mode: cn-id, dns-id, srv-id, or uri-id. Multiple reference-ids of any type may be added. Use the no form of each command to remove reference-ids.

A reference identity is created when configuring one with a previously unused name. Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity.

When multiple entries are used, the following behavior is expected if the certificate contains at least one instance of srv-id, uri-id, or dns-id:

- If any instance of uri-id in the certificate matches any instance of uri-id on the named reference id, then the certificate matches the reference identity.
- If any instance of srv-id in the certificate matches any instance of srv-id on the named reference id, then the certificate matches the reference identity.
- If any instance of dns-id in the certificate matches any instance of dns-id on the named reference id, then the certificate matches the reference identity.
- If none of these scenarios exist, the certificate does not match the reference identity.

When multiple entries are used, the following behavior is expected if the certificate does not contain at least one instance of srv-id, uri-id, or dns-id but does contain at least one cn-id:

- If any instance of cn-id in the certificate matches any instance of cn-id on the named reference id, then the certificate matches the reference identity. Otherwise, the certificate does not match the reference identity.
- If the certificate does not contain at least one instance of srv-id, uri-id, dns-id, or cn-id, then the certificate does not match the reference identity.

When the ASA is acting as a TLS client, it supports rules for verification of an application server's identity as defined in RFC 6125. Reference identities are configured on the ASA, to be compared to the identity presented in a server certificate during connection establishment. These identifiers are specific instances of the four identifier types also specified in RFC 6125.

The reference identifiers **cn-id** and **dns-id** MAY NOT contain information identifying the application service and MUST contain information identifying the DNS domain name.

Examples

The following example creates a reference-identity for a syslog server:

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Related Commands

Command	Description
cn-id	Configures a Common Name Identifier in the reference-identity object.
dns-id	Configures and DNS domain name Identifier in a reference identity object.
srv-id	Configures a SRV-ID identifier in a reference identity object.
uri-id	Configures a URI identifier in a reference identity object.
logging host	Configures a logging server that can use a reference-identity object for a secure connection.
call-home profile destination address http	Configures a Smart Call Home server that can use a reference-identity object for a secure connection.

crypto ca server (Deprecated)

To set up and manage a local CA server on the ASA, use the **crypto ca server** command in global configuration mode. To delete the configured local CA server from the ASA, use the **no** form of this command.

crypto ca server
no crypto ca server

Syntax Description

This command has no arguments or keywords.

Command Default

A certificate authority server is not enabled on the ASA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.12(1)	Provision to configure user's FQDN for the enrollment URL, under smtp command. If not configured, the ASAs' FQDN will be used by default. This command is being deprecated and will be removed in a future release.
9.13(1)	This command was removed.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

There can only be one local CA on an ASA.

The **crypto ca server** command configures the CA server, but does not enable it. Use the **no** form of the **shutdown** command in ca server configuration mode to enable the local CA.

When you activate the CA server with the **no shutdown** command, you establish the RSA keypair of the CA and a trustpoint named LOCAL-CA-SERVER to hold the self-signed certificate. This newly generated self-signed certificate always has digital signature, CRL signing, and certificate signing key usage settings set.

Beginning with version 9.12(1), ASA allows users to configure their FQDN for the enrollment URL. Typically, users have an internal DNS configured as the ASAs FQDN and an external DNS configured with the FQDN that is included in the enrollment email. Using the fqdn command, the users can configure their FQDN for the enrollment URLinstead of ASAs' FQDN. If not configured, ASA uses its FQDN by default.

Caution The **no crypto ca server** command deletes the configured local CA server, its RSA keypair, and the associated trustpoint, regardless of the current state of the local CA server.

Examples

The following example enters ca server configuration mode, then lists the local CA server commands available in that mode:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# ?
CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
                        certificates
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

The following example shows configuration of user's fqdn under smtp command and the verification output:

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp fqdn asa1-localCA.server.amazon.com
ciscoasa(config-ca-server)# show run crypto ca server
crypto ca server
smtp fqdn asa1-localCA.server.amazon.com
```

The following example uses the **no** form of the **crypto ca server** command in ca server configuration mode to delete the configured and enabled CA server from the ASA:

```
ciscoasa
(config-ca-server)
# no crypto ca server
Certificate server 'remove server' event has been queued for processing.
ciscoasa(config)#
```

Related Commands

Command	Description
debug crypto ca server	Shows debugging messages when you configure the local CA server.
show crypto ca server	Displays the status and parameters of the configured CA server.

Command	Description
show crypto ca server cert-db	Displays local CA server certificates.

crypto ca server crl issue

To force the issuance of a Certificate Revocation List (CRL), use the **crypto ca server crl issue** command in privileged EXEC mode.

crypto ca server crl issue

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use this command to recover a lost CRL. Normally, the CRL is reissued automatically at expiration by resigning the existing CRL. The **crypto ca server crl issue** command regenerates the CRL based on the certificate database and should only be used as required to regenerate a CRL based on the certificate database contents.

Examples

The following example forces the issuance of a CRL by the local CA server:

```
ciscoasa
(config-ca-server)
# crypto ca server crl issue
```

A new CRL has been issued.

```
ciscoasa
```

```
(config-ca-server)
#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point to be included in the certificates issued by the CA.
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
show crypto ca server crl	Displays the current CRL of the local CA.

crypto ca server revoke

To mark a certificate issued by the local Certificate Authority (CA) server as revoked in the certificate database and the CRL, use the **crypto ca server revoke** command in privileged EXEC mode.

crypto ca server revoke *cert-serial-no*

Syntax Description

cert-serial-no	Specifies the serial number of the certificate to be revoked, which must be in hexadecimal format.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You revoke a specific certificate that has been issued by the local CA on an ASA by entering the **crypto ca server revoke** command on that ASA. Revocation is accomplished when this command marks the certificate as revoked in the certificate database on the CA server and in the CRL. You specify the certificate to be revoked by entering the certificate serial number in hexadecimal format.

The CRL is regenerated automatically after the specified certificate is revoked.

Examples

The following example revokes the certificate with the serial number 782ea09f issued by the local CA server:

```
ciscoasa
(config-ca-server)#
# crypto ca server revoke 782ea09f
```

Certificate with the serial number 0x782ea09f has been revoked. A new CRL has been issued.

```
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server unrevoke	Unrevokes a revoked certificate issued by the local CA server.
crypto ca server user-db remove	Removes a user from the CA server user database.
show crypto ca server crl	Displays the current CRL of the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server unrevoke

To unrevoke a revoked certificate issued by the local CA server, use the **crypto ca server unrevoke** command in privileged EXEC mode.

crypto ca server unrevoke *cert-serial-no*

Syntax Description

cert-serial-no	Specifies the serial number of the certificate to be unrevoked, which must be in hexadecimal format.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You unrevoke a revoked certificate issued by the local CA on an ASA by entering the **crypto ca server unrevoke** command. The validity of the certificate is restored when this command marks the certificate as valid in the certificate database and removes it from the CRL. You specify the certificate to be unrevoked by entering the certificate serial number in hexadecimal format.

The CRL is regenerated after the specified certificate is unrevoked.

Examples

The following example unrevokes the certificate with the serial number 782ea09f issued by the local CA server:

```
ciscoasa
(config-ca-server)
# crypto ca server unrevoke 782ea09f
```

Certificate with the serial number 0x782ea09f has been unrevoked. A new CRL has been issued.

```
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
crypto ca server user-db add	Adds a user to the CA server user database.
show crypto ca server cert-db	Displays local CA server certificates.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server user-db add

To insert a new user into the CA server user database, use the **crypto ca server user-db add** command in privileged EXEC mode.

crypto ca server user-db *user* [**dn** *dn*] [**email** *e-mail-address*]

Syntax Description

dn *dn*	Specifies a subject-name distinguished name for certificates issued to the added user. If a DN string contains spaces, enclose value with double quotes. You can only use commas to separate DN attributes (for example, “OU=Service, O=Company, Inc.”).
email *e-mail-address*	Specifies the e-mail address for the new user.
user	Specifies a single user to whom to grant enrollment privileges. The username can be a simple username or an e-mail address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The *user argument* can be a simple username such as user1 or an e-mail address such as user1@example.com. The *username* must match the username specified by the end user in the enrollment page.

The *username* is added to the database as a user without privileges. You must use the **crypto ca server allow** command to grant enrollment privileges.

The *username* argument, along with the one-time password, is used to enroll the user on the enrollment interface page.

Note For e-mail notification of the one-time password (OTP), an e-mail address should be specified either in the *username* or *email-address* argument. A missing e-mail address at mailing time generates an error.

The **email** *e-mail-address* keyword-argument pair is used only as an e-mail address to notify the user for enrollment and renewal reminders and does not appear in the issued certificate.

Inclusion of the e-mail address ensures that the user can be contacted with any questions and is notified of the required one-time password for enrollment.

If an optional DN is not specified for a user, the subject name DN is formed using the *username* and the subject-name-default DN setting as cn=*username* , subject-name-default.

Examples

The following example adds a user to the user database with a username of user1@example.com with a complete subject-name DN:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db add dn "cn=Jane Doe, ou=engineering, o=Example, l=RTP, st=NC,
c=US"
```

ciscoasa (config-ca-server) #

The following example grants enrollment privileges to the user named user2.

```
ciscoasa
(config-ca-server)
# crypto ca server user-db allow user2
```

ciscoasa (config-ca-server)

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage a local CA.
crypto ca server user-db allow	Permits a specific user or a subset of users in the CA server database to enroll with the CA.
crypto ca server user-db remove	Deletes a user from the CA server database.
crypto ca server user-db write	Copies the user information in the CA server database to the file specified by the **database path** command.
database path	Specifies a path or location for the local CA database. The default location is flash memory.

crypto ca server user-db allow

To permit a user or a group of users to enroll in the local CA server database, use the **crypto ca server user-db allow** command in privileged EXEC mode. This command also includes options to generate and display one-time passwords or to e-mail them to users.

crypto ca server user-db allow { *username* | **all-unenrolled** | **all-certholders** } [**display-otp**] [**email-otp**] [**replace-otp**]

Syntax Description

all-certholders	Specifies that enrollment privileges be granted to all users in the database who have been issued a certificate, whether the certificate is valid or not. This is equivalent to granting renewal privileges.
all-unenrolled	Specifies that enrollment privileges be granted to all users in the database who have not been issued a certificate.
email-otp	(Optional) Sends the specified users one-time passwords by e-mail to their configured e-mail addresses.
replace-otp	(Optional) Specifies that one-time passwords be regenerated for all specified users who originally had valid one-time passwords.
display-otp	(Optional) Displays the one-time passwords for all specified users on the console.
username	Specifies a single user to whom to grant enrollment privileges. The username can be a simple username or e-mail address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Release	Modification
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **replace-otp** keyword generates OTPs for all specified users. These new OTPs replace any valid ones generated for the specified users.

The OTP is not stored on the ASA, but is generated and regenerated as required to notify a user or to authenticate a user during enrollment.

Examples

The following example grants enrollment privileges to all users in the database who have not enrolled yet:

```
ciscoasa
(config-ca-server)#
 crypto ca server user-db allow all-unenrolled
ciscoasa
(config-ca-server)#
```

The following example grants enrollment privileges to the user named user1:

```
ciscoasa
(config-ca-server)#
 crypto ca server user-db allow user1
ciscoasa
(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage a local CA.
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db write	Copies the user information in the CA server database to the file specified by the **database path** command.
enrollment-retrieval	Specifies the time in hours that an enrolled user can retrieve a PKCS12 enrollment file.
show crypto ca server cert-db	Displays all certificates issued by the local CA.

crypto ca server user-db email-otp

To e-mail the OTP to a specific user or a subset of users in the local CA server database, use the **crypto ca server user-db email-otp** command in privileged EXEC mode.

crypto ca server user-db email-otp { *username* | **all-unenrolled** | **all-certholders** }

Syntax Description

all-certholders	Specifies that OTPs are e-mailed to all users in the database who have been issued a certificate, whether that certificate is valid or not.
all-unenrolled	Specifies that the OTPs are e-mailed to all users in the database who have never been issued a certificate, or who only hold expired or revoked certificate(s).
username	Specifies that the OTP for a single user is e-mailed to that user. The username can be a username or an e-mail address.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example e-mails the OTP to all unenrolled users in the database:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db email-otp all-unenrolled
ciscoasa
(config-ca-server)
#
```

The following example e-mails the OTP to the user named user1:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db email-otp user1
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server user-db show-otp	Displays the one-time password for a specific user or a subset of users in the CA server database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server user-db remove

To remove a user from the local CA server user database, use the **crypto ca server user-db remove** command in privileged EXEC mode.

crypto ca server user-db remove *username*

Syntax Description

username	Specifies the name of the user to remove in the form of a username or an e-mail address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command removes a username from the CA user database so that user cannot enroll. The command also provides the option to revoke previously issued, valid certificates.

Examples

The following example removes a user with a username, user1, from the CA server user database :

```
ciscoasa
(config-ca-server)
# crypto ca server user-db remove user1
WARNING: No certificates have been automatically revoked. Certificates issued to user user1
 should be revoked if necessary.
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
show crypto ca server user-db	Displays users included in the CA server user database.
crypto ca server user-db write	Writes the user information configured in the local CA database to the file specified by the **database path** command.

crypto ca server user-db show-otp

To display the OTP for a specific user or a subset of users in the local CA server database, use the **crypto ca server user-db show-otp** command in privileged EXEC mode.

crypto ca server user-db show-otp { *username* | **all-certholders** | **all-unenrolled** }

Syntax Description

all-certholders	Displays the OTPs for all users in the database who have been issued a certificate, whether the certificate is currently valid or not.
all-unenrolled	Displays the OTPs for all users in the database who have never been issued a certificate, or who only hold expired or revoked certificate(s).
username	Specifies that the OTP for a single user be displayed. The *username* can be a username or an e-mail address.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example displays the OTP for all users who have valid or invalid certificates in the database:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db show-otp all-certholders
ciscoasa
```

```
(config-ca-server)
#
```

The following example displays the OTP for the user named user1:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db show-otp user1
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db allow	Allows a specific user or a subset of users in the CA server database to enroll with the local CA.
crypto ca server user-db email-otp	E-mails the one-time password to a specific user or to a subset of users in the CA server database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.

crypto ca server user-db write

To configure a directory location to store all the local CA database files, use the **crypto ca server user-db write** command in privileged EXEC mode.

crypto ca server user-db write

Syntax Description

This command has no keywords or arguments.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global Configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **crypto ca server user-db write** command is used to save new user-based configuration data to the storage specified by the database path configuration. The information is generated when new users are added or allowed with the **crypto ca server user-db add** and **crypto ca server user-db allow** commands.

Examples

The following example writes the user information configured in the local CA database to storage:

```
ciscoasa
(config-ca-server)
# crypto ca server user-db write
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
database path	Specifies a path or location for the local CA database. The default location is flash memory.
crypto ca server user-db remove	Removes a user from the CA server user database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca trustpoint

To configure CA to a trustpoint, enter the crypto ca trustpoint configuration mode for the specified trustpoint using the **crypto ca trustpoint** command in global configuration mode. To remove the specified trustpoint, use the **no** form of this command.

crypto ca trustpoint *trustpoint-name*
no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

Syntax Description

noconfirm	Suppresses all interactive prompting
trustpoint-name	Identifies the name of the trustpoint to manage. The maximum name length allowed is 128 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	Added options to support the OCSP. These include **match certificate map**, **ocsp disable-nonce**, **ocsp url**, and **revocation-check**.
8.0(2)	Added options to support certificate validation. These include **id-usage** and **validation-policy. The following are being deprecated: accept-subordinates, id-cert-issuer, and support-user-cert-validation.**
8.0(4)	The **enrollment self** option was added to support enrollment of self-signed certificates between trusted enterprises, such as between phone proxy and TLS proxy.
9.13(1)	The **crl required | optional | nocheck** option was removed. The **match certificate** option was modified to include **override CDP** configuration
9.20(1)	The **alt-fqdn** option was added.
9.22(3), 9.23(1)	Support to enroll ACME CA was added.

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA. Issuing this command puts you in crypto ca trustpoint configuration mode.

This command manages trustpoint information. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint mode control CA-specific configuration parameters, which specify how the ASA obtains the CA certificate, how the ASA obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

You can specify characteristics for the trustpoint using the following commands:

- **accept-subordinates**—Deprecated. Indicates whether CA certificates subordinate to the CA associated with the trustpoint are accepted if delivered during phase one IKE exchange when not previously installed on the ASA.
- **alt-fqdn** *fqdn*—During enrollment, asks the CA to include the specified FQDN values in the subject alternative name extension of the certificate or requests.
- **auto-enroll**—Configures the parameters that control if CMPv2 auto update is used, when it is triggered, and if a new keypair is generated. Enter a percentage of the absolute lifetime of the certificate after which auto-enroll will be necessary. Then specify if you want to generate a new key while renewing the certificate: **[no] auto-enroll [<percent>] [regenerate]**
- **crl required | optional | nocheck**—Specifies CRL configuration options. Removed in ASA 9.13(1).
- **crl configure**—Enters crl configuration mode (see the **crl** command).
- **default enrollment**—Returns all enrollment parameters to their system default values. Invocations of this command do not become part of the active configuration.
- **email** *address*—During enrollment, asks the CA to include the specified email address in the subject alternative name extension of the certificate.
- **enrollment protocol acme|cmp|est|scep** *url*—Specifies ACME, CMP, EST, or SCEP enrollment to enroll with this trustpoint and configures the enrollment URL (*url*).
- **enrollment retry period** —Specifies a retry period in minutes for SCEP enrollment.
- **enrollment retry count**—Specifies a maximum number of permitted retries for SCEP enrollment.
- **enrollment terminal**—Specifies cut and paste enrollment with this trustpoint.
- **enrollment self**—Specifies enrollment that generates a self-signed certificate.
- **enrollment url**—Specifies the SCEP enrollment to enroll with this trustpoint and configures the enrollment URL (*url*).
- **exit**—Leaves the configuration mode.
- **fqdn** *fqdn*—During enrollment, asks the CA to include the specified FQDN in the subject alternative name extension of the certificate.
- **id-cert-issuer**—Deprecated. Indicates whether the system accepts peer certificates issued by the CA associated with this trustpoint.
- **id-usage**— Specifies how the enrolled identity of a trustpoint can be used.
- **ip-addr** *ip-address*—During enrollment, asks the CA to include the IP address of the ASA in the certificate.

- **keypair** *name*—Specifies the key pair whose public key is to be certified.
- **keypair** *name*—Specifies the keypair, as either RSA or EDCSA ,whose public key is to be certified and their modulus bits or elliptic curve bits.
- **match certificate** *map-name* **override ocsp | override cdp**—Matches a certificate map to an OCSP override or CDP override rule.
- **ocsp disable-nonce**—Disables the nonce extension, which cryptographically binds revocation requests with responses to avoid replay attacks.
- **ocsp url**—Specifies that the OCSP server at this URL check all certificates associated with this trustpoint for revocation status.
- **exit**—Leaves the configuration mode.
- **password** *string*—Specifies a challenge phrase that is registered with the CA during enrollment. The CA typically uses this phrase to authenticate a subsequent revocation request.
- **revocation check**—Specifies the revocation checking method, which includes CRL, OCSP, and none.
- **serial-number**—During enrollment, asks the CA to include the ASA serial number in the certificate.
- **subject-name** *X.500 name*—During enrollment, asks the CA to include the specified subject DN in the certificate. If a DN string includes a comma, enclose the value string with double quotes (for example, O=”Company, Inc.”)
- **support-user-cert-validation**—Deprecated. If enabled, the configuration settings to validate a remote user certificate can be taken from this trustpoint, provided that it is authenticated to the CA that issued the remote certificate. This option applies to the configuration data associated with the subcommands **crl required | optional | nocheck** and all settings in the CRL mode.
- **validation-policy**—Specifies trustpoint conditions for validating certificates associated with user connections.

Note When you try to connect, a warning occurs to indicate that the trustpoint does not contain an ID certificate when an attempt is made to retrieve the ID certificate from the trustpoint.

Examples

The following example enters ca trustpoint configuration mode for managing a trustpoint named central:

```
ciscoasa(config)# crypto ca trustpoint
central
ciscoasa(ca-trustpoint)#
```

Examples

The following example shows the enrollment process for ACME CA certification:

```
ciscoasa(config)# crypto ca trustpoint my_acme_tp
ciscoasa(config-ca-trustpoint)# enrollment protocol ?
crypto-ca-trustpoint mode commands/options:
  acme  Automatic Certificate Management Environment
  cmp   Certificate Management Protocol Version 2
```

```
  est   Enrollment over Secure Transport
  scep  Simple Certificate Enrollment Protocol
ciscoasa(config-ca-trustpoint)# enrollment protocol acme ?
crypto-ca-trustpoint mode commands/options:
  authentication  ACME authentication method
  url             CA server enrollment URL

ciscoasa(config-ca-trustpoint)# enrollment protocol acme authentication ?
crypto-ca-trustpoint mode commands/options:
  http01  Use the HTTP-01 method, which opens port 80 on the specified interface
ciscoasa(config-ca-trustpoint)# enrollment protocol acme authentication http01 <inf-name>
ciscoasa(config-ca-trustpoint)# enrollment protocol acme url ?
crypto-ca-trustpoint mode commands/options:
  LINE < 477 char  URL
  LetsEncrypt      Use the Let's Encrypt CA
```



Note When you configure with LetsEncrypt, the URL is automatically generated. You can view the URL using the **show crypto ca certificates** command.

The following is an example of configuring the CA URL and its parameters when you have not chosen LetsEncrypt.

```
ciscoasa(config-ca-trustpoint)#  enrollment protocol acme url
https://mytest.com:8443/acme/acme/directory
ciscoasa(config-ca-trustpoint)#  subject-name cn=mytest-asa.com
ciscoasa(config-ca-trustpoint)#  fqdn mytest-asa.com
ciscoasa(config-ca-trustpoint)#  no serial-number
ciscoasa(config-ca-trustpoint)#  keypair rsa modulus 2048
ciscoasa(config-ca-trustpoint)#  auto-enroll 90 regenerate
ciscoasa(config-ca-trustpoint)#  exit
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca certificate map	Enters crypto ca certificate map configuration mode. Defines certificate-based ACLs.
crypto ca crl request	Requests a CRL based on configuration parameters of a specified trustpoint.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request.

crypto ca trustpool export

To export the certificates that constitute the PKI trustpool, use the crypto ca trustpool export command in privileged EXEC configuration mode.

crypto ca trustpool export *filename*

Syntax Description

filename	The file in which to store the exported trustpool certificates.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command copies the entire contents of the active trustpool to the indicated filepath in pem-coded format.

Examples

```
ciscoasa# crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
ciscoasa#
ciscoasa# more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

Related Commands

Command	Description
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.

crypto ca trustpool import

To import the certificates that constitute the PKI trustpool, use the crypto ca trustpool import command in global configuration mode.

crypto ca trustpool import [**clean**] **url** *url* [**noconfirm** [**signature-required**]]

Syntax Description

clean	Removes all downloaded trustpool certificates prior to import.
noconfirm	Suppresses all interactive prompts.
signature-required	Indicates that only signed files are accepted.
url	The location of the trustpool file to be imported.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.
9.12(1)	The option to use the ASA's default trusted CA list was removed.

Usage Guidelines

This command provides the ability to validate the signature on the file when a trustpool bundle is downloaded from cisco.com. A valid signature is not mandatory when downloading bundles from other sources or in a format that does not support signatures. Users are informed of the signature status and are given the option to accept the bundle or not.

The possible interactive warnings are:

- Cisco bundle format with invalid signature
- Non-cisco bundle format
- Cisco bundle format with valid signature

The **signature-required** keyword is allowed only if the **noconfirm** option is selected. If the **signature-required** keyword is included but the signature is not present or cannot be verified, the import fails.



Note Unless you have verified the legitimacy of the file through some other means, do not install the certificates if a file signature cannot be verified,

The following example shows the behavior of the **crypto ca trustpool** import command when suppressing interactive prompting and requiring signatures:

ciscoasa(config)# **crypto ca trustpool import url ?**

configure mode commands/options:disk0: Import from disk0: file systemdisk1: Import from disk1: file systemflash: Import from flash: file systemftp: Import from ftp: file systemhttp: Import from http: file systemhttps: Import from https: file systemsmb: Import from smb: file systemsystem: Import from system: file systemtftp: Import from tftp: file system

ciscoasa(config)# **crypto ca trustpool import url http://mycompany.com ?**exec mode commands/options:noconfirm Specify this keyword to suppress all interactive prompting.

ciscoasa(config)# **crypto ca trustpool import url http://mycompany.com noconfirm ?**exec mode commands/options:signature-required Indicate that only signed files will be accepted

Related Commands

Command	Description
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.

crypto ca trustpool policy

To enter a submode that provides the commands that define the trustpool policy, use the crypto ca trustpool policy command in global configuration mode. To set up the automatic import of a trustpool certificate bundle, specify the URL which the ASA uses to download and import the bundle.

crypto ca trustpool policy

Syntax Description

This command has no arguments or keywords.

auto-import	Configure automatic import of trustpool certificates
auto-import [time <H:M:S>] [url <URL address>]	Set custom time and custom URL for downloading certificates in trustpool if you need to schedule this download during off peak hours or any other convenient times.
auto-import time	Specify the download time in hours, minutes, and seconds. An attempt is made for every 24 hours at this specified time. If not provided, the default time of 22:00 hours is used.
auto-import url	Specify automatic import of trustpool certificates. If not provided, the default Cisco URL is used.

Command Default

No default behavior or values.

The automatic import option is turned off by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Object Configuration	• Yes	—	—	—	—

Command History

Release	Modification
9.0(1)	This command was added.
9.5(2)	The auto-import command option was added.

Examples

ciscoasa(config)# **crypto ca trustpool ?**

configure mode commands/options: policy Define trustpool policy

ciscoasa(config)# **crypto ca trustpool policy**ciscoasa(config-ca-trustpool)# **?**

CA Trustpool configuration commands:crl CRL optionsexit Exit from certificate authority trustpool entry modematch Match a certificate mapno Negate a command or set its defaultsrevocation-check Revocation checking options

auto-import Configure automatic import of trustpool certificatesciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import?

crypto-ca-trustpool mode commands/options:

time Specify the auto import time in hours, minutes, and secondsDefault is 22:00:00. An attempt is made every 24 hours at the specified time.url Specify the HTTP based URL address for automatic import of trustpool certificates

<cr>

ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import url ?

crypto-ca-trustpool mode commands/options:LINE URL for automatic importciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import time ?H:M:S Specify the auto import time in hours, minutes & seconds. E.g. 18:00:00 (attempt to import is made at every 24 hours at 6PM)ciscoasa(config-ca-trustpool)#

Related Commands

Command	Description
show crypto ca trustpool policy	Displays the configured trustpool policy.

crypto ca trustpool remove

To remove a single specified certificate from the PKI trustpool, use the crypto ca trustpool remove command in privileged EXEC configuration mode.

crypto ca trustpool remove *cert fingerprint* [**noconfirm**]

Syntax Description

cert fingerprint	Hex data.
noconfirm	Specify this keyword to suppress all interactive prompting.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Because this command will commit a change to the trusted root certificate content, interactive users will be prompted to confirm their actions.

Examples

```
ciscoasa# crypto ca trustpool remove ?
  Hex-data  Certificate fingerprint
ciscoasa# crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0 ?
noconfirm  Specify this keyword to suppress all interactive prompting.
```

Related Commands

Command	Description
clear crypto ca trustpool	Removes all certificates from the trustpool.
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.

crypto dynamic-map match address

To match the address of an access list for the dynamic crypto map entry, use the crypto dynamic-map match address command in global configuration mode. To disable the address match, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*
no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

Syntax Description

acl-name	Identifies the access list to be matched for the dynamic crypto map entry.
dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

For a dynamic crypto map (with the crypto dynamic-map command), the access-list command is not required but is strongly recommended.

Use the access-list command to define the access lists. The access list hit counts only increase when the tunnel initiates. After the tunnel is up, the hit counts do not increase on a per-packet flow. If the tunnel drops and then reinitiates, the hit count will increase.

The ASA uses the access lists to differentiate the traffic to protect with IPsec crypto from the traffic that does not need protection. It protects outbound packets that match a permit ACE, and ensures that inbound packets that match a permit ACE have protection.

See the crypto map match address command for additional information about this command.

Examples

The following example shows the use of the **crypto dynamic-map** command to match address of an access list named aclist1:

```
ciscoasa(config)# crypto dynamic-map mymap 10 match address aclist1
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set df-bit

To set the per-signature algorithm (SA) do-not-fragment (DF) policy, use the **crypto dynamic-map set df-bit** command in global configuration mode. To disable the DF policy, use the **no** form of this command.

crypto dynamic-map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]
no crypto dynamic-map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

Syntax Description

name	Specifies the name of the crypto dynamic map set.
priority	Specifies the priority that you assign to the crypto dynamic map entry.

Command Default

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The original DF policy command is retained and acts as a global policy setting on an interface, but it is superseded for an SA by the **crypto map** command.

crypto dynamic-map set ikev1 transform-set

To specify the IKEv1 transform sets to use in a dynamic crypto map entry, use the **crypto dynamic-map set ikev1 transform-set** command in global configuration mode.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*...transform-set-name11*]

To remove the transform sets from the dynamic crypto map entry, specify the transform set name in the **no** form of this command:

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*...transform-set-name11*]

To remove the dynamic crypto map entry, use the no form of the command and specify all or none of the transform sets:

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set**

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.
transform-set-name1 *transform-set-name11*	Specifies one or more names of the transform sets. Any transform sets named in this command must be defined in the **crypto ipsec ikev1 transform-set** command. Each crypto map entry supports up to 11 transform sets.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0	This command was added.
7.2(1)	Changed the maximum number of transform sets in a crypto map entry.
8.4(1)	Added the ikev1 keyword.

Release	Modification
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A dynamic crypto map is a crypto map without all of the parameters configured. It acts as a policy template where the missing parameters are later dynamically learned, as the result of an IPsec negotiation, to match the peer requirements. The ASA applies a dynamic crypto map to let a peer negotiate a tunnel if its IP address is not already identified in a previous static or dynamic crypto map. This occurs with the following types of peers:

- Peers with dynamically assigned public IP addresses.

Both LAN-to-LAN and remote access peers can use DHCP to obtain a public IP address. The ASA uses this address only to initiate the tunnel.

- Peers with dynamically assigned private IP addresses.

Peers requesting remote access tunnels typically have private IP addresses assigned by the headend. Generally, LAN-to-LAN tunnels have a predetermined set of private networks that are used to configure static maps and therefore used to establish IPsec SAs.

As an administrator configuring static crypto maps, you might not know the IP addresses that are dynamically assigned (via DHCP or some other method), and you might not know the private IP addresses of other clients, regardless of how they were assigned. VPN clients typically do not have static IP addresses; they require a dynamic crypto map to allow IPsec negotiation to occur. For example, the headend assigns the IP address to a Cisco VPN client during IKE negotiation, which the client then uses to negotiate IPsec SAs.

Dynamic crypto maps can ease IPsec configuration and we recommend them for use in networks where the peers are not always predetermined. Use dynamic crypto maps for Cisco VPN clients (such as mobile users) and routers that obtain dynamically assigned IP addresses.

Tip Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If the traffic covered by such a **permit** entry could include multicast or broadcast traffic, insert **deny** entries for the appropriate address range into the access list. Remember to insert **deny** entries for network and subnet broadcast traffic, and for any other traffic that IPsec should not protect.

Dynamic crypto maps work only to negotiate SAs with remote peers that initiate the connection. The ASA cannot use dynamic crypto maps to initiate connections to a remote peer. With a dynamic crypto map configured, if the outbound traffic matches a permit entry in an access list and the corresponding SA does not yet exist, the ASA drops the traffic.

A crypto map set may include a dynamic crypto map. Dynamic crypto map sets should be the lowest priority crypto maps in the crypto map set (that is, they should have the highest sequence numbers) so that the ASA evaluates other crypto maps first. It examines the dynamic crypto map set only when the other (static) map entries do not match.

Similar to static crypto map sets, a dynamic crypto map set consists of all of the dynamic crypto maps with the same dynamic map name. The dynamic sequence number differentiates the dynamic crypto maps in a set. If you configure a dynamic crypto map, insert a permit ACL to identify the data flow of the IPsec peer for the crypto access list. Otherwise the ASA accepts any data flow identity the peer proposes.

Caution Do not assign static (default) routes for traffic to be tunneled to a ASA interface configured with a dynamic crypto map set. To identify the traffic that should be tunneled, add the ACLs to the dynamic crypto map. Use care to identify the proper address pools when configuring the ACLs associated with remote access tunnels. Use Reverse Route Injection to install routes only after the tunnel is up.

You can combine static and dynamic map entries within a single crypto map set.

Examples

The following example creates a dynamic crypto map entry named “dynamic0” consisting of the same ten transform sets.

```
ciscoasa(config)# crypto dynamic-map dynamic0 1 set
ikev1
transform-set 3des-md5 3des-sha 56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5
192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec **ikev1** transform-set	Configures an IKEv1 transform set.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto dynamic-map set ikev2 ipsec-proposal

To specify the IPsec proposals for IKEv2 to use in a dynamic crypto map entry, use the **crypto dynamic-map set ikev2 ipsec-proposal** command in global configuration mode. To remove the names of the transform sets from a dynamic crypto map entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name 1* [*...transform-set-name11*]
no crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name 1* [*...transform-set-name11*]

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
transform-set-name1 *transform-set-name11*	Specifies one or more names of the transform sets. Any transform sets named in this command must be defined in the **crypto ipsec ikev2 transform-set** command. Each crypto map entry supports up to 11 transform sets.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

crypto dynamic-map set nat-t-disable

To disable NAT-T for connections based on this crypto map entry, use the **crypto dynamic-map set nat-t-disable** command in global configuration mode. To enable NAT-T for this crypto may entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**
no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

Syntax Description

dynamic-map-name	Specifies the name of the crypto dynamic map set.
dynamic-seq-num	Specifies the number that you assign to the crypto dynamic map entry.

Command Default

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **isakmp nat-traversal** command to globally enable NAT-T. Then you can use the **crypto dynamic-map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command disables NAT-T for the crypto dynamic map named mymap:

```
ciscoasa(config)# crypto dynamic-map mymap 10 set nat-t-disable
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set peer

See the crypto map set peer command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*
no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.
hostname	Identifies the peer in the dynamic crypto map entry by hostname, as defined by the **name** command.
ip_address	Identifies the peer in the dynamic crypto map entry by IP address, as defined by the **name** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example shows setting a peer for a dynamic-map named mymap to the IP address 10.0.0.1:

```
ciscoasa(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set pfs

To set IPsec to ask for PFS when requesting new security associations for this dynamic crypto map entry or that IPsec requires PFS when receiving requests for new security associations, use the **crypto dynamic-map set pfs** command in global configuration mode. To specify that IPsec should not request PFS, use the **no** form of this command.

crypto dynamic-map *map-name map-index* **set pfs** [**group1** | **group2** | **group5** | **group14** | **group19** | **group20** | **group21** | **group24**]
no crypto dynamic-map *map-name map-index* **set pfs** [**group1** | **group2** | **group5** | **group14** | **group19** | **group20** | **group21** | **group24**]

Syntax Description

group14	Specifies which Diffie-Hellman key exchange group to use.
group15	Specifies which Diffie-Hellman key exchange group to use.
group16	Specifies which Diffie-Hellman key exchange group to use.
group19	Specifies which Diffie-Hellman key exchange group to use.
group20	Specifies which Diffie-Hellman key exchange group to use.
group21	Specifies which Diffie-Hellman key exchange group to use.
group24	Specifies which Diffie-Hellman key exchange group to use.
map-name	Specifies the name of the crypto map set.
map-index	Specifies the number you assign to the crypto map entry.

Command Default

By default, PFS is not set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to add Diffie-Hellman group 7.
8.0(4)	The group 7 command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.

Release	Modification
9.0(1)	Support for multiple context mode was added.
9.12(1)	Support was removed for DH group 1. The **group 1** commands was deprecated.
9.13(1)	Support for group14, 15, and 16 command option was added. The **group 2** and **group 5** commands were deprecated and will be removed in later releases.
9.15(1)	Support for **group 1, 2, 5** and **24** command options is removed in this release.

With PFS, every time a new security association is negotiated, a new Diffie-Hellman exchange occurs, which requires additional processing time. PFS adds another level of security because if one key is ever cracked by an attacker, only the data sent with that key is compromised.

The **crypto dynamic-map** commands, such as **match address**, **set peer**, and **set pfs** are described with the crypto map commands. If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, the ASA assumes a default of group2. If the local configuration does not specify PFS, it accepts any offer of PFS from the peer.

When interacting with the Cisco VPN Client, the ASA does not use the PFS value, but instead uses the value negotiated during Phase 1.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto dynamic-map mymap 10. The group specified is group 2:

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2
The following example specifies support for group14:
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs groyp14
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2 (DEPRECATED)
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set reverse route

See the crypto map set reverse-route command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**
no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

Syntax Description

dynamic-map-name	Specifies the name of the crypto map set.
dynamic-seq-num	Specifies the number you assign to the crypto map entry.

Command Default

The default value for this command is off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following command enables Reverse Route Injection for the crypto dynamic map named mymap:

```
ciscoasa(config)# crypto dynamic-map mymap 10 set reverse route
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set security-association lifetime

To override (for a particular dynamic crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations, use the **crypto dynamic-map set security-association lifetime** command in global configuration mode. To reset a dynamic crypto map entry's lifetime value to the global value, use the **no** form of this command.

crypto dynamic-map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }
no crypto dynamic-map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }

Syntax Description

kilobytes {*number* | **unlimited**}	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes. The global default is 4,608,000 kilobytes. This setting does not apply to remote access VPN connections. It applies to site-to-site VPN only.
map-name	Specifies the name of the crypto map set.
seconds *number*	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The global default is 28,800 seconds (eight hours). This setting applies to both remote access and site-to-site VPN.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.1(2)	Added **unlimited** argument.

Usage Guidelines

The dynamic crypto map's security associations are negotiated according to the global lifetimes.

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the ASA requests new security associations during security association negotiation, it specifies its crypto map lifetime values in the request to the peer; it uses these values as the lifetime of the new security associations. When the ASA receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

For site-to-site VPN connections, there are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached. For remote access VPN sessions, only the timed lifetime applies.



Note The ASA lets you change crypto map, dynamic map, and IPsec settings on-the-fly. If you do so, the ASA brings down only the connections affected by the change. If you change an existing access list associated with a crypto map, specifically by deleting an entry within the access list, the result is that only the associated connection is brought down. Connections based on other entries in the access list are not affected.

To change the timed lifetime, use the **crypto dynamic-map set security-association lifetime seconds** command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

Examples

The following command, entered in global configuration mode, specifies a security association lifetime in seconds and kilobytes for the dynamic crypto dynamic map mymap:

```
ciscoasa(config)# crypto
 dynamic-map mymap 10 set security-association
lifetime seconds 1400 kilobytes 3000000
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all crypto dynamic maps.
show running-config crypto dynamic-map	Displays the crypto dynamic map configuration.

crypto dynamic-map set tfc-packets

To enable dummy Traffic Flow Confidentiality (TFC) packets on an IPsec SA, use the **crypto dynamic-map set tfc-packets** command in global configuration mode. To disable TFC packets on an IPsec SA, use the **no** form of this command.

crypto dynamic-map *name priority* **set tfc-packets** [**burst length** | **auto**] [**payload-size bytes** | **auto**] [**timeout second** | **auto**]
no crypto dynamic-map *name priority* **set tfc-packets** [**burst length** | **auto**] [**payload-size bytes** | **auto**] [**timeout second** | **auto**]

Syntax Description

name	Specifies the name of the crypto map set.
priority	Specifies the priority that you assign to the crypto map entry.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command configures the existing DF policy (at an SA level) for the crypto map.

crypto dynamic-map set validate-icmp-errors

To specify whether to validate incoming ICMP error messages, received through an IPsec tunnel, that are destined for an interior host on the private network, use the **crypto dynamic-map set validate-icmp-errors** command in global configuration mode. To remove validation of incoming ICMP error messages from a crypto dynamic map entry, use the **no** form of this command.

crypto dynamic-map *name priority* **set validate-icmp-errors**
no crypto dynamic-map *name priority* **set validate-icmp-errors**

Syntax Description

name	Specifies the name of the crypto dynamic map set.
priority	Specifies the priority that you assign to the crypto dynamic map entry.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This crypto map command is valid only for validating incoming ICMP error messages.

crypto engine accelerator-bias

To change the allocation of the cryptographic cores on Symmetric Multi-Processing (SMP) platforms, use the **crypto engine accelerator-bias** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]
no crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

Syntax Description

balanced	Equally distributes cryptographic hardware resources (Admin/SSL and IPsec cores)
ipsec	Allocates cryptographic hardware resources to favor IPsec cores (includes SRTP encrypted voice traffic). This is the default bias on ASA 5500-X series devices.
ssl	Allocates cryptographic hardware resources to favor Admin/SSL cores. Use this bias when you support SSL-based Secure Client remote access VPN sessions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Cryptographic core rebalancing is available on the following platforms: ASA 5585, 5580, 5545/5555, ASASM, FP4110, FP4120, FP4140, FP4150, FP9300, SM-24, SM-36, and SM-44.

This command causes traffic disruption to services that require crypto operations. You must apply it in a maintenance window and without IPsec failure being configured.

Examples

The following examples show the options available for configuring the crypto engine acccelerator-bias command:

```
ciscoasa (config)# crypto engine accelerator-bias ssl
```

crypto engine large-mod-accel

To switch large modulus operations on an ASA 5510, 5520, 5540, or 5550 from software to hardware, use the **crypto engine large-mod-accel** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

crypto engine large-mod-accel
no crypto engine large-mod-accel

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA performs large modulus operations in the software.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command is available only with the ASA models 5510, 5520, 5540, and 5550. It switches large modulus operations from software to hardware. The switch to hardware accelerates the following:

- 2048-bit RSA public key certificate processing.
- Diffie Hellman Group 5 (DH5) key generation.

We recommend that you use this command when necessary to improve the connections per second. Depending on the load, it might have a limited performance impact on SSL throughput.

We also recommend that you use either form of this command during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware or hardware to software.

Note The ASA 5580/5500-X platforms already integrate this capability to switch large modulus operations; therefore, **crypto engine** commands are not applicable on these platforms.

Examples

The following example switches large modulus operations from software to hardware:

```
ciscoasa(config)# crypto engine large-mod-accel
```

The following example removes the previous command from the configuration and switches large modulus operations back to software:

```
ciscoasa(config)# no crypto engine large-mod-accel
```

Related Commands

Command	Description
show running-config crypto engine	Shows if large modulus operations are switched to hardware.
clear configure crypto engine	Returns large modulus operations to software. This command is equivalent to the **no crypto engine large-mod-accel** command.

crypto ikev1 enable

To enable ISAKMP IKEv1 negotiation on the interface on which the IPsec peer communicates with the ASA, use the **crypto ikev1 enable** command in global configuration mode. To disable ISAKMP IKEv1 on the interface, use the **no** form of this command.

crypto ikev1 enable *interface-name*
no crypto ikev1 enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP IKEv1 negotiation.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This **isakmp enable** command was added.
7.2(1)	The **crypto isakmp enable** command replaced the **isakmp enable** command.
8.4(1)	With the addition of IKEv2 capability, the crypto isakmp enable command was changed to the crypto ikev1 enable command.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
ciscoasa(config)# no crypto isakmp enable
 inside
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.

Command	Description
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev1 limit max-in-negotiation-sa

To limit the number of IKEv1 in-negotiation (open) SAs on the ASA, use the **crypto ikev1 limit max-in-negotiation-sa** command in global configuration mode. To disable limits on the number of open SAs, use the **no** form of this command:

crypto ikev1 limit max-in-negotiation-sa *threshold percentage*
no crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

Syntax Description

threshold percentage	The percentage of the total allowed SAs for the ASA that are allowed to be in negotiation (open). After reaching the threshold, additional connections are denied. The range is 1 to 100%. The default is 20% for all ASA platforms except ASA5506/ASA5508 (which is 100%).

Command Default

The default is 20%. The ASA limits the number of open SAs to 20% except ASA5506/ASA5508.

Usage Guidelines

The **crypto ikev1 limit-max-in-negotiation-sa** command limits the maximum number of SAs that can be in negotiation at any time. 1

The **crypto ikev1 limit max in-negotiation-sa** command stops further connections from negotiating to protect current connections and prevent memory and/or CPU attacks that the cookie-challenge feature may be unable to thwart.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Examples

The following example limits the number of IKEv1 connections that are in negotiation to 70 percent of the maximum allowable IKEv1 connections:

```
ciscoasa(config)# crypto ikev1 limit max in-negotiation-sa 70
```

Related Commands

Command	Description
crypto ikev1 limit max-sa	Limits the number of IKEv1 connections on the ASA,

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev1 policy

To create an IKEv1 security association (SA) for IPsec connections, use the crypto ikev2 policy command in global configuration mode. To remove the policy, use the **no** form of this command:

crypto ikev1 policy *priority*
no crypto ikev1 policy *priority*

Syntax Description

priority	The policy suite priority. The range is 1-65535, with 1 being the highest and 65535 the lowest.

Command Default

No default behavior or values.

Usage Guidelines

The command enters IKEv1 policy configuration mode, in which you specify additional IKEv1 SA settings. An IKEv1 SA is a key used in phase 1 to enable IKEv1 peers to communicate securely in phase 2. After entering the crypto ikev1 policy command, you can use additional commands to set the SA encryption algorithm, DH group, integrity algorithm, lifetime, and hash algorithm.

As the 3DES encryption cipher has been deprecated, the default encryption cipher for newly created IKE policies and IPsec proposals will now be AES-128. This applies only to new policies and proposals and will not affect any existing configuration items.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

9.13(1)	• Support for DH groups 14, 15, and 16 was added. The **groups 1, 2** and **group 5** option is considered as insecure. These options were deprecated and will be removed in the later release.
	• Several integrity and PRF ciphers used ASA/Lina IKE, IPsec, and SSH modules are considered as insecure. The following ciphers are deprecated and will be removed in the later release:
	  • HMAC-MD5 integrity and PRF ciphers
	  • HMAC-MD5 integrity ciphers in IPsec
	  • HMAC-MD5, HMAC-MD5-96, and HMAC-SHA1-96 integrity ciphers
	  • AES-GMAC,3DES, DES.

Release	Modification

9.15(1)	• Support for DH groups **groups 1, 2** and **group 5** option is considered as insecure and are removed.
	• The following integrity and PRF ciphers used ASA/Lina IKE, IPsec, and SSH are considered insecure; they are removed from IKEv1 policy configuration:
	  • HMAC-MD5 integrity and PRF ciphers
	  • HMAC-MD5 integrity ciphers in IPsec
	  • HMAC-MD5, HMAC-MD5-96, and HMAC-SHA1-96 integrity ciphers
	  • AES-GMAC,3DES, DES.

Examples

The following example creates the priority 1 IKEv1 SA and enters IKEv1 policy configuration mode:

```
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)# authentication rsa-sig
ciscoasa(config-ikev1-policy)# hash md5
ciscoasa(config-ikev1-policy)# group 14
ciscoasa(config-ikev1-policy)# lifetime 300
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiate packets,
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev2 cookie-challenge

To enable the ASA to send cookie challenges to peer devices in response to SA initiate packets, use the crypto ikev2 cookie-challenge command in global configuration mode. To disable cookie challenges, use the **no** form of this command:

crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**
no crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

Syntax Description

threshold percentage	The percentage of the total allowed SAs for the ASA that are in negotiation, which triggers cookie challenges for any future SA negotiations. The range is zero to 99%. The default is 50%.
always	Always cookie-challenges incoming SAs.
never	Never cookie-challenges incoming SAs.

Command Default

No default behavior or values.

Usage Guidelines

Cookie challenging a peer prevents possible denial-of-service (DoS) attacks. An attacker initiates a DoS attack when the peer device sends an SA initiate packet and the ASA sends its response, but the peer device does not respond further. If the peer device does this continually, all the allowed SA requests on the ASA can be used up until it stops responding.

Enabling a threshold percentage using the crypto ikev2 cookie-challenge command limits the number of open SA negotiations. For example, with the default setting of 50%, when 50% of the allowed SAs are in negotiation (open), the ASA cookie-challenges any additional SA initiate packets that arrive. For the Cisco ASA 5580 with 10000 allowed IKEv2 SAs, after 5000 SAs have become open, any more incoming SAs are cookie-challenged.

If used in conjunction with the **crypto kev2 limit max in-negotiation-sa** command, configure the cookie-challenge threshold lower than the maximum in-negotiation threshold for an effective cross-check.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

In the following example, the cookie-challenge threshold is set to 30%:

```
ciscoasa(config)# crypto ikev2 cookie-challenge 30
```

Related Commands

Command	Description
crypto ikev2 limit max-sa	Limits the number of IKEv2 connections on the ASA,
crypto ikev2 limit max-in-negotiation-sa	Limits the number of IKEv2 in-negotiation (open) SAs on the ASA.
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev2 enable

To enable ISAKMP IKEv2 negotiation on the interface on which the IPsec peer communicates with the ASA, use the **crypto ikev2 enable** command in global configuration mode. To disable ISAKMP IKEv2 on the interface, use the **no** form of this command.

crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]
no crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP IKEv2 negotiation.
client-services	Enables client services for IKEv2 connections on the interface. The Client Services Server provides HTTPS (SSL) access to allow the Secure Client Downloader to receive enhanced Secure Client features including software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy. If you disable client services, the Secure Client still establishes basic IPsec connections with IKEv2. If you do not enable the Client Services Server, users will not be able to download any of these files that the Secure Client might need. **Note** You can use the same port that you use for SSL VPN running on the same device. Even if you have an SSL VPN configured, you must select this option to enable file downloads over SSL for IPsec-IKEv2 clients.
port port	Specifies a port to enable client services for IKEv2 connections. The range is 1-65535. The default is port 443.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Using this command alone will not enable client services. This command requires SSL functionality.

Examples

The following example, entered in global configuration mode, shows how to enable IKEv2 on the outside interface:

```
ciscoasa(config)# crypto ikev2 enable outside client-services port 443
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev2 fragmentation

To configure fragmentation settings for IKEv2, use the **crypto ikev2 fragmentation** command in global configuration mode.

[**no**] **crypto ikev2 fragmentation** [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]
no crypto ikev2 fragmentation [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]

Syntax Description

mtu-size	The MTU size, 68-1500. The MTU value used should include the IPv4/IPv6 header + UDP header size. If you specify a value, the same value is used for both IPv4 and IPv6.
preferred-method	The preferred fragmentation method: Standard RFC-7383 based method (**ietf**) or Cisco Proprietary method (**cisco**).

Command Default

By default both the IKEv2 Fragmentation methods are enabled, the MTU is 576 for IPv4 or 1280 for IPv6, and the IETF method is preferred:

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

Use this command to:

- Set the MTU used to determine whether the IKE packets need fragmentation, packets exceeding this value will be fragmented.
- Change the preferred fragmentation method.
- Disable IKE fragmentation all together.

IETF RFC-7383 standard based IKEv2 fragmentation method will be used when both peers specify support and preference during negotiation. Using this method, encryption is done after fragmentation, providing individual protection for each IKEv2 Fragment message.

Cisco proprietary fragmentation will be used if it is the only method provided by a peer, such as the Secure Client, or if both peers specify support and preference during negotiation. Using this method fragmentation

is done after encryption. The receiving peer cannot decrypt or authenticate the message until all fragments are received.

Examples

The following example, entered in global configuration mode, shows how to enable IKEv2 on the outside interface:

Change the MTU value to 600:

```
ciscoasa(config)# crypto ikev2 fragmentation mtu 600
```

To change the preferred method of fragmentation to Cisco:

```
ciscoasa(config)# crypto ikev2 fragmentation preferred-method cisco
```

Related Commands

Command	Description
show crypto ikev2 sa detail	Shows the MTU.
show running-config all crypto ikev2	Displays the configuration.

crypto ikev2 limit max-in-negotiation-sa

To limit the number of IKEv2 in-negotiation (open) SAs on the ASA, use the **crypto ikev2 limit max-in-negotiation-sa** command in global configuration mode. To disable limits on the number of open SAs, use the **no** form of this command:

crypto ikev2 limit max-in-negotiation-sa { *percentage* | **value** *limit* }
no crypto ikev2 limit max-in-negotiation-sa { *percentage* | **value** *limit* }

Syntax Description

percentage	The threshold percentage of the number of SAs that are allowed to be in negotiation. The range is 1 to 100%. The default is 100%.
value *limit*	The maximum number of SAs that are allowed to be in negotiation. The possible range differs by device; use ? to see the range allowed for your device.

Command Default

The default is disabled. There is no limit to the number of open SAs.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.15(1)	Support was added to configure the maximum in-negotiation SAs as an absolute value up to 15000 or a maximum value derived from the maximum device capacity, rather than only a percentage.

Usage Guidelines

The **crypto ikev2 limit-max-in-negotiation-sa** command limits the maximum number of SAs that can be in negotiation at any time. Once the limit is reached, additional connections are denied. If used in conjunction with the crypto ikev2 cookie-challenge command, configure the cookie-challenge threshold lower than this limit for an effective cross-check.

Unlike the crypto ikev2 cookie-challenge command which challenges incoming connections with a cookie, the **crypto kev2 limit max in-negotiation-sa** command stops further connections from negotiating to protect current connections and prevent memory and/or CPU attacks that the cookie-challenge feature may be unable to thwart.

Examples

The following example limits the number of IKEv2 connections that are in negotiation to 70 percent of the maximum allowable IKEv2 connections:

```
ciscoasa(config)# crypto ikev2 limit max in-negotiation-sa 70
```

Related Commands

Command	Description
crypto ikev2 limit max-sa	Limits the number of IKEv2 connections on the ASA,
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev2 limit max-sa

To limit the number of IKEv2 connections on the ASA, use the **crypto ikev2 limit max-sa** command in global configuration mode. To disable the limit on the number of connections, use the **no** form of this command:

crypto ikev2 limit max-sa *number*
no crypto ikev2 limit max-sa *number*

Syntax Description

number	The number of IKEv2 connections allowed on the ASA. After reaching the limit, additional connections are denied. The range is 1 to 10000.

Command Default

The default is disabled. The ASA does not limit the number of IKEv2 connections. The maximum number of allowed IKEv2 connections equals the maximum number of connections specified by the license.

Usage Guidelines

The **crypto ikev2 limit max-sa** command limits the maximum number of SAs on the ASA.

If used in conjunction with the crypto ikev2 cookie-challenge command, configure the cookie-challenge threshold lower than this limit for an effective cross-check.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example limits the number of IKEv2 connections to 5000:

```
ciscoasa(config)# crypto ikev2 limit max-sa 5000
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
clear configure crypto isakmp	Clears all the ISAKMP configuration.

Command	Description
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev2 limit queue sa_init

To limit the number of security association (SA) initial packets to be processed per second in IKEv2 connections on the ASA, use the **crypto ikev2 limit queue sa_init** command in global configuration mode. To disable the limit on the number of SA initial packets, use the **no** form of this command:

crypto ikev2 limit queue sa_init *number*
no crypto ikev2 limit queue sa_init

Syntax Description

number The maxim number of IKEv2 SA INIT packets allowed on the ASA. After reaching the limit, more connections are denied.

By default, the SA_INIT queue limit is the default platform SA limit.

Command Default

By default, the SA_INIT queue limit is the default platform SA limit. You can use the **crypto ikev2 limit queue sa_init** command to change the default limit.

Usage Guidelines

The **crypto ikev2 limit queue sa_init**command limits the maximum number of SA INIT packets on the ASA.

When many remote access VPN sessions are established at same time or instability (link-down), CPU-hog can happen and most of the SA-INIT packets can stay in queue way past their allowed time. You can use this command to limit the number of SA-INIT packets that can be present in the queue at any time, rejecting the remaining packets.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.16(1)	This command was added.

Examples

The following example limits the number of IKEv2 SA_INIT packets to 5000:

```
ciscoasa(config)# crypto ikev2 limit queue sa_init 500
```

Related Commands

Command	Description
show crypto ikev2 stats	Display the IKEv2 runtime statistics.

Command	Description
show crypto ikev2 sa	Displays the IKEv2 runtime SA database.

crypto ikev2 notify

To allow an administrator to enable sending an IKE notification to the peer when an inbound packet is received on an SA that does not match the traffic selectors for that SA, use the **crypto ikev2 notify** command. To disable sending this notification, use the no form of the command:

crypto ikev2 notify invalid-selectors
[no] crypto ikev2 notify invalid-selectors

Syntax Description

invalid-selectors	Notify the peer if a packet is received on an SA but does not match the traffic selectors.
notify	Enable/disable IKEv2 notification to be sent to the peer.

Command Default

Sending the notification is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Examples

```
100/act(config) # crypto ikev2 ?
configure mode commands/options:
 cookie-challenge     Enable and configure IKEv2 cookie challenges based on half-open SAs
 enable     Enable IKEv2 on the specified interface
 limit     Enable limits on IKEv2 SAs
 policy     Set IKEv2 policy suite
 redirect     Set IKEv2 redirect
 remote-access     Configure IKEv2 for Remote Access
 notify     Enable/Disable IKEv2 notifications to be sent to the peer
100/act(config)# crypto ikev2 notify ?
configure mode commands/options:
 invalid-selectors     Notify the peer if a packet is received on an SA but does not match
 the traffic selectors
```

crypto ikev2 policy

To create an IKEv2 security association (SA) for IPsec connections, use the crypto ikev2 policy command in global configuration mode. To remove the policy, use the **no** form of this command:

crypto ikev2 policy *policy_index group < number >*
no crypto ikev2 policy *policy_index group < number >*

Syntax Description

group <number>	Specifies the Diffie-Hellman group(s) for this policy index as 14, 15, 16, 19, 20, 21, or 31.
policy index	Accesses the IKEv2 policy configuration mode and specifies the priority of the policy entry.

Command Default

No default behavior or values.

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, you enter IKEv2 policy configuration mode, in which you specify additional IKEv2 SA settings. You can use additional commands to set the SA encryption algorithm, DH group, integrity algorithm, lifetime, and hash algorithm.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	Support is added for configuring additional key exchange to secure the IPsec communication from quantum computer attacks.
9.16(1)	Support is added for DH group 31.

Release	Modification
9.15(1)	The following integrity, encryption, and ciphers are removed from this release in strong crypto license mode: • md5 • 3des encryption • des encryption • null encryption (removed from both strong and weak crypto license modes) Support is removed for DH groups 1, 2, 5, and 24.
9.13(1)	The following integrity, encryption, and ciphers are deprecated and will be removed in the future release: • md5 • 3des encryption • des encryption • null encryption Added Diffie-Hellman groups 15 and 16 and deprecated DH groups 1, 2, 5, and 24.
9.0(1)	Support for multiple context mode was added. Added policy index option.
8.4(1)	This command was added.

Examples

The following example creates the priority 1 IKEv2 SA and enters IKEv2 policy configuration mode:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5(DEPRECATED)
ciscoasa(config-ikev2-policy)# integrity sha
ciscoasa(config-ikev2-policy)# prf mad5(DEPRECATED)
ciscoasa(config-ikev2-policy)# prf sha
ciscoasa(config-ikev2-policy)# encryption 3des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption null(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption aes
ciscoasa(config-ikev2-policy)# encryption aes-192
ciscoasa(config-ikev2-policy)# additional-key-exchange 1
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.

Command	Description
show running-config crypto isakmp	Displays all the active configuration.
additional-key-exchange	Configures an additional key exchange transform for an IKEv2 policy.
show running-config crypto ikev2	Shows the details of the IKEv2 policy.
show crypto ikev2 sa detail	Shows the details of the IKEv2 SAs.

crypto ikev2 redirect

To specify the IKEv2 phase at which load-balancing redirection from master to cluster member occurs, use the **crypto ikev2 redirect** command in global configuration mode. To remove the command, use the **no** form of this command:

crypto ikev2 redirect { **during-init** | **during-auth** }
no crypto ikev2 redirect { **during-init** | **during-auth** }

Syntax Description

during-auth	Enables load-balancing redirection to a cluster member during the IKEv2 authentication exchange.
during-init	Enables load-balancing redirection to a cluster member during the IKEv2 SA initiated exchange.

Command Default

The default is load-balancing redirection to a cluster member, which occurs during the IKEv2 authentication exchange.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example sets the load-balancing redirection to a cluster member to occur during the IKEv2 initiated exchange:

```
ciscoasa(config)# crypto ikev2 redirect during-init
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables the ASA to send cookie challenges to peer devices in response to SA initiated packets,
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.

Command	Description
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto ikev2 remote-access trust-point

To specify a global trustpoint to be referenced and used as the identity certificate trustpoint of the ASA for AnyConnect IKEv2 connections, use the **crypto ikev2 remote-access trust-point** command in tunnel group configuration mode. To remove the command from the configuration, use the no form of the command.

crypto ikev2 remote-access trust-point *name* [*line number*]
no crypto ikev2 remote-access trust-point *name* [*line number*]

Syntax Description

name	The name of the trustpoint, up to 65 characters.
line number	Specifies where in the line number you want the trustpoint inserted. Typically, this option is used to insert a trustpoint at the top without removing and readding the other line. If a line is not specified, the ASA adds the trustpoint at the end of the list.

Command Default

No default behavior or values.

Usage Guidelines

Use the this command to configure a trustpoint for the ASA to authenticate itself to the Secure Client for all IKEv2 connections. Using this command allows the Secure Client to support group selection for the user.

You can configure two trustpoints at the same time: two RSA, two ECDSA, or one of each. The ASA scans the configured trustpoint list and chooses the first one that the client supports. If ECDSA is preferred, you should configure that trustpoint before the RSA trustpoint. If you try to add a trustpoint that already exists, you receive an error.

Note

1. If you use the no form of command without specifying which trustpoint name to remove, all trustpoint configuration is removed.
2. If there are one or more certificates with the same attributes, and one of them has expired, a "Certificate Validation Failure" error occurs. We recommend that you delete the expired certificate using the no form of this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added..

Release	Modification
9.0(1)	Support for multiple context mode and the configuration of two trustpoints were added.

Examples

The following example specifies the trustpoint *cisco_asa_trustpoint* :

```
ciscoasa(config)# crypto ikev2 remote-access trust-point cisco_asa_trustpoint
```

crypto ipsec df-bit

To configure DF-bit policy for IPsec packets, use the **crypto ipsec df-bit** command in global configuration mode.

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

Syntax Description

clear-df	(Optional) Specifies that the outer IP header will have the DF bit cleared and that the ASA may fragment the packet to add the IPsec encapsulation.
copy-df	(Optional) Specifies that the ASA will look in the original packet for the outer DF bit setting.
set-df	(Optional) Specifies that the outer IP header will have the DF bit set; however, the ASA may fragment the packet if the original packet had the DF bit cleared.
interface	Specifies an interface name.

Command Default

This command is disabled by default. If this command is enabled without a specified setting, the ASA uses the **copy-df** setting as the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The DF bit with IPsec tunnels feature lets you specify whether or not the ASA can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. The DF bit within the IP header determines whether or not a device is allowed to fragment a packet.

Use the **crypto ipsec df-bit** command in global configuration mode to configure the ASA to specify the DF bit in an encapsulated header. This command treats the DF-bit setting of the clear-text packet and either clears, set, or copies it to the outer IPsec header when encryption is applied.

When encapsulating tunnel mode IPsec traffic, use the **clear-df** setting for the DF bit. This setting lets the device send packets larger than the available MTU size. Also, this setting is appropriate if you do not know the available MTU size.

Caution Packets will get dropped if you set the following conflicting configuration: **crypto ipsec fragmentation after-encryption** (fragment packets) **crypto ipsec df-bit set-df outside** (set the DF bit)

Examples

The following example, entered in global configuration mode, sets the IPsec DF policy to **clear-df**:

```
ciscoasa(config)# crypto
 ipsec df-bit clear-df outside
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.
show crypto ipsec fragmentation	Displays the fragmentation policy for a specified interface.

crypto ipsec fragmentation

To configure the fragmentation policy for IPsec packets, use the **crypto ipsec fragmentation** command in global configuration mode.

crypto ipsec fragmentation { **after-encryption** | **before-encryption** } *interface*

Syntax Description

after-encryption	Specifies the ASA to fragment IPsec packets that are close to the maximum MTU size after encryption (disables prefragmentation).
before-encryption	Specifies the ASA to fragment IPsec packets that are close to the maximum MTU size before encryption (enables prefragmentation).
interface	Specifies an interface name.

Command Default

Before-encryption is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

When a packet is near the size of the MTU of the outbound link of the encrypting ASA, and it is encapsulated with IPsec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting device reassemble in the process path. Prefragmentation for IPsec VPNs increases the performance of the device when decrypting by letting it operate in the high performance CEF path instead of the process path.

Prefragmentation for IPsec VPNs lets an encrypting device predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPsec SA. If the device predetermines that the packet will exceed the MTU of the output interface, the device fragments the packet before encrypting it. This avoids process level reassembly before decryption and helps improve decryption performance and overall IPsec traffic throughput.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

Note Layer 2 Tunneling Protocol (L2TP) over IPsec supports only post fragmentation. Changes to the fragmentation policy **crypto ipsec fragmentation before-encryption/after-encryption <interface>** does not apply to L2TP.

Caution Packets will get dropped if you set the following conflicting configuration: **crypto ipsec fragmentation after-encryption** (fragment packets) **crypto ipsec df-bit set-df outside** (set the DF bit)

Examples

The following example, entered in global configuration mode, enables prefragmentation for IPsec packets on the inside interface only:

```
ciscoasa(config)# crypto
 ipsec fragmentation before-encryption inside
ciscoasa(config)#
```

The following example, entered in global configuration mode, disables prefragmentation for IPsec packets on the interface:

```
ciscoasa(config)# crypto
 ipsec fragmentation after-encryption inside
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the DF-bit policy for IPsec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPsec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

crypto ipsec ikev1 transform-set

To create or remove an IKEv1 transform set, use the **crypto ipsec ikev1 transform-set** command in global configuration mode. To remove a transform set, use the **no** form of this command.

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]
no crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

Syntax Description

authentication	(Optional) Specify one of the following authentication methods to ensure the integrity of IPsec data flows: **esp-md5-hmac** to use the MD5/HMAC-128 as the hash algorithm. **esp-sha-hmac** to use the SHA/HMAC-160 as the hash algorithm. **esp-none** to not use HMAC authentication.
encryption	Specify one of the following encryption methods to protect IPsec data flows: **esp-aes** to use AES with a 128-bit key. **esp-aes-192** to use AES with a 192-bit key. **esp-aes-256** to use AES with a 256-bit key. **esp-des** to use 56-bit DES-CBC. **esp-3des** to use triple DES algorithm. **esp-null** to not use encryption.
transform-set-name	Name of the transform set being created or modified. To view the transform sets already present in the configuration, enter the **show running-config ipsec** command.

Command Default

The default authentication setting is esp-none (no authentication).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0	This command was added.
7.2(1)	This section was rewritten.

Release	Modification
8.4(1)	The ikev1 keyword was added.
9.0(1)	Support for multiple context mode was added.
9.13(1)	This following options are deprecated and will be removed in the later release: • esp-md5-hmac • esp-3des • esp-des
9.15(1)	This following options are removed from this release: • esp-md5-hmac • esp-3des • esp-des

Usage Guidelines

This command identifies the IPsec encryption and hash algorithms to be used by the transform set.

Following the configuration of a transform set, you assign it to a crypto map. You can assign up to six transform sets to a crypto map. When the peer attempts to establish an IPsec session, the ASA evaluates the peer using the access list of each crypto map until it finds a match. The ASA then evaluates all of the protocols, algorithms, and other settings negotiated by the peer using those in the transform sets assigned to the crypto map until it finds a match. If the ASA matches the peer's IPsec negotiations to the settings in a transform set, it applies them to the protected traffic as part of its IPsec security association. The ASA terminates the IPsec session if it fails to match the peer to an access list and find an exact match of the security settings of the peer to those in a transform set assigned to the crypto map.

You can specify either the encryption or the authentication first. You can specify the encryption without specifying the authentication. If you specify the authentication in a transform set that you are creating, you must specify the encryption with it. If you specify only the authentication in a transform set that you are modifying, the transform set retains its current encryption setting.

If you are using AES encryption, we recommend that you use the **isakmp policy priority group 5** command, also in in global configuration mode, to assign Diffie-Hellman group 5 to accommodate the large key sizes provided by AES.



Tip When you apply transform sets to a crypto map or a dynamic crypto map and view the transform sets assigned to it, you will find it helpful if the names of the transform sets reflect their configuration. For example, the name "3des-md5" in the first example below shows the encryption and authentication used in the transform set. The values that follow the name are the actual encryption and authentication settings assigned to the transform set.

Examples

The following commands show all possible encryption and authentication options, excluding those that specify no encryption and no authentication:

```
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-md5 esp-3des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-sha esp-3des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-md5 esp-des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-sha esp-des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-md5 esp-aes esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-sha esp-aes esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-sha esp-aes-192 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-sha esp-aes-256 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-des (DEPRECATED)
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-3des(DEPRECATED)
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-md5-hmac (DEPRECATED)
```

Related Commands

Command	Description
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

crypto ipsec ikev1 transform-set mode transport

To specify the transport mode for IPsec IKEv1 connections, use the **crypto ipsec ikev1 transform-set** mode transport command in global configuration mode. To remove the command, use the **no** form of this command:

crypto ipsec ikev1 transform-set *transform-set-name* **mode** { **transport** }
no crypto ipsec ikev1 transform-set *transform-set-name* **mode** { **transport** }

Syntax Description

transform-set-name	Name of the transform set being modified. To view the transform sets already present in the configuration, enter the **show running-config ipsec** command.

Command Default

The default setting for the transport mode is disabled. IPsec uses the networked tunnel mode.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was rewritten.
8.4(1)	The ikev1 keyword was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **crypto ipsec ikev1 transform-set** mode transport command to specify the host-to-host transport mode for IPsec, instead of the default networked tunnel mode.

Examples

The following commands show all possible encryption and authentication options, excluding those that specify no encryption and no authentication:

```
ciscoasa(config)# crypto ipsec ikev1 transform-set
ciscoasa(config)#
```

Related Commands

Command	Description
show running-config ipsec	Displays the configuration of all transform sets.

Command	Description
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

crypto ipsec ikev2 ipsec-proposal

To create an IKEv2 proposal, use the **crypto ipsec ikev2 ipsec-proposal** command in global configuration mode.To remove the proposal, use the **no** form of this command.

crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*
no crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

Syntax Description

proposal name	Accesses the IPsec ESP proposal sub-mode.
proposal tag	The name of the IKEv2 IPsec proposal, a string from 1 to 64 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.13(1)	The following IKEv2/IPsec proposal integrity and encryption ciphers are deprecated and will be removed in the later release: • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

Release	Modification
9.15(1)	The following IKEv2/IPsec proposal integrity and encryption ciphers are removed from this release: • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

Usage Guidelines

This command creates a proposal and enters ipsec proposal configuration mode, in which you can specify multiple encryption and integrity types for the proposal.

Examples

The following example creates the IPsec proposal named secure, and enters IPsec proposal configuration mode:

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal secure
ciscoasa(config-ipsec-proposal)# protocol esp encryption ?
```

ciscoasa(config-ipsec-proposal)# **protocol esp aes**ciscoasa(config-ipsec-proposal)# **protocol esp 3des**(**DEPRECATED**

```
ciscoasa(config-ipsec-proposal)# protocol esp integrity ?
ciscoasa(config-ipsec-proposal)# protocol esp sha
ciscoasa(config-ipsec-proposal)# protocol esp md5
(DEPRECATED
)
```

Related Commands

Command	Description
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

crypto ipsec ikev2 sa-strength-enforcement

Ensures that the strength of the IKEv2 encryption cipher is higher than the strength of its child IPsec SA's encryption ciphers. To disable this feature, use the **no** form of this command.

crypto ipsec ikev2 sa-strength-enforcement
no crypto ipsec ikev2 sa-strength-enforcement

Command Default

Enforcement is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

Security is not increased when a child SA has a stronger encryption cipher than its parent IKEv2 connection. It is good security practice to configure the IPsec so this does not happen. The strength enforcement setting only affects the encryption cipher; it does not alter the integrity or key exchange algorithms. The IKEv2 system compares the relative strength of each child SA's selected encryption cipher as follows:

When enabled, verifies that the configured encryption cipher for the child SA is not stronger than the parent IKEv2 encryption cipher. If found, then the child SA will be updated to use the parent cipher. If no compatible cipher is found, then the child SA negotiation is be aborted. The syslog and debug message logs these actions.

The supported encryption ciphers are listed below in order of strength, from highest to lowest. Ciphers on the same line have equivalent strength for purposes of this check.

- AES-GCM-256, AES-CBC-256
- AES-GCM-192, AES-CBC, 192
- AES-GCM-128, AES-CBC-128
- 3DES
- DES
- AES-GMAC (any size), NULL

Related Commands

Command	Description
show running-config ipsec	Displays crypto ipsec ikev2 sa-strength-enforcement when enabled.

crypto ipsec inner-routing-lookup

To enable IPsec inner routing lookup, use the **crypto ipsec inner-routing-lookup** command in configuration mode. To disable IPsec inner routing lookup, use the **no** form of this command.

crypto ipsec inner-routing-lookup
no crypto ipsec inner-routing-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

IPsec inner-routing-lookup is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

By default, per-packet adjacency lookups are done for the outer ESP packets, but lookups are not done for packets sent through the IPsec tunnel.

In some network topologies, when a routing update has altered the inner packet's path, but the local IPsec tunnel is still up, packets through the tunnel may not be routed correctly and fail to reach their destination.

To prevent this, enable per-packet routing lookups for the IPsec inner packets. To avoid any performance impact from these lookups, this feature is disabled by default. Enable it only when necessary.

When this command is enabled, packets are punted to CPU for a route lookup before encryption is done. If too much traffic is sent to CPU, it will be discarded and the ASP drop counter will increase (punt-no-mem). This command is disabled by default. To avoid any potential impact on traffic, enable the command only when required.

This command, when configured, is only applicable for non-VTI based tunnels.

Examples

The following example configures and shows that inner-routing-lookup is enabled.:

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec

crypto ipsec inner-routing-lookup
```

Related Commands

Command	Description
show run crypto ipsec	Show the running crypto ipsec configuration.

crypto ipsec profile

To create a new IPsec profile, use the **crypto ipsec profile** command in the Global Configuration mode. Use the no form of the command to delete the IPsec profile.

crypto ipsec profile *name set pfs < group# >*
no crypto ipsec profile *name set pfs < group# >*

Syntax Description

name	Specifies a name for a new IPsec profile. The name can contain less than 65 characters.
group #	Specifies which Diffie-Hellman key exchange group to use.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	No	• Yes	No	—

Command History

Release	Modification
9.7(1)	We introduced this command and its submodes.

Examples

In the following example, VTIipsec is the new IPsec profile:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
```

Related Commands

Command	Description
responder-only	Sets the VTI tunnel interface to responder only mode.
set ikev1 transform-set	Specifies the IKEv1 transform set to be used in the IPsec profile configuration.
set pfs	Specifies the PFS group to be used in the IPsec profile configuration.
set security-association lifetime	Specifies the duration of security association in the IPsec profile configuration. This is specified in kilobytes or seconds, or both.

Command	Description
set trustpoint	Specifies a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection.

crypto ipsec security-association lifetime

To configure global lifetime values, use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset a global lifetime value to the default value, use the **no** form of this command.

crypto ipsec security-association lifetime { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }
no crypto ipsec security-association lifetime { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }

Syntax Description

kilobytes {*number* | **unlimited**}	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes. The default is 4,608,000 kilobytes. This setting does not apply to remote access VPN connections. It applies to site-to-site VPN only.
seconds *number*	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The default is 28,800 seconds (eight hours). This setting applies to both remote access and site-to-site VPN.
unlimited	Does not send Kilobytes in quick mode 1 packet when ASA is the initiator of the tunnel.

Command Default

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.1(2)	The **unlimited** argument was added.

Usage Guidelines

The **crypto ipsec security-association lifetime** command changes global lifetime values used when negotiating IPsec security associations.

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has no lifetime values configured, when the ASA requests new security associations during negotiation, it specifies its global lifetime value in the request to the peer; it uses this value as the lifetime of the new security associations. When the ASA receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

For site-to-site VPN connections, there are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached. For remote access VPN sessions, only the timed lifetime applies.

The ASA lets the user change crypto map, dynamic map, and IPsec settings on the fly. If this is changed, the ASA brings down only the connections affected by the change. If the user changes an existing access list associated with a crypto map, specifically by deleting an entry within the access list, the result is that only the associated connection is brought down. Connections based on other entries in the access list are not affected.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The security association (and corresponding keys) expires according to whichever occurs sooner, either after the number of seconds has passed or after the amount of traffic in kilobytes has passed.

Examples

The following example specifies a global timed lifetime for security associations:

```
ciscoasa(config)# crypto ipsec-security association lifetime seconds 240
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all IPsec configuration (that is, global lifetimes and transform sets).
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec security-association pmtu-aging

To enable path maximum transfer unit (PMTU) aging, use the **crypto ipsec security-association pmtu-aging** command in global configuration mode. To disable PMTU aging, use the no form of the command:

crypto ipsec security-association pmtu-aging *reset-interval*
no crypto ipsec security-association pmtu-aging *reset-interval*

Syntax Description

reset-interval	Sets the interval at which the PMTU value is reset.

Command Default

This feature is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The reset interval is specified in seconds.

crypto ipsec security-association replay

To configure the IPsec antireplay window size, use the **crypto ipsec security-association replay** command in global configuration mode. To reset the window size to the default value, use the **no** form of this command.

crypto ipsec security-association replay { **window-size** *n* | **disable** }
no crypto ipsec security-association replay { **window-size** *n* | **disable** }

Syntax Description

n	Sets the window size. Values can be 64, 128, 256, 512, or 1024. The default is 64.
disable	Disables antireplay checking.

Command Default

The default window size is 64.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Cisco IPsec authentication provides antireplay protection from an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association antireplay is a security service in which the receiver can reject old or duplicate packets to protect itself from replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, QoS gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor; this event can generate warning syslog messages that are false alarms. The **crypto ipsec security-association replay** command lets you expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the antireplay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number

on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future antireplay problems.

Examples

The following example specifies the antireplay window size for security associations:

```
ciscoasa(config)# crypto ipsec security-association replay window-size 1024
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all IPsec configuration (that is, global lifetimes and transform sets).
shape	Enables traffic shaping.
priority	Enables priority queuing.
show running-config crypto map	Displays all configuration for all the crypto maps.



crypto is – cz

- crypto isakmp disconnect-notify, on page 1043
- crypto isakmp identity, on page 1045
- crypto isakmp nat-traversal, on page 1047
- crypto isakmp policy authentication, on page 1049
- crypto isakmp policy encryption, on page 1051
- crypto isakmp policy group, on page 1053
- crypto isakmp policy hash, on page 1055
- crypto isakmp policy lifetime, on page 1057
- crypto isakmp reload-wait, on page 1059
- crypto key generate, on page 1060
- crypto key zeroize, on page 1063
- crypto large-cert-acceleration enable (Deprecated), on page 1065
- crypto map interface, on page 1067
- crypto map ipsec-isakmp dynamic, on page 1069
- crypto map match address, on page 1071
- crypto map set connection-type, on page 1073
- crypto map set df-bit, on page 1075
- crypto map set ikev1 phase1-mode, on page 1076
- crypto map set ikev2 ipsec-proposal, on page 1078
- crypto map set ikev2 mode, on page 1081
- crypto map set ikev2 phase1-mode, on page 1083
- crypto map set ikev2 pre-shared-key, on page 1085
- crypto map set inheritance, on page 1086
- crypto map set nat-t-disable, on page 1088
- crypto map set peer, on page 1090
- crypto map set pfs, on page 1092
- crypto map set reverse-route, on page 1094
- crypto map set security-association lifetime, on page 1096
- crypto map set tfc-packets, on page 1098
- crypto map set transform-set, on page 1099
- crypto map set trustpoint, on page 1102
- crypto map set validate-icmp-errors, on page 1104
- csc, on page 1105

- csd enable (Deprecated), on page 1108
- csd hostscan image (Deprecated), on page 1110
- csd image (Deprecated), on page 1112
- ctl, on page 1115
- ctl-file (Deprecated), on page 1117
- ctl-provider, on page 1119
- cts import-pac, on page 1121
- cts manual, on page 1124
- cts refresh environment-data, on page 1126
- cts role-based sgt-map, on page 1128
- cts server-group, on page 1130
- cts sxp connection peer, on page 1132
- cts sxp default password, on page 1134
- cts sxp default source-ip, on page 1136
- cts sxp delete-hold-down period, on page 1138
- cts sxp enable, on page 1139
- cts sxp mapping network-map, on page 1140
- cts sxp reconciliation period, on page 1141
- cts sxp retry period, on page 1143
- customization, on page 1145
- cxsc, on page 1147
- cxsc auth-proxy port, on page 1151

crypto isakmp disconnect-notify

To enable disconnect notification to peers, use the **crypto isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

crypto isakmp disconnect-notify
no crypto isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **isakmp disconnect-notify** command was added.
7.2.(1)	The **crypto isakmp disconnect-notify** command replaced the **isakmp disconnect-notify** command**.**
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can enable disconnect notifications to peers with the use of the following delete reasons:

- IKE_DELETE_RESERVED = 0An invalid code. Do not send.
- IKE_DELETE_BY_ERROR = 1A transmission error for a timeout or failure when expecting a response to a keepalive or any other IKE packet ACK. The default text is “Connectivity to client lost.”
- IKE_DELETE_BY_USER_COMMAND = 2The SA was actively deleted with manual intervention by the user or administrator. The default text is “Manually Disconnected by Administrator.”
- IKE_DELETE_BY_EXPIRED_LIFETIME = 3The SA has expired. The default text is “Maximum Configured Lifetime Exceeded.”
- IKE_DELETE_NO_ERROR = 4An unknown error caused the delete.
- IKE_DELETE_SERVER_SHUTDOWN = 5The server is being shut down.
- IKE_DELETE_SERVER_IN_FLAMES = 6The server has some severe problems. The default text is “Peer is having heat problems.”

- IKE_DELETE_MAX_CONNECT_TIME = 7The maximum allowed time of an active tunnel has expired. Unlike EXPIRED_LIFETIME, this reason indicates that the entire IKE-negotiated/controlled tunnel is being disconnected, not just this one SA. The default text is “Maximum Configured Connection Time Exceeded.”
- IKE_DELETE_IDLE_TIMEOUT = 8The tunnel has been idle for the maximum allowed time; therefore, the entire IKE-negotiated tunnel has been disconnected, not just this one SA. The default text is “Maximum Idle Time for Session Exceeded.”
- IKE_DELETE_SERVER_REBOOT = 9The server is rebooting.
- IKE_DELETE_P2_PROPOSAL_MISMATCH = 10Phase2 proposal mismatch.
- IKE_DELETE_FIREWALL_MISMATCH = 11Firewall parameter mismatch.
- IKE_DELETE_CERT_EXPIRED = 12User certification required. The default message is “User or Root Certificate has Expired.”
- IKE_DELETE_CLIENT_NOT_ALLOWED = 13Client type or version not allowed.
- IKE_DELETE_FW_SERVER_FAIL = 14Failed to contact Zone Integrity Server.
- IKE_DELETE_ACL_ERROR = 15ACL downloaded from AAA cannot be inserted. The default message is “ACL parsing error.”

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
ciscoasa(config)# crypto isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp identity

To set the Phase 1 ID to be sent to the peer, use the **crypto isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

crypto isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }
no crypto isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISAKMP negotiation by connection type; IP address for preshared key or cert DN for certificate authentication.
hostname	Uses the fully qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Command Default

The default ISAKMP identity is **crypto isakmp identity auto**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **isakmp identity** command was added.
7.2(1)	The **crypto isakmp identity** command replaced the **isakmp identity** command.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPsec peer, depending on connection type:

```
ciscoasa(config)# crypto isakmp identity auto
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp nat-traversal

To enable NAT traversal globally, check that ISAKMP is enabled (you enable it with the **crypto isakmp enable** command) in global configuration mode. To disable the NAT traversal, use the **no** form of this command.

crypto isakmp nat-traversal *natkeepalive*
no crypto isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keep alive interval, from 10 to 3600 seconds. The default is 20 seconds.

Command Default

By default, NAT traversal is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **isakmp nat-traversal** command was added.
7.2.(1)	The **crypto isakmp nat-traversal** command replaced the **isakmp nat-traversal** command**.**
8.0(2)	NAT traversal is enabled by default.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

NAT including PAT is used in many networks where IPsec is also used, but there are a number of incompatibilities that prevent IPsec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The ASA supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html , and supports NAT traversal for both dynamic and static crypto maps.

This command enables NAT-T globally on the ASA. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then sets NAT traversal with a keepalive interval of 30 seconds:

```
ciscoasa(config)# crypto isakmp enable
ciscoasa(config)# crypto isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy authentication

To specify an authentication method within an IKE policy, use the **crypto isakmp policy authentication** command in global configuration mode. To remove the ISAKMP authentication method, use the related **clear configure** command.

crypto isakmp policy *priority* **authentication** { **crack** | **pre-share** | **rsa-sig** }

Syntax Description

crack	Specifies IKE CRACK as the authentication method.
pre-share	Specifies preshared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
rsa-sig	Specifies RSA signatures as the authentication method. RSA signatures provide non-repudiation for the IKE negotiation. This basically means you can prove to a third party whether you had an IKE negotiation with the peer.

Command Default

The default ISAKMP policy authentication is **pre-share**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy authentication** command was added.
7.2.(1)	The **crypto isakmp policy authentication** command replaced the **isakmp policy authentication** command**.**

Usage Guidelines

IKE policies define a set of parameters for IKE negotiation.

If you specify RSA signatures, you must configure the ASA and its peer to obtain certificates from a CA server. If you specify preshared keys, you must configure these preshared keys separately within the ASA and its peer.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy authentication** command. This example sets the authentication method of RSA signatures to be used for the IKE policy with the priority number of 40.

```
ciscoasa(config)# crypto isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy encryption

To specify the encryption algorithm to use within an IKE policy, use the **crypto isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is des, use the **no** form of this command.

crypto isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }
no crypto isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }

Syntax Description

3des	Specifies that the triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Command Default

The default ISAKMP policy encryption is **3des**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy encryption** command was added.
7.2.(1)	The **crypto isakmp policy encryption** command replaced the **isakmp policy encryption** command**.**

Examples

The following example, entered in global configuration mode, shows use of the **crypto isakmp policy encryption** command; it sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25.

```
ciscoasa(config)# crypto isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40.

```
ciscoasa(config)# crypto isakmp policy 40 encryption 3des
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy group

To specify the Diffie-Hellman group for an IKE policy, use the **crypto isakmp policy group** command in global configuration mode.To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

crypto isakmp policy *priority* **group** { **1** | **2** | **5** }
no crypto isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
priority	Uniquely identifies the IIKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Command Default

The default group policy is group 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy group** command was added.
7.2.(1)	The **crypto isakmp policy group** command replaced the **isakmp policy group** command**.**
8.0(4)	The group 7 command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

IKE policies define a set of parameters to use during IKE negotiation.

There are three group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), and 1536-bit (DH Group 5). The 1024-bit and 1536-bit Diffie-Hellman Groups provide stronger security, but require more CPU time to execute.

Note The Cisco VPN Client Version 3.x or higher requires ISAKMP policy to use DH group 2. (If you configure DH group 1, the Cisco VPN Client cannot connect.)AES support is available on ASAs licensed for VPN-3DES only. Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman (DH) group 5 instead of group 1 or group 2. To configures group 5, use the **crypto isakmp policy priority group 5** command.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy group** command. This example sets group 2, the 1024-bit Diffie Hellman, to use for the IKE policy with the priority number of 40.

```
ciscoasa(config)# crypto isakmp policy 40 group   2
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **crypto isakmp policy hash** command in global configuration mode. To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

crypto isakmp policy *priority* **hash** { **md5** | **sha** }
no crypto isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) as the hash algorithm for the IKE policy.
priority	Uniquely identifies and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies SHA-1 (HMAC variant) as the hash algorithm for the IKE policy.

Command Default

The default hash algorithm is SHA-1 (HMAC variant).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy hash** command was added.
7.2.(1)	The **crypto isakmp policy hash** command replaced the **isakmp policy hash** command**.**

Usage Guidelines

IKE policies define a set of parameters to be used during IKE negotiation.

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy hash** command. This example specifies the MD5 hash algorithm for the IKE policy, with the priority number of 40.

```
ciscoasa(config)# crypto isakmp policy 40 hash    md5
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy lifetime

To specify the lifetime of an IKE security association before it expires, use the **crypto isakmp policy lifetime** command in global configuration mode. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command .

crypto isakmp policy *priority* **lifetime** *seconds*
no crypto isakmp policy *priority* **lifetime**

Syntax Description

priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for an infinite lifetime.

Command Default

The default value is 86,400 seconds (one day).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy lifetime** command was added.
7.2.(1)	The **crypto isakmp policy lifetime** command replaced the **isakmp policy lifetime** command**.**

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. You can specify an infinite lifetime if the peer does not propose a lifetime. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPsec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the ASA sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) for the IKE policy with the priority number of 40:

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime:

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 0
```

Related Commands

clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp reload-wait

To enable waiting for all active sessions to voluntarily terminate before rebooting the ASA, use the **crypto isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the ASA, use the **no** form of this command.

crypto isakmp reload-wait
no crypto isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **isakmp reload-wait** command was added.
7.2.(1)	The **crypto isakmp reload-wait** command replaced the **isakmp reload-wait** command**.**
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, tells the ASA to wait until all active sessions have terminated before rebooting:

```
ciscoasa(config)# crypto isakmp reload-wait
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto key generate

To generate key pairs for identity certificates, use the **crypto key generate** command in global configuration mode.

crypto key generate { **rsa** [**usage-keys** | **general-keys**] [**modulus** *size*] | **eddsa** [**edwards-curve ed25519**] | **ecdsa** [**elliptic-curve** *size*] } [**label** *key-pair-label*] [**noconfirm**]

Syntax Description

ecdsa	Generates an ECDSA key pair.
eddsa	Generates an EdDSA key pair. This type is not supported for SSH if you use the CiscoSSH stack. See the **ssh stack ciscossh** command.
edwards-curve ed25519	Specifies the ED25519 signature scheme, which is 256 bits.
elliptic-curve *size*	Specifies the bit length of the Suite B ECDSA key pair, 256, 384, or 521. The default is 384.
general-keys	Generates a single pair of RSA general purpose keys. This is the default key-pair type.
label *key-pair-label*	Specifies the name to be associated with the key pair. This key pair must be uniquely labeled. If you do not provide a label, the key pair is statically named Default-*type*-Key.
modulus *size*	Specifies the modulus size of the RSA key pairs: 2048, 3072, 4096. The default modulus size is 2048.
noconfirm	Suppresses all interactive prompting.
rsa	Generates an RSA key pair.
usage-keys	Generates two RSA key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.

Command Default

The default RSA key-pair type is **general key**. The default modulus size is 2048.

The default ECDSA key pair size is 384 bits.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for ECDSA keys was added.
9.9(2)	You can now set the modulus size to 3072.
9.16(1)	Support for EdDSA keys was added. Support for RSA modulus sizes below 2048 was removed. SSH support for EDCSA and EdDSA keys was added; previously, only RSA keys were supported.
9.17(1)	The EdDSA type is not supported for SSH if you use the CiscoSSH stack. See the **ssh stack ciscossh** command.

Usage Guidelines

Use the **crypto key generate** command to generate key pairs to support SSL, SSH, and IPsec connections. The generated key pairs are identified by labels that you can provide as part of the command syntax. Trustpoints that do not reference a key pair can use the default one, Default-*type*-Key. SSH connections always use this key. This does not affect SSL, because SSL generates its own certificate or key dynamically, unless a trustpoint has one configured.

For SSH, existing smaller keys can continue to be used after upgrading to 9.16, but we recommend that you upgrade to a larger size, or to a higher security key type. For other features, these RSA keys cannot be used in 9.16 and later. You can use the **crypto ca permit-weak-crypto** command to allow use of existing smaller keys, but even with this command, you cannot generate new smaller RSA keys.

Examples

The following example generates an RSA key pair with the label mypubkey:

```
ciscoasa(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
ciscoasa(config)#
```

The following example generates an RSA key pair with the default label:

```
ciscoasa(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

The following example generates an ECDSA key: a warning message because there is not enough space to save the RSA keypair:

```
ciscoasa(config)# crypto key generate ecdsa label new-ecdsa-key elliptic-curve 521

INFO: The name for the keys will be: new-ecdsa-key
Keypair generation process begin. Please wait...
```

Related Commands

Command	Description
crypto key zeroize	Removes key pairs.

Command	Description
show crypto key	Displays the key pairs.

crypto key zeroize

To remove the key pairs of the indicated type, use the **crypto key zeroize** command in global configuration mode.

crypto key zeroize { **rsa** | **eddsa** | **ecdsa** } [**label** *key-pair-label*] [**default**] [**noconfirm**]

Syntax Description

default	Removes the default key pair of the specified type.
ecdsa	Specifies ECDSA as the key type.
eddsa	Specifies EDDSA as the key type.
label *key-pair-label*	Identifies the key pair to remove. If you do not provide a label, the system removes all key pairs of the indicated type.
noconfirm	Suppresses all interactive prompting.
rsa	Specifies RSA as the key type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for ECDSA was added.
9.16(1)	Support for EDDSA was added

Examples

The following example, entered in global configuration mode, removes all RSA key pairs:

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no] y
ciscoasa(config)#
```

Related Commands

Command	Description
crypto key generate	Generates key pairs for identity certificates.

crypto large-cert-acceleration enable (Deprecated)

To enable the ASA to perform 2048-bit RSA key operations in hardware, use the **crypto large-cert-acceleration enable** command in global configuration mode. To perform 2048-bit RSA key operations in software, use the **no crypto large-cert-acceleration enable** command.

crypto large-cert-acceleration enable
no crypto large-cert-acceleration enable

Syntax Description

This command has no keywords or arguments.

Command Default

By default, 2048-bit RSA key operations are performed in software.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(3)	This command was added.
8.2(5)	This command was deprecated. The **crypto engine large-mod-accel** command has replaced it.

Usage Guidelines

This command is only available on the ASA 5510, ASA 5520, ASA 5540, and 5550. The command is not available on the ASA 5580.

Examples

The following example shows that 2048-bit RSA key operations have been enabled in hardware:

```
ciscoasa
 (config)#
show r
unning-config crypto large-cert-acceleration
crypto large-cert-acceleration enable
ciscoasa
 (config)#
```

Related Commands

Command	Description
clear configure crypto	Clears the 2048-bit RSA key configuration with the rest of the crypto configuration.

Command	Description
show running-config crypto	Shows the 2048-bit RSA key configuration with the rest of the crypto configuration.

crypto map interface

To apply a previously defined crypto map set to an interface, use the **crypto map interface** command in global configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]
no crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

Syntax Description

interface-name	Specifies the interface for the ASA to use for establishing tunnels with VPN peers. If ISAKMP is enabled, and you are using a CA to obtain certificates, this should be the interface with the address specified in the CA certificates.
map-name	Specifies the name of the crypto map set.
ipv6-local-address ipv6-address	Specifies an IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	The ipv6-local-address keyword was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use this command to assign a crypto map set to any active ASA interface. The ASA supports IPsec termination on any and all active interfaces. You must assign a crypto map set to an interface before that interface can provide IPsec services.

You can assign only one crypto map set to an interface. If multiple crypto map entries have the same map name but a different sequence number, they are part of the same set and are all applied to the interface. The ASA evaluates the crypto map entry with the lowest sequence number first.

Use the ipv6-local-address keyword when you have multiple IPv6 addresses configured on an interface and are configuring the ASA to support LAN-to-LAN VPN tunnels in an IPv6 environment.

Note The ASA lets you change crypto map, dynamic map, and IPsec settings on the fly. If you do so, the ASA brings down only the connections affected by the change. If you change an existing access list associated with a crypto map, specifically by deleting an entry within the accesslist, the result is that only the associated connection is brought down. Connections based on other entries in the access list are not affected.Every static crypto map must define three parts: an access list, a transform set, and an IPsec peer. If one of these is missing, the crypto map is incomplete and the ASA moves on to the next entry. However, if the crypto map matches the access list but not either or both of the other two requirements, this ASA drops the traffic. Use the **show running-config crypto map** command to ensure that every crypto map is complete. To fix an incomplete crypto map, remove the crypto map, add the missing entries, and reapply it.

Examples

The following example, entered in global configuration mode, assigns the crypto map set named mymap to the outside interface. When traffic passes through the outside interface, the ASA evaluates it using all the crypto map entries in the mymap set. When outbound traffic matches an access list in one of the mymap crypto map entries, the ASA forms a security association using that crypto map entry's configuration.

```
ciscoasa(config)# crypto map mymap interface outside
```

The following example shows the minimum required crypto map configuration:

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap set transform-set my_t_set1
ciscoasa(config)# crypto map mymap set peer 10.0.0.1
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map ipsec-isakmp dynamic

To require a given crypto map entry to refer to a preexisting dynamic crypto map, use the **crypto map ipsec-isakmp dynamic** command in global configuration mode. To remove the cross-reference, use the **no** form of this command.

Use the **crypto dynamic-map** command to create dynamic crypto map entries. After you create a dynamic crypto map set, use the **crypto map ipsec-isakmp dynamic** command to add the dynamic crypto map set to a static crypto map.

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*
no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

Syntax Description

dynamic-map-name	Specifies the name of the crypto map entry that refers to a preexisting dynamic crypto map.
ipsec-isakmp	Indicates that IKE establishes the IPsec security associations for this crypto map entry.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to remove the **ipsec-manual** keyword.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

After you define crypto map entries, you can use the **crypto map interface** command to assign the dynamic crypto map set to interfaces.

Dynamic crypto maps provide two functions: filtering/classifying traffic to protect, and defining the policy to apply to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPsec dynamic crypto maps identify the following:

- The traffic to protect
- IPsec peer(s) with which to establish a security association
- Transform sets to use with the protected traffic
- How to use or manage keys and security associations

A crypto map set is a collection of crypto map entries, each with a different sequence number (*seq-num*) but the same map name. Therefore, for a given interface, you could have certain traffic forwarded to one peer with specified security applied to that traffic, and other traffic forwarded to the same or a different peer with different IPsec security applied. To accomplish this, you create two crypto map entries, each with the same map name, but each with a different sequence number.

The number you assign as the *seq-num* argument should not be arbitrary. This number ranks multiple crypto map entries within a crypto map set. A crypto map entry with a lower sequence number is evaluated before a map entry with a higher sequence number; that is, the map entry with the lower number has a higher priority.



Note When you link the crypto map to a dynamic crypto map, you must specify the dynamic crypto map. This links the crypto map to an existing dynamic crypto map that was previously defined using the **crypto dynamic-map** command. Now any changes you make to the crypto map entry after it has been converted will not take affect. For example, a change to the set peer setting does not take effect. However, the ASA stores the change while it is up. When the dynamic crypto map is converted back to the crypto map, the change is effective and appears in the output of the **show running-config crypto map** command. The ASA maintains these settings until it reboots.

Examples

The following command, entered in global configuration mode, configures the crypto map mymap to refer to a dynamic crypto map named test:

```
ciscoasa(config)# crypto map mymap ipsec-isakmp dynamic test
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map match address

To assign an access list to a crypto map entry, use the **crypto map match address** command in global configuration mode. To remove the access list from a crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **match address** *acl_name*
no crypto map *map-name seq-num* **match address** *acl_name*

Syntax Description

acl_name	Specifies the name of the encryption access list. This name should match the name argument of the named encryption access list being matched.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use the **access-list** command to define the access lists. The access list hit counts only increase when the tunnel initiates. After the tunnel is up, the hit counts do not increase on a per-packet flow. If the tunnel drops and then reinitiates, the hit count will be increased.

The ASA uses the access lists to differentiate the traffic to protect with IPsec crypto from the traffic that does not need protection. It protects outbound packets that match a permit ACE, and ensures that inbound packets that match a permit ACE have protection.

When the ASA matches a packet to a deny statement, it skips the evaluation of the packet using the remaining ACEs in the crypto map, and resumes evaluation of the packet using the ACEs in the next crypto map in sequence. *Cascading ACLs* involves the use of deny ACEs to bypass evaluation of the remaining ACEs in an ACL, and the resumption of evaluation of traffic using the ACL assigned to the next crypto map in the crypto

map set. Because you can associate each crypto map with different IPsec settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security.

Note The crypto access list does not determine whether to permit or deny traffic through the interface. An access list applied directly to the interface with the **access-group** command makes that determination. In transparent mode, the destination address should be the IP address of the ASA, the management address. Only tunnels to the ASA are allowed in transparent mode.

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set connection-type

To specify the connection type for the backup Site-to-Site feature for this crypto map entry, use the **crypto map set connection-type** command in global configuration mode. To return to the default setting, use the **no** form of this command.

crypto map *map-name seq-num* **set connection-type** { **answer-only** | **originate-only** | **bidirectional** }
no crypto map *map-name seq-num* **set connection-type** { **answer-only** | **originate-only** | **bidirectional** }

Syntax Description

answer-only	Specifies that this peer only responds to inbound IKE connections first during the initial proprietary exchange to determine the appropriate peer to connect to.
bidirectional	Specifies that this peer can accept and originate connections based on this crypto map entry. This is the default connection type for all Site-to-Site connections.
map-name	Specifies the name of the crypto map set.
originate-only	Specifies that this peer initiates the first proprietary exchange to determine the appropriate peer to connect to.
seq-num	Specifies the number you assign to the crypto map entry.
set connection-type	Specifies the connection type for the backup Site-to-Site feature for this crypto map entry. There are three types of connections: answer-only, originate-only, and bidirectional.

Command Default

The default setting is bidirectional.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0	This command was added.
9.0	Support for multiple context mode was added.

Usage Guidelines

The **crypto map set connection-type** command specifies the connection types for the backup LAN-to-LAN feature. It allows multiple backup peers to be specified at one end of the connection.

This feature works only between the following platforms:

- Two Cisco ASA 5500 series
- A Cisco ASA 5500 series and a Cisco VPN 3000 concentrator
- A Cisco ASA 5500 series and a security appliance running Cisco PIX security appliance software Version 7.0, or higher

To configure a backup LAN-to-LAN connection, we recommend that you configure one end of the connection as originate-only using the **originate-only** keyword, and the end with multiple backup peers as answer-only using the **answer-only** keyword. On the originate-only end, use the **crypto map set peer** command to order the priority of the peers. The originate-only ASA attempts to negotiate with the first peer in the list. If that peer does not respond, the ASA works its way down the list until either a peer responds or there are no more peers in the list.



Note IKEv2 does not support backup site to site, which is set when using the originate-only or answer-only keyword. The cryto map set connection-type must be bidirectional when using IKEv2.

When configured in this way, the originate-only peer initially attempts to establish a proprietary tunnel and negotiate with a peer. Thereafter, either peer can establish a normal LAN-to-LAN connection and data from either end can initiate the tunnel connection.

In transparent firewall mode, you can see this command but the connection-type value cannot be set to anything other than answer-only for crypto map entries that are part of a crypto map that has been attached to the interface.

<xref> lists all supported configurations. Other combinations may result in unpredictable routing issues.

Table 6: Supported Backup LAN-to-LAN Connection Types

Remote Side	Central Side
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the connection-type to originate-only.

```
ciscoasa(config)# crypto map mymap 10 set connection-type
originate-only
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set df-bit

To set the per-signature algorithm (SA) do-not-fragment (DF) policy, use the **crypto map set df-bit** command in global configuration mode. To disable the DF policy, use the **no** form of this command.

crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]
no crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

Syntax Description

name	Specifies the name of the crypto map set.
priority	Specifies the priority that you assign to the crypto map entry.

Command Default

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The original DF policy command is retained and acts as a global policy setting on an interface, but it is superseded for an SA by the **crypto map** command.

crypto map set ikev1 phase1-mode

To specify the IKEv1 mode for phase 1 when initiating a connection to either main or aggressive, use the **crypto map set ikev1 phase1-mode** command in global configuration mode. To remove the setting for phase 1 IKEv1 negotiations, use the **no** form of this command.

crypto map *map-name seq-num* **set ikev1 phase1-mode** [**main** | **aggressive** [**group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20** | **group21**]]
no crypto map *map-name seq-num* **set ikev1 phase1-mode** [**main** | **aggressive** [**group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20** | **group21**]]

Syntax Description

aggressive	Specifies aggressive mode for Phase 1 IKEv1 negotiations.
group14	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group15	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group16	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group19	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group20	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group21	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
main	Specifies main mode for Phase 1 IKEv1 negotiations.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

The default Phase 1 mode is **main**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(4)	The group 7 command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.
8.4(1)	The **ikev1** keyword was added.
9.0(1)	Support for multiple context mode was added.
9.13(1)	Support for DH groups 14, 15, and 16 is added and set as default. The **groups 1, 2,** and **group 5** option was deprecated and will be removed in the later release.
9.15(1)	Support for DH groups 1, **2 and 5 is removed.**

Usage Guidelines

Phase 1 IKEv1 negotiations can use either main mode or aggressive mode. Both provide the same services, but aggressive mode requires only two exchanges between the peers totaling three messages, rather than three exchanges totaling six messages.

The aggressive mode is faster because it uses only three messages, to exchange data and identify the two VPN endpoints. The identification of the VPN endpoints makes Aggressive Mode less secure.

When you use Aggressive mode, the number of exchanges between two endpoints is fewer than it would be if you used Main Mode, and the exchange relies mainly on the ID types used in the exchange by both appliances. Aggressive Mode does not ensure the identity of the peer. Main Mode ensures the identity of both peers, but can only be used if both sides have a static IP address. If your device has a dynamic IP address, you should use Aggressive mode for Phase 1.

This command works only in initiator mode; not in responder mode. Including a Diffie-Hellman group with aggressive mode is optional. If one is not included, the ASA uses group 2.

Examples

The following example, entered in global configuration mode, configures the crypto map my map and sets the phase one mode to aggressive using group 2:

```
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group2
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group14
```

Related Commands

Command	Description
clear isakmp sa	Delete the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set ikev2 ipsec-proposal

To specify the IKEv2 proposal to use in a crypto map entry, use the **crypto map set ikev2 ipsec-proposal** command in global configuration mode. To remove the names of the proposals from a crypto map entry, use the **no** form of this command with the specified proposal name. To specify all or none of the proposal and remove the crypto map entry, use the **no** form of the command.

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*...proposal-name11*]
no crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*...proposal-name11*]
no crypto map *map-name seq-num* **set ikev2 ipsec-proposal**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the sequence number that corresponds to the crypto map entry.
propsal-name1 *proposal-name11*	Specifies one or more names of the IPsec proposals for IKEv2. Any proposal named in this command must be defined in the **crypto ipsec ikev2 ipsec-proposal** command. Each crypto map entry supports up to 11 proposals.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.15(1)	The following integrity, encryption, and ciphers are removed from this release • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

Usage Guidelines

For all crypto map entries, an IKEv1 transform set or an IKEv2 proposal is required.

The peer at the opposite end of the IPsec IKEv2 initiation uses the first matching proposal for the security association. If the local ASA initiates the negotiation, the order specified in the **crypto map** command determines the order in which theASA presents the contents of the proposals to the peer. If the peer initiates the negotiation, the local ASA uses the first proposal in the crypto map entry that matches the IPsec parameters sent by the peer.

If the peer at the opposite end of the IPsec initiation fails to match the values of the proposals, IPsec does not establish a security association. The initiator drops the traffic because there is no security association to protect it.

To change the list of proposals, create a new list and specify it to replace the old one.

If you use this command to modify a crypto map, the ASA modifies only the crypto map entry with the same sequence number you specify. For example, the ASA inserts the proposal named 56des-sha in the last position if you enter the following commands:

```
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal
128aes-md5

128aes-sha

192aes-md5

ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal
56des-sha
ciscoasa(config)#
```

The response to the following command shows the cumulative effect of the previous two commands:

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set ipsec-proposal 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

To reconfigure the sequence of proposals in a crypto map entry, delete the entry, specifying both the map name and sequence number; then recreate it. For example, the following commands reconfigure the crypto map entry named map2, sequence 3:

```
asa2(config)# no crypto map map2 3 set
ikev2
ipsec-proposal
asa2(config)# crypto map map2 3 set
ikev2
ipsec-proposal 192aes-sha 192aes-md5 128aes-sha 128aes-md5
asa2(config)#
```

Examples

The following example creates a crypto map entry named map2, consisting of ten proposals.

```
ciscoasa(config)# crypto map map2 10 set ikev2 ipsec-proposal 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.

Command	Description
clear configure crypto map	Clears all crypto maps from the configuration.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
crypto ipsec transform-set	Configures a transform set.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto map set ikev2 mode

To specify the IKEv2 mode to use in a crypto map entry, use the **crypto map set ikev2 mode** command in global configuration mode. To reset the mode, use the **no** form of this command with the configured mode.

crypto map *map-name seq-num* **set ikev2 mode** { **transport** | **transport-require** | **tunnel** }
no crypto map *map-name seq-num* **set ikev2 mode** { **transport** | **transport-require** | **tunnel** }

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the sequence number that corresponds to the crypto map entry.
transport	Set preference for transport mode.
transport-require	Require transport mode.
tunnel	Set tunnel mode (default)

Command Default

If the mode is not set, it is tunnel by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For IKEv2, specify the mode for applying ESP encryption and authentication to the tunnel. This determines what part of the original IP packet has ESP applied.

Where tunnel encapsulation mode is the default. transport encapsulation mode is transport mode with the option to fallback to tunnel mode if the peer does not support it, and transport-require encapsulation mode enforces transport mode only. Transport mode is not recommended for Remote Access VPNs.

- Tunnel mode—(default) Encapsulation mode will be tunnel mode. Tunnel mode applies ESP encryption andauthentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destinationaddresses.The entire original IP datagram is encrypted, and it becomes the payload in a new IP packet.

This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPsec

tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPsec. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

- Transport mode— Encapsulation mode will be transport mode with option to fallback on tunnel mode, if peer does not support it. In Transport mode only the IP payload is encrypted, and the original IP headers are left intact.

This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. With transport mode, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header is encrypted, which limits examination of the packet.

- Transport Required— Encapsulation mode will be transport mode only, falling back to tunnel mode is not allowed.

Negotiation of the encapsulation mode is as follows:

- If the initiator proposes transport mode, and the responder responds with tunnel mode, the initiator will fall back to Tunnel mode.
- If the initiator proposes tunnel mode, and responder responds with transport mode, the responder will fallback to Tunnel mode.
- If the initiator proposes tunnel mode and responder has transport-require mode, then NO PROPOSAL CHOSEN will be sent by the responder.
- Similarly if initiator has transport-require, and responder has tunnel mode, NO PROPOSAL CHOSEN will be sent by the responder.

Related Commands

Command	Description
show running-config crypto map	Displays the crypto map configuration.
clear configure crypto map	Clears all crypto maps from the configuration.

crypto map set ikev2 phase1-mode

To specify the IKEv2 mode for Phase 1 when initiating a connection to either main or aggressive, use the **crypto map set ikev2 phase1-mode** command in global configuration mode. To remove the setting for Phase 1 IKEv2 negotiations, use the **no** form of this command.

crypto map *map-name seq-num* **set ikev2 phase1-mode** { **main** | **aggressive** [**group1** | **group2** | **group5**] }
no crypto map *map-name seq-num* **set ikev2 phase1-mode** { **main** | **aggressive** [**group1** | **group2** | **group5**] }

Syntax Description

aggressive	Specifies aggressive mode for Phase 1 IKEv2 negotiations.
group1	Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
main	Specifies main mode for Phase 1 IKEv2 negotiations.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

The default Phase 1 mode is **main**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(4)	The group 7 command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command works only in initiator mode; not in responder mode. Including a Diffie-Hellman group with aggressive mode is optional. If one is not included, the ASA uses group 2.

Examples

The following example, entered in global configuration mode, configures the crypto map my map and sets the Phase 1 mode to aggressive, using group 2.

```
ciscoasa(config)# crypto map mymap 10 set ikev2 phase1mode aggressive group2
ciscoasa(config)#
```

Related Commands

Command	Description
clear isakmp sa	Delete the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set ikev2 pre-shared-key

To specify a preshared key for remote access IKEv2 connections, the crypto map set ikev2 pre-shared-key command in global configuration mode. To return to the default setting, use the **no** form of this command.

crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*
no crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

Syntax Description

key	Alphanumeric string from 1 to 128 characters.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example configures the preshared key SKTIWHT:

```
ciscoasa(config)# crypto map crypto_map_example set ikev2 pre-shared-key SKTIWHT
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set inheritance

To set the granularity (single or multiple) of security associations generated for this crypto map entry, use the **set inheritance** command in global configuration mode. To remove the inheritance setting for this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set inheritance** { **data** | **rule** }
no crypto map *map-name seq-num* **set inheritance** { **data** | **rule** }

Syntax Description

data	Specifies one tunnel for every address pair within the address ranges specified in the rule.
map-name	Specifies the name of the crypto map set.
rule	Specifies one tunnel for each ACL entry associated with this crypto map. This is the default.
seq-num	Specifies the number that you assign to the crypto map entry.
set inheritance	Specifies the type of inheritance: **data or rule**. Inheritance allows a single security association (SA) to be generated for each security policy database (SPD) rule or multiple security SAs for each address pair in the range.

Command Default

The default value is **rule**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command works only when the ASA is initiating the tunnel, not when responding to a tunnel. Using the data setting may create a large number of IPsec SAs. This consumes memory and results in fewer overall tunnels. You should use the data setting only for extremely security-sensitive applications.

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the inheritance type to data:

```
ciscoasa(config)# crypto map mymap 10 set inheritance data
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set nat-t-disable

To disable NAT-T for connections based on this crypto map entry, use the **crypto map set nat-t-disable** command in global configuration mode. To enable NAT-T for this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set nat-t-disable**
no crypto map *map-name seq-num* **set nat-t-disable**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Command Default

The default setting for this command is not on (therefore NAT-T is enabled by default).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **isakmp nat-traversal** command to globally enable NAT-T. Then you can use the **crypto map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command, entered in global configuration mode, disables NAT-T for the crypto map entry named mymap:

```
ciscoasa(config)# crypto map mymap 10 set nat-t-disable
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
isakmp nat-traversal	Enables NAT-T for all connections.

Command	Description
show running-config crypto map	Displays the crypto map configuration.

crypto map set peer

To specify an IPsec peer in a crypto map entry, use the **crypto map set peer** command in global configuration mode. Use the no form of this command to remove an IPsec peer from a crypto map entry.

crypto map *map-name seq-num* **set peer** { *ip_address* | *hostname* } { *...ip_address10* | *hostname10*
no crypto map *map-name seq-num* **set peer** { *ip_address* | *hostname* } { *...ip_address10* | *hostname10*

Syntax Description

hostname	Specifies a peer by its hostname as defined by the ASA **name** command.
ip_address	Specifies a peer by its IP address (IPv4 or IPv6).
map-name	Specifies the name of the crypto map set.
peer	Specifies an IPsec peer in a crypto map entry either by hostname or IP address (IPv4 or IPv6). From 9.14(1), multiple peers are supported also for IKEv2.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to allow up to 10 peer addresses.
9.0(1)	Support for multiple context mode was added.
9.14(1)	Multiple peer support for IKEv2 was added.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used because the peer is usually unknown.

Configuring multiple peers is equivalent to providing a fallback list. For each tunnel, the ASA attempts to negotiate with the first peer in the list. If that peer does not respond, the ASA works its way down the list until either a peer responds or there are no more peers in the list. You can set up multiple peers only when using the backup LAN-to-LAN feature (that is, when the crypto map connection type is originate-only). For more information, see the **crypto map set connection-type** command.

Note From 9.14(1), multiple peers are supported for IKEv2.

Examples

The following example, entered in global configuration mode, shows a crypto map configuration using IKE to establish the security associations. In this example, you can set up a security association to either the peer at 10.0.0.1 or the peer at 10.0.0.2:

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap 10 set transform-set my_t_set1
ciscoasa(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set pfs

Use the **crypto map set pfs** command in global configuration mode to set IPsec to ask for PFS when requesting new security associations for this crypto map entry or that IPsec requires PFS when receiving requests for new security associations. To specify that IPsec should not request PFS, use the **no** form of this command.

crypto map *map-name seq-num* **set pfs** [**group14** | **group15** | **group16** | **group19** | **group20** | **group21**]
no crypto map *map-name seq-num* **set pfs** [**group14** | **group15** | **group16** | **group19** | **group20** | **group21**]

Syntax Description

group14	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group15	Specifies that IPsec should use the 3072-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group16	Specifies that IPsec should use the 4096-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group19	Specifies that IPsec should use the 256-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. Unsupported for IKEv1.
group20	Specifies that IPsec should use the 384-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. Unsupported for IKEv1.
group21	Specifies that IPsec should use the 521-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. Unsupported for IKEv1.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

By default PFS is not set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to add Diffie-Hellman group 7.

Release	Modification
8.0(4)	The group 7 command option was deprecated. Attempts to configure group 7 will generate an error message and use group 5 instead.
9.0(1)	Support for multiple context mode was added.
9.13(1)	Support for DH groups 14, 15, and 16 was added. The DH groups 1, 2, 5, and 24 options are deprecated and will be removed in the later releases.
9.15(1)	Support for the DH groups 1, 2, 5, and 24 options are removed in this release.

Usage Guidelines

With PFS, each time a new security association is negotiated, a new Diffie-Hellman exchange occurs, which requires additional processing time. PFS adds another level of security because if one key is ever cracked by an attacker, only the data sent with that key is compromised.

During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. If the **set pfs** statement does not specify a group, the ASA sends the default. The default is group2 for releases prior to 9.13, and group14 for release 9.13 and later.

If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, the ASA assumes the default group. If the local configuration specifies a group, that group must be part of the peer's offer or the negotiation fails.

For a negotiation to succeed, PFS has to be set on both ends of the LAN to LAN tunnel (with or without the Diffie-Hellman group). If set, the groups have to be an exact match. The ASA does not accept just any offer of PFS from the peer.

In general, higher groups provide more security than lower groups, but they require more processing time than the lower groups.

When interacting with the Cisco VPN Client, the ASA does not use the PFS value, but instead uses the value negotiated during Phase 1.

Examples

The following example, entered in global configuration mode, specifies that PFS should be used whenever a new security association is negotiated for the crypto map mymap 10:

```
ciscoasa(config)# crypto map mymap 12 set pfs group14
ciscoasa{config}# crypto map mymap 12 set pfs group15
.
```

Related Commands

Command	Description
clear isakmp sa	Deletes the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel groups and their parameters.

crypto map set reverse-route

To enable reverse route injection for any connection based on this crypto map entry, use the **crypto map set reverse-route** command in global configuration mode. To disable reverse route injection for any connection based this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set reverse-route** [**dynamic**]
no crypto map *map-name seq-num* **set reverse-route** [**dynamic**]

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.
dynamic	RRI is dynamic, added or deleted whenever an IPsec tunnel is created or destroyed.

Command Default

The default setting for this command is off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.7(1)	Support for dynamic RRI added.

Usage Guidelines

Do not enable RRI if you specify any source/destination (0.0.0.0/0.0.0.0) as the protected network, because this will impact traffic that uses your default route.

If **dynamic** is not specified, RRI is done upon configuration and is considered static, remaining in place until the configuration changes or is removed. The ASA automatically adds static routes to the routing table and announces these routes to its private network or border routers using OSPF.

If dynamic is specified, routes are created upon the successful establishment of IPsec security associations (SA's). Routes will be added based on the negotiated selector information. The routes will be deleted after the IPsec SA's are deleted. Also, a configuration change from dynamic to static and vice-versa causes the existing IPsec tunnels for that crypto map to be torn down.

Typically, RRI routes are used to Initiate a tunnel if one is not present and traffic needs to be encrypted. With dynamic RRI support, no routes are present before the tunnel is brought up. Therefore, an ASA with dynamic RRI configured would typically work only as a responder.

Dynamic RRI applies to IKEv2 based static crypto maps only.

Examples

The following example, entered in global configuration mode, enables reverse route injection for the crypto map named mymap.

```
ciscoasa(config)# crypto map mymap 10 set reverse-route
ciscoasa(config)#
```

The following example, entered in global configuration mode, enables reverse route injection upon tunnel establishment:

```
ciscoasa(config)#crypto map mymap 1 set reverse-route dynamic
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations, use the **crypto map set security-association lifetime** command in global configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

crypto map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }
no crypto map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }

Syntax Description

kilobytes {*number* | **unlimited**}	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes. The global default is 4,608,000 kilobytes. This setting does not apply to remote access VPN connections. It applies to site-to-site VPN only.
map-name	Specifies the name of the crypto map set.
seconds *number*	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The global default is 28,800 seconds (eight hours). This setting applies to both remote access and site-to-site VPN.
seq-num	Specifies the number that you assign to the crypto map entry.

Command Default

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.1(2)	Added unlimited argument.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the ASA requests new security associations during security association negotiation, it specifies its crypto map lifetime values in the request to the peer; it uses these values as the lifetime of the new security associations. When the ASA receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

For site-to-site VPN connections, there are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached. For remote access VPN sessions, only the timed lifetime applies.

Note The ASA lets you change crypto map, dynamic map, and IPsec settings on-the-fly. If you do so, the ASA brings down only the connections affected by the change. If you change an existing access list associated with a crypto map, specifically by deleting an entry within the access list, the result is that only the associated connection is brought down. Connections based on other entries in the access list are not affected.

Note We recommend that you configure different security association timers on either side of the site-to-site IKEv2 tunnel to avoid the rekey collision.

To change the timed lifetime, use the **crypto map set security-association lifetime seconds** command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

Examples

The following command, entered in global configuration mode, specifies a security association lifetime in seconds and kilobytes for the crypto map mymap:

```
ciscoasa(config)# crypto
 map mymap 10 set security-association lifetime seconds 1400 kilobytes 3000000
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set tfc-packets

To enable dummy Traffic Flow Confidentiality (TFC) packets on an IPsec SA, use the **crypto map set tfc-packets** command in global configuration mode. To disable TFC packets on an IPsec SA, use the **no** form of this command.

crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]
no crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

Syntax Description

name	Specifies the name of the crypto map set.
priority	Specifies the priority that you assign to the crypto map entry.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command configures the existing DF policy (at an SA level) for the crypto map.

crypto map set transform-set

To specify the IKEv1 transform sets to use in a crypto map entry, use the **crypto map set transform-set** command in global configuration mode. To remove the names of the transform sets from a crypto map entry, use the **no** form of this command with the specified transform set name. To specify all or none of the transform sets and remove the crypto map entry, use the **no** form of the command.

crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*...transform-set-name11*]
no crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*...transform-set-name11*]
no crypto map *map-name seq-num* **set transform-set**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the sequence number that corresponds to the crypto map entry.
transform-set-name1transform-set-name11	Specifies one or more names of the transform sets. Any transform sets named in this command must be defined in the **crypto ipsec transform-set** command. Each crypto map entry supports up to 11 transform sets.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The maximum number of transform sets in a crypto map entry was modified.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This command is required for all crypto map entries.

The peer at the opposite end of the IPsec initiation uses the first matching transform set for the security association. If the local ASA initiates the negotiation, the order specified in the **crypto map** command determines the order in which the ASA presents the contents of the transform sets to the peer. If the peer initiates the negotiation, the local ASA uses the first transform set in the crypto map entry that matches the IPsec parameters sent by the peer.

If the peer at the opposite end of the IPsec initiation fails to match the values of the transform sets, IPsec does not establish a security association. The initiator drops the traffic because there is no security association to protect it.

To change the list of transform sets, specify a new list to replace the old one.

If you use this command to modify a crypto map, the ASA modifies only the crypto map entry with the same sequence number you specify. For example, the ASA inserts the transform set named 56des-sha in the last position if you enter the following commands:

```
ciscoasa(config)# crypto map map1 1 set transform-set
128aes-md5

128aes-sha

192aes-md5

ciscoasa(config)# crypto map map1 1 transform-set
56des-sha
ciscoasa(config)#
```

The response to the following command shows the cumulative effect of the previous two commands:

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

To reconfigure the sequence of transform sets in a crypto map entry, delete the entry, specifying both the map name and sequence number; then recreate it. For example, the following commands reconfigure the crypto map entry named map2, sequence 3:

```
asa2(config)# no crypto map map2 3 set transform-set

asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha 128aes-md5
asa2(config)#
```

Examples

The **crypto ipsec transform-set** (create or remove transform set) section shows ten transform set commands. The following example creates a crypto map entry named map2 consisting of the same ten transform sets:

```
ciscoasa(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5 56des-sha
 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

The following example, entered in global configuration mode, shows the minimum required crypto map configuration when the ASA uses IKE to establish the security associations:

```
ciscoasa(config)# crypto map
map2
 10 ipsec-isakmp
ciscoasa(config)# crypto map
map2
 10 match address 101
ciscoasa(config)# crypto map
map2
 set transform-set
3des-md5
```

```
ciscoasa(config)# crypto map map2 set peer 10.0.0.1
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.
clear configure crypto map	Clears all crypto maps from the configuration.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
crypto ipsec transform-set	Configures a transform set.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto map set trustpoint

To specify the trustpoint that identifies the certificate to send for authentication during Phase 1 negotiations for the crypto map entry, use the **crypto map set trustpoint** command in global configuration mode. To remove a trustpoint from a crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]
no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

Syntax Description

chain	(Optional) Sends a certificate chain. A CA certificate chain includes all CA certificates in a hierarchy of certificates from the root certificate to the identity certificate. The default value is disable (no chain).
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number that you assign to the crypto map entry.
trustpoint-name	Identifies the certificate to be sent during Phase 1 negotiations. The default is none.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This crypto map command is valid only for initiating a connection. For information on the responder side, see the **tunnel-group** commands.

Examples

The following example, entered in global configuration mode, specifies a trustpoint named tpoint1 for crypto map mymap and includes the chain of certificates:

```
ciscoasa(config)# crypto map mymap 10 set trustpoint tpoint1 chain
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel groups.

crypto map set validate-icmp-errors

To specify whether or not to validate incoming ICMP error messages received through an IPsec tunnel that are destined for an interior host on the private network, use the **crypto map set validate-icmp-errors** command in global configuration mode. To remove a trustpoint from a crypto map entry, use the **no** form of this command.

crypto map *name priority* **set validate-icmp-errors**
no crypto map *name priority* **set validate-icmp-errors**

Syntax Description

name	Specifies the name of the crypto map set.
priority	Specifies the priority that you assign to the crypto map entry.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This crypto map command is valid only for validating incoming ICMP error messages.

csc

To enable the ASA to send network traffic to the CSC SSM, use the csc command in class configuration mode. To remove the configuration, use the **no** form of this command.

csc { **fail-open | fail-close** }
nocsc

Syntax Description

fail-close	Specifies that the adaptive ASA should block traffic if the CSC SSM fails. This applies to the traffic selected by the class map only. Other traffic not sent to the CSC SSM is not affected by a CSC SSM failure.
fail-open	Specifies that the adaptive ASA should allow traffic if the CSC SSM fails. This applies to the traffic selected by the class map only. Other traffic not sent to the CSC SSM is not affected by a CSC SSM failure.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Class configuration mode is accessible from policy map configuration mode.

The **csc** command configures a security policy to send to the CSC SSM all traffic that is matched by the applicable class map. This occurs before the ASA allows the traffic to continue to its destination.

You can specify how the ASA treats matching traffic when the CSC SSM is not available to scan the traffic. The **fail-open** keyword specifies that the ASA permits the traffic to continue to its destination even though the CSC SSM is not available. The **fail-close** keyword specifies that the ASA never lets matching traffic continue to its destination when the CSC SSM is not available.

The CSC SSM can scan HTTP, SMTP, POP3, and FTP traffic. It supports these protocols only when the destination port of the packet requesting the connection is the well-known port for the protocol, that is, CSC SSM can scan only the following connections:

- FTP connections opened to TCP port 21
- HTTP connections opened to TCP port 80

- POP3 connections opened to TCP port 110
- SMTP connections opened to TCP port 25

If policies using the **csc** command select connections that misuse these ports for other protocols, the ASA passes the packets to the CSC SSM; however, the CSC SSM passes the packets without scanning them.

To maximize the efficiency of the CSC SSM, configure class maps used by policies implementing the **csc** command as follows:

- Select only the supported protocols that you that want the CSC SSM to scan. For example, if you do not want to scan HTTP traffic, be sure that service policies do not divert HTTP traffic to the CSC SSM.
- Select only those connections that risk trusted hosts protected by the ASA. These are connections from outside or untrusted networks to inside networks. We recommend scanning the following connections:
  - Outbound HTTP connections
  - FTP connections from clients inside the ASA to servers outside the ASA
  - POP3 connections from clients inside the ASA to servers outside the ASA
  - Incoming SMTP connections destined to inside mail servers

FTP Scanning

The CSC SSM supports scanning of FTP file transfers only if the primary channel for the FTP session uses the standard port, which is TCP port 21.

FTP inspection must be enabled for the FTP traffic that you want scanned by the CSC SSM. This is because FTP uses a dynamically assigned secondary channel for data transfer. The ASA determines the port assigned for the secondary channel and opens a pinhole to allow the data transfer to occur. If the CSC SSM is configured to scan FTP data, the ASA diverts the data traffic to the CSC SSM.

You can apply FTP inspection either globally or to the same interface that the **csc** command is applied to. By default, FTP inspection is enabled globally. If you have not changed the default inspection configuration, no further FTP inspection configuration is required to enable FTP scanning by the CSC SSM.

For more information about FTP inspection or the default inspection configuration, see the CLI configuration guide.

Examples

The ASA should be configured to divert traffic to CSC SSM requests from clients on the inside network for HTTP, FTP, and POP3 connections to the outside network and incoming SMTP connections from outside hosts to the mail server on the DMZ network. HTTP requests from the inside network to the web server on the DMZ network should not be scanned.

The following configuration creates two service policies. The first policy, csc_out_policy, is applied to the inside interface and uses the csc_out access list to ensure that all outbound requests for FTP and POP3 are scanned. The csc_out access list also ensures that HTTP connections from inside to networks on the outside interface are scanned, but the access list includes a deny ACE to exclude HTTP connections from inside to servers on the DMZ network.

The second policy, csc_in_policy, is applied to the outside interface and uses the csc_in access list to ensure that requests for SMTP and HTTP originating on the outside interface and destined for the DMZ network are scanned by the CSC SSM. Scanning HTTP requests protects the web server from HTTP file uploads.

```
ciscoasa(config)#access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
ciscoasa(config)#access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0 eq 80 ciscoasa(config)#access-list csc_out permit tcp 192.168.10.0 255.255.255.0
any eq 80 ciscoasa(config)#access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq
110 ciscoasa(config)# class-map csc_outbound_class ciscoasa(config-cmap)#match access-list
csc_out ciscoasa(config-cmap)# policy-map csc_out_policy ciscoasa(config-cmap)#class
csc_outbound_class ciscoasa(config-pmap-c)# csc fail-close ciscoasa(config)#service-policy
csc_out_policy interface insideciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0
255.255.255.0 eq 25 ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0
255.255.255.0 eq 80 ciscoasa(config)#class-map csc_inbound_class
ciscoasa(config-cmap)#match access-list csc_inciscoasa(config)# policy-map csc_in_policy
ciscoasa(config-pmap)#class csc_inbound_classciscoasa(config-pmap-c)# csc fail-close
ciscoasa(config)# service-policy csc_in_policy interface outside
```

Note FTP inspection must be enabled for the CSC SSM to scan files transferred by FTP. FTP inspection is enabled by default.

Related Commands

Commands	Description
class (policy-map)	Specifies a class map for traffic classification.
class-map	Creates a traffic classification map, for use with a policy map.
match port	Matches traffic using a destination port.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.

csd enable (Deprecated)

Note The last supported release of this command was Version 9.5(1).

To enable Cisco Secure Desktop (CSD) for clientless SSL VPN remote access or remote access using the Secure Client, use the csd enable command in webvpn configuration mode. To disable CSD, use the **no** form of this command.

csd enable
no csd enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated and replaced by the **hostscan** command.

Usage Guidelines

CSD is enabled or disabled globally for all remote access connection attempts made to the ASA with one exception.

The **csd enable** command does the following:

1. Provides a validity check that supplements the check performed by the previous csd image *path* command.
2. Creates an sdesktop folder on disk0: if one is not already present.
3. Inserts a data.xml (Cisco Secure Desktop configuration) file in the sdesktop folder if one is not already present.
4. Loads the data.xml from the flash device to the running configuration.
5. Enables CSD.

Note You can enter the **show webvpn csd** command to determine whether or not Cisco Secure Desktop is enabled.

- The csd image *path* command must be in the running configuration before you enter the **csd enable** command.
- The **no csd enable** command disables CSD in the running configuration. If CSD is disabled, you cannot access CSD Manager and remote users cannot use CSD.
- If you transfer or replace the data.xml file, disable and then enable CSD to load the file into the running configuration.
- CSD is enabled or disabled globally for all remote access connection attempts made to the ASA. You cannot enable or disable CSD for an individual connection profile or group policy.

Exception: Connection profiles for clientless SSL VPN connections can be configured so that CSD will not run on the client computer if the computer is attempting to connect to the ASA using a group URL and CSD is enabled globally. For example:

ciscoasa(config)# **tunnel-group***group-name***webvpn-attributes**

ciscoasa(config-tunnel-webvpn)# **group-url https://www.url-string.com**

ciscoasa(config-tunnel-webvpn)# without-csd

Examples

The following commands shows how to view the status of the CSD image and enable it:

```
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
csd image	Copies the CSD image named in the command from the flash drive specified in the path to the running configuration.
show webvpn csd	Identifies the version of CSD if it is enabled. Otherwise, the CLI indicates “Secure Desktop is not enabled.”
without-csd	Configures connection profiles for clientless SSL VPN sessions so that CSD will not run on the client computer if the computer is attempting to connect to the ASA using a group URL and CSD is enabled globally.

csd hostscan image (Deprecated)

Note The last supported release of this command was Version 9.5(1).

To install or upgrade the Cisco Host Scan distribution package and add it to the running configuration, use the csd hostscan image command in webvpn configuration mode. To remove the Host Scan distribution package from the running configuration, use the **no** form of this command:

csd hostscan image *path*
no csd hostscan image *path*

Syntax Description

path Specifies the path and filename of the Cisco Host Scan package, up to 255 characters.

The Host Scan package can be a standalone Host Scan package that can be downloaded from Cisco.com and has the file name convention, hostscan-version.pkg, or it can be the full Secure Client package that can also be downloaded from Cisco.com and has the file name convention, anyconnect-win-version-k9.pkg. When customers specify the Secure Client, the ASA extracts the Host Scan package from the Secure Client package and installs it.

The Host Scan package contains the Host Scan software as well as the Host Scan library and support charts.

This command cannot upload a CSD image. Use the **csd image** command for that operation.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.5(2)	This command was deprecated. It is replace by the command **hostscan image**.

Usage Guidelines

Enter the **show webvpn csd hostscan** command to determine the version of the Host Scan image that is currently installed and enabled.

After installing Host Scan with the **csd hostscan image** command, enable the image using the csd enable command.

Enter the **write memory** command to save the running configuration to ensure that the Host Scan image is available the next time that the ASA reboots.

Examples

The following commands show how to install a Cisco Host Scan package, enable it, view it, and save the configuration on the flash drive:

```
ciscoasa> en
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# csd hostscan image disk0:/hostscan_3.0.0333-k9.pkg

ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e
22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
show webvpn csd hostscan	Identifies the version of Cisco Host Scan if it is enabled. Otherwise, the CLI indicates “Secure Desktop is not enabled.”
csd enable	Enables CSD for management and remote user access.

csd image (Deprecated)



Note The last supported release of this command was Version 9.5(1).

To validate the Cisco Secure Desktop (CSD) distribution package and add it to the running configuration, effectively installing CSD, use the csd image command in webvpn configuration mode. To remove the CSD distribution package from the running configuration, use the **no** form of the command:

csd image *path*
no csd image *path*

Syntax Description

path	Specifies the path and filename of the CSD package, up to 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated and replaced by the **hostscan image** command.

Usage Guidelines

Enter the **show webvpn csd** command to determine whether or not the CSD image is enabled before entering this command. The CLI indicates the version of the CSD image that is currently installed if it is enabled.

Use the **csd image** command to install a new Cisco Secure Desktop image, or upgrade an existing image, after you download it to your computer, and transfer it to the flash drive. When downloading it, be sure to get the correct file for the ASA; it is in the form securedesktop_asa_<n>_<n>*.pkg.

Entering the **no csd image** command removes both management access to CSD Manager and remote user access to CSD. The ASA does not make any changes to the CSD software and the CSD configuration on the flash drive when you enter this command.

Note Enter the **write memory** command to save the running configuration to ensure CSD is available the next time that the ASA reboots.

Examples

The following commands show how to view the current CSD distribution package, view the contents of the flash file system, and upgrade to a new version:

```
ciscoasa# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg
38600704 bytes available (24281088 bytes used)
******** Flash Card Geometry/Format Info ********
COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184
COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
ciscoasa(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6
19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
show webvpn csd	Identifies the version of CSD if it is enabled. Otherwise, the CLI indicates “Secure Desktop is not enabled.”
csd enable	Enables CSD for management and remote user access.

ctl

To enable the Certificate Trust List (CTL) provider to parse the CTL file from the CTL client and install trustpoints, use the ctl command in ctl provider configuration mode. To remove the configuration, use the **no** form of this command.

ctl install
no ctl install

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl provider configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the ctl command in ctl provider configuration mode to enable the CTL provider to parse the CTL file from the CTL client and install trustpoints for entries from the CTL file. Ttrustpoints installed by this command have names prefixed with "_internal_CTL_<ctl_name>."

If this command is disabled, each CallManager server and CAPFs certificate must be manually imported and installed via the crypto ca trustpoint and crypto ca certificate chain commands.

Examples

The following example shows how to create a CTL provider instance:

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.

Commands	Description
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

ctl-file (Deprecated)

To specify the CTL instance to create for a phone proxy or to parse the CTL file stored in flash memory, use the **ctl-file** command in global configuration mode. To specify the CTL instance to use when configuring the Phone Proxy, use the **ctl-file** command in phone-proxy configuration mode. To remove the CTL instance, use the **no** form of this command.

ctl-file*ctl_name*
no ctl-file *ctl_name* [**noconfirm**]

Syntax Description

ctl_name	Specifies the name of the CTL instance.
noconfirm	(Optional, global mode only.) Used with the **no** command, stops warnings about deleting trustpoints when the CTL file is removed from being printed to the ASA console.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

If users have phones that require LSC provisioning, you must also import the CAPF certificate into the ASA from the CUMC when configuring the CTL file instance with the **ctl-file** command.

Note To create the CTL file, use the **no shutdown** command in the ctl file configuration mode. To modify or add entries to a CTL file or to delete a CTL file, use the **shutdown** command.

Using the **no** form of the command removes the CTL file and all enrolled trustpoints internally created by a phone proxy. Additionally, removing the CTL file deletes all certificates received from the related certificate authority.

Examples

The following example shows how to configure the CTL file for the phone proxy feature:

```
ciscoasa
(config)#
ctl-file myctl
```

The following example shows the use of the **ctl-file** command to configure the CTL file for the Phone Proxy feature in phone proxy mode:

```
ciscoasa
(config-phone-proxy)#
ctl-file myctl
```

Related Commands

Command	Description
ctl-file (phone-proxy)	Specifies the CTL file to use when configuring the phone proxy instance.
cluster-ctl-file	Parses the CTL file stored in flash memory to install the trustpoints from that file.
phone-proxy	Configures the phone proxy instance.
record-entry	Specifies the trustpoints to be used for the creation of the CTL file.
sast	Specifies the number of SAST certificates to create in the CTL record.

ctl-provider

To configure a CTL provider instance in CTL provider mode, use the ctl-provider command in global configuration mode. To remove the configuration, use the **no** form of this command.

ctl-provider *ctl_name*
no ctl-provider *ctl_name*

Syntax Description

ctl_name	Specifies the name of the CTL provider instance.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the ctl-provider command to enter CTL provider configuration mode to create a CTL provider instance.

Examples

The following example shows how to create a CTL provider instance:

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and the username and password for client authentication.
ctl	Parses the CTL file from the CTL client and install trustpoints.
export	Specifies the certificate to be exported to the client.
service	Specify the port to which the CTL provider listens.

Commands	Description
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

cts import-pac

To import a Protected Access Credential (PAC) file from the Cisco ISE, use the **cts import-pac** command in global configuration mode:

cts import-pac *filepath* **password** *value*

Syntax Description

filepath	Specifies one of the following **exec** mode commands and options:. **Single Mode** • **disk0**: Path and filename on disk0 • **disk1**: Path and filename on disk1 • **flash**: Path and filename on flash • **ftp**: Path and filename on FTP • **http**: Path and filename on HTTP • **https**: Path and filename on HTTPS • **smb**: Path and filename on SMB • **tftp**: Path and filename on TFTP **Multi-mode** • **http**: Path and filename on HTTP • **https**: Path and filename on HTTPS • **smb**: Path and filename on SMB • **tftp**: Path and filename on TFTP
password *value*	Specifies the password used to encrypt the PAC file. The password is independent of the password that was configured on the ISE as part of the device credentials. The password must match the one provided when the PAC file was requested, and is necessary to decrypt the PAC data. This password is not related to the one that is configured on the ISE as part of the device credentials.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Importing the PAC file to the ASA establishes the connection with the ISE. After the channel is established, the ASA initiates a secure RADIUS transaction with the ISE and downloads Cisco TrustSec environment data; specifically, the ASA downloads the security group table. The security group table maps SGTs to security group names. Security group names are created on the ISE and provide user-friendly names for security groups. No channel is established prior to the RADIUS transaction. The ASA initiates a RADIUS transaction with the ISE using the PAC for authentication.

Tip The PAC file contains a shared key that allows the ASA and ISE to secure the RADIUS transactions that occur between them. Given the sensitive nature of this key, it must be stored securely on the ASA.

After successfully importing the file, the ASA download Cisco TrustSec environment data from the ISE without requiring the device password configured in the ISE.

The ASA stores the PAC file in an area of NVRAM that is not accessible through the user interface.

Prerequisites

- The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can generate a PAC file. The ASA can import any PAC file but it will only work on the ASA when the file was generated by a properly configured ISE.
- Obtain the password used to encrypt the PAC file when generating it on the ISE.

The ASA requires this password to import and decrypt the PAC file.

- Access to the PAC file generated by the ISE. The ASA can import the PAC file from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC file does not have to reside on the ASA flash before you can import it.)
- The server group has been configured for the ASA.

Restrictions

- When the ASA is part of an HA configuration, you must import the PAC file to the primary ASA device.
- When the ASA is part of a clustering configuration, you must import the PAC file to the master device.

Examples

The following example imports a PAC from the ISE:

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

Related Commands

Command	Description
cts refresh environment-data	Refreshes the Cisco TrustSec environment data from the ISE when the ASA is integrated with Cisco TrustSec
cts sxp enable	Enables the SXP protocol on the ASA.

cts manual

To enable SGT plus Ethernet Tagging (also called Layer 2 SGT Imposition) and enter cts manual interface configuration mode, use the **cts manual** command in interface configuration mode. To disable SGT plus Ethernet Tagging, use the **no** form of this command.

cts manual
no cts manual

Syntax Description

This command has no arguments or key words.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command enables Layer 2 SGT Imposition and enters cts manual interface configuration mode.

Restrictions

- Supported only on physical interfaces, VLAN interfaces, port channel interfaces, and redundant interfaces.
- Not supported on logical interfaces or virtual interfaces, such as BVI, TVI, and VNI.
- Does not support failover links.
- Does not support cluster control links.

Examples

The following example enables Layer 2 SGT Imposition and enters cts manual interface configuration mode:

```
ciscoasa(config-if)# cts
 manual
ciscoasa(config-if-cts-manual)#
```

Related Commands

Command	Description
policy static sgt	Applies a policy to a manually configured CTS link.
propagate sgt	Enables propagation of a security group tag (called **sgt**) on an interface.

cts refresh environment-data

To refresh the Cisco TrustSec environment data from the ISE and reset the reconcile timer to the configured default value, use the **cts refresh environment-data** command in global configuration mode:

cts refresh environment-data

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

When the ASA is integrated with Cisco TrustSec, the ASA downloads environment data from the ISE, which includes the Security Group Tag (SGT) name table. The ASA automatically refreshes its environment data obtained from the ISE when you complete the following tasks on the ASA:

- Configure a AAA server to communicate with the ISE.
- Import a PAC file from the ISE.
- Identify the AAA server group that the ASA will use for retrieval of Cisco TrustSec environment data.

Normally, you will not need to manually refresh the environment data from the ISE; however, security groups can change on the ISE. These changes are not reflected on the ASA until you refresh the data in the ASA security group table. Refresh the data on the ASA to make sure any security group made on the ISE are reflected on the ASA.

Tip We recommend that you schedule policy configuration changes on the ISE and the manual data refresh on the ASA during a maintenance window. Handling policy configuration changes in this way maximizes the chances of security group names getting resolved and security policies becoming active immediately on the ASA.

Prerequisites

The ASA must be configured as a recognized Cisco TrustSec network device in the ISE and the ASA must have successfully imported a PAC file, so that the changes made for Cisco TrustSec are applied to the ASA.

Restrictions

- When the ASA is part of an HA configuration, you must refresh the environment data on the primary ASA device.
- When the ASA is part of a clustering configuration, you must refresh the environment data on the master device.

Examples

The following example downloads the Cisco TrustSec environment data from the ISE:

```
ciscoasa(config)# cts
 refresh
 environment-data
```

Related Commands

Command	Description
cts import-pac	Imports a Protected Access Credential (PAC) file from the Cisco ISE when the ASA is integrated with Cisco TrustSec.
cts sxp enable	Enables the SXP protocol on the ASA.

cts role-based sgt-map

To configure IP-SGT bindings manually, use the **cts role-based sgt-map** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cts role-based sgt-map { *IPv4_addr* [/ *mask*] | *IPv6_addr* [/ *prefix*] } **sgt** *sgt_value*
no cts role-based sgt-map { *IPv4_addr* [/ *mask*] | *IPv6_addr* [/ *prefix*] } **sgt** *sgt_value*

Syntax Description

IPv4_addr [/*mask*]	Specifies the IPv4 address to be used. Add a subnet mask in CIDR format to create a mapping for a subnet; for example, 10.100.10.0/24.
IPv6_addr [/*prefix*]	Specifies the IPv6 address to be used. Add a prefix to create a mapping for an IPv6 network.
sgt *sgt_value*	Specifies the SGT number that the IP address maps to. Valid values are from 2-65519.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.
9.6(1)	The ability to add mappings for subnets was added.

Usage Guidelines

This command enables you to configure IP-SGT bindings manually.

Examples

The following example configures an IP-SGT binding table entry:

```
ciscoasa(config)#
cts role-based sgt-map 10.2.1.2 sgt 50
```

Related Commands

Command	Description
clear configure cts role-based [**sgt-map**]	Removes the user-defined IP-SGT binding table entries.

Command	Description
show running-config [**all**] **cts role-based [sgt-map]**	Displays the user-defined IP-SGT binding table entries.

cts server-group

To identify the AAA server group that the ASA uses to integrate with Cisco TrustSec for environment data retrieval, use the **cts server-group** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts server-group *aaa-server-group-name*
no cts server-group [*aaa-server-group-name*]

Syntax Description

aaa-server-group-name	Specifies the name of an existing, locally configured AAA server group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

As part of configuring the ASA to integrate with Cisco TrustSec, you must configure the ASA so that it can communicate with the ISE. Only one instance of the server group can be configured on the ASA for Cisco TrustSec.

Prerequisites

- The referenced server group must be configured to use the RADIUS protocol. If you add a non-RADIUS server group to the ASA, the feature configuration will fail.
- If the ISE is also used for user authentication, obtain the shared secret that was entered on the ISE when you registered the ASA with the ISE. Contact your ISE administrator if you do not have this information.

Examples

The following example locally configures on the ASA the AAA server group for the ISE and configures the ASA to use that AAA server group for the ASA integration with Cisco TrustSec:

```
ciscoasa(config)#
aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)#
aaa-server ISEserver (inside) host 192.0.2.1
```

```
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
cts server-group ISEserver
```

Related Commands

Command	Description
aaa-server *server-tag* **protocol radius**	Creates the AAA server group and configures the AAA server parameters for the ASA to communicate with the ISE server; where *server-tag* specifies the server group name.
aaa-server *server-tag* (*interface-name*) **host** *server-ip*	Configures a AAA server as part of a AAA server group and sets host-specific connection data; where (*interface-name*) specifies the network interface where the ISE server resides, and *server-tag* is the name of the AAA server group for the Cisco TrustSec integration, and e *server-ip* specifies the IP address of the ISE server.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp connection peer

To set up an SXP connection to an SXP peer, use the **cts sxp connection peer** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** { **default** | **mode** } [**mode** { **local** | **peer** }] { **speaker** | **listener** }
no cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** { **default** | **mode** } [**mode** { **local** | **peer** }] { **speaker** | **listener** }

Syntax Description

default	Used with the **password** keyword. Specifies to use the default password configured for SXP connections.
listener	Specifies that the ASA functions as a listener for the SXP connection; meaning that the ASA can receive IP-SGT mappings from downstream devices. Specifying a speaker or listener role for the ASA for the SPX connection is required.
local	Used with the **mode** keyword. Species to use the local SXP device.
mode	(Optional) Specifies the mode of the SXP connection.
none	Used with the **password** keyword. Specifies not to use a password for the SXP connection.
password	(Optional) Specifies whether to use the authentication key for the SXP connection.
peer	Used with the **mode** keyword. Species to use the peer SXP device.
peer_ip_address	Specifies the IPv4 or IPv6 address of the SXP peer. The peer IP address must be reachable from the ASA outgoing interface.
source *source_ip_address*	(Optional) Specifies the local IPv4 or IPv6 address of the SXP connection.
speaker	Specifies that the ASA functions as a speaker for the SXP connection; meaning that the ASA can forward IP-SGT mappings to upstream devices. Specifying a speaker or listener role for the ASA for the SPX connection is required.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

SXP connections between peers are point-to-point and use TCP as the underlying transport protocol. SXP connections are set per IP address; a single device pair can service multiple SXP connections.

Restrictions

- The ASA does not support per-connection passwords for SXP connection.
- When you use the **cts sxp default password to configure a default SXP password, you should configure the SXP connection to use the default password; conversely, when you do not configure a default password, you should not configure a default password for the SXP connection. If you do not follow these two guidelines, SXP connections can fail.**
- When you configure an SXP connection with a default password, but the ASA does not have default password configured, the SXP connection will fail.
- When you configure a source IP address for an SXP connection, you must specify the same address as the ASA outbound interface. If the source IP address does not match the address of the outbound interface, the SXP connection will fail.

When the source IP address for an SXP connection is not configured, the ASA performs a route/ARP lookup to determine the outbound interface for the SXP connection. We recommend that you do not configure a source IP address for SXP connection and allow the ASA to perform a route/ARP lookup to determine the source IP address for the SXP connection.

- Configuring an IPv6 local link address for an SXP peer or source is not supported.
- Configuring multiple IPv6 addresses on the same interface for SXP connections is not supported.

Examples

The following example creates an SXP connection on the ASA:

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100
source 192.168.1.1 password default mode peer speaker
```

Related Commands

Command	Description
cts sxp default password	Specifies the default password for SXP connectios.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp default password

To configure a default password for TCP MD5 authentication with SXP peers, use the **cts sxp default password** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp default password [**0** | **8**] *password*
no cts sxp default password [**0** | **8**] *password*

Syntax Description

0	(Optional) Specifies that the default password use unencrypted cleartext for the encryption level. You can only set one encryption level for the default password.
8	(Optional) Specifies that the default password use encrypted text for the encryption level.
password	Specifies an encrypted string up to 162 characters or an ASCII key string up to 80 characters.

Command Default

By default, SXP connections do not have a password set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

When you configure an SXP connection with a default password, but the ASA does not have default password configured, the SXP connection will fail.

Restrictions

- The ASA does not support per-connection passwords for SXP connection.
- When you use the **cts sxp default password to configure a default SXP password, you should configure the SXP connection to use the default password; conversely, when you do not configure a default password, you should not configure a default password for the SXP connection. If you do not follow these two guidelines, SXP connections can fail.**

Examples

The following example shows how to set default values for all SXP connections, including a default password for SXP connections:

```
ciscoasa(config)# cts sxp enable
```

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer. Specifying the **password default** keywords with this command, enables the use of the default password for that SXP connection.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp default source-ip

To configure a default local IP address for SXP connections, use the **cts sxp default source-ip** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp default source-ip *ipaddress*
no cts sxp default source-ip *ipaddress*

Syntax Description

ipaddress	Specifies an IPv4 or IPv6 address for the source IP address.

Command Default

By default, there is no default source IP address set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

When you configure a default source IP address for SXP connections, you must specify the same address as the ASA outbound interface. If the source IP address does not match the address of the outbound interface, SXP connections will fail.

When a source IP address for an SXP connection is not configured, the ASA performs a route/ARP lookup to determine the outbound interface for the SXP connection. We recommend that you do not configure a default source IP address for SXP connections and allow the ASA to perform a route/ARP lookup to determine the source IP address for an SXP connection.

Examples

The following example shows how to set default values for all SXP connections, including a default source IP address for SXP connections:

```
ciscoasa(config)# cts sxp enable

ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA. Specifying the **source** *source_ip_address* keyword and argument with this command, enables the use of the default source IP address for that SXP connection.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp delete-hold-down period

To configure the delete-hold-down timer for the IP-SGT mappings learned from a peer after an SXP peer terminates its SXP connection, use the **cts sxp delete-hold-down period** command in global configuration mode. To reset the timer to the default value, use the **no** form of this command.

cts sxp delete-hold-down period *timervalue*
no cts delete-hold-down period

Syntax Description

timervalue	Specifies the number of seconds, 120-64000, that IP-SGT mappings learned from a torn-down SXP connection are held before being deleted.

Command Default

By default, the *timervalue* is 120 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.8(3)	This command was added.

Usage Guidelines

Each SXP connection is associated with a delete hold down timer. This timer is triggered when an SXP connection on the listener side is torn down. The IP-SGT mappings learned from this SXP connection are not deleted immediately. Instead, they are held until the delete hold down timer expires. The mappings are deleted upon the expiry of this timer.

Examples

The following example shows how to set the delete-hold-down period.

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp enable

To enable the SXP protocol on the ASA, use the **cts sxp enable** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp enable
no cts sxp enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the SXP protocol is disabled on the ASA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example enables the SXP protocol on the ASA:

```
ciscoasa(config)# cts sxp enable
```

Related Commands

Command	Description
clear cts	Clears data used by the ASA when integrated with Cisco TrustSec.
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer.

cts sxp mapping network-map

To configure the depth of IPv4 subnet expansion when acting as a speaker to peers that use SXPv2 or lower, use the **cts sxp mapping network-map** command in global configuration mode. To remove the configuration, use the **no** form of this command.

cts sxp mapping network-map *maximum_hosts*
no cts sxp mapping network-map *maximum_hosts*

Syntax Description

maximum_hosts	The maximum number of host bindings that can be expanded from a network binding, from 0 to 65535. The default is 0.

Command Default

By default, no expansion is done.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If a listener peer uses SXPv2 or lower, the peer cannot understand SGT to subnet bindings. The ASA can expand the IPv4 subnet bindings to individual host bindings (IPv6 bindings are not expanded). This command specifies the maximum number of host bindings that can be generated from a subnet binding. If all listener peers are using SXPv3 or higher, or the ASA is the listener, this command has no impact.

Examples

The following example allows subnet mappings to be expanded to as many as 1000 host bindings:

```
ciscoasa(config)#
cts sxp mapping network-map 1000
```

Related Commands

Command	Description
cts sxp connection peer	Configures Trustsec peers.

cts sxp reconciliation period

To start a hold down timer after an SXP peer terminates its SXP connection, use the **cts sxp reconciliation period** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp reconciliation period *timervalue*
no cts sxp reconciliation period [*timervalue*]

Syntax Description

timervalue	Specifies the default value for the reconciliation timer. Enter the number of seconds in the range of 1 to 64000 seconds.

Command Default

By default, the *timervalue* is 120 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

After an SXP peer terminates its SXP connection, the ASAstarts a hold down timer. If an SXP peer connects while the hold down timer is running, the ASA starts the reconciliation timer; then, the ASA updates the SXP mapping database to learn the latest mappings.

When the reconciliation timer expires, the ASA scans the SXP mapping database to identify stale mapping entries (entries that were learned in a previous connection session). The ASA marks these connections as obsolete. When the reconciliation timer expires, the ASA removes the obsolete entries from the SXP mapping database.

You cannot specify 0 for the timer because specifying 0 would prevent the reconciliation timer from starting. Not allowing the reconciliation timer to run would keep stale entries for an undefined time and cause unexpected results from the policy enforcement.

Examples

The following example shows how to set default values for all SXP connections, including a default reconciliation timer:

```
ciscoasa(config)# cts sxp enable

ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

```
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer.
cts sxp enable	Enables the SXP protocol on the ASA.

cts sxp retry period

To specify the default time interval between ASA attempts to set up new SXP connections between SXP peers., use the **cts sxp retry period** command in global configuration mode. To disable support for the command, use the **no** form of this command.

cts sxp retry period *timervalue*
no cts sxp retry period [*timervalue*]

Syntax Description

timervalue	Specifies the default value for the retry timer. Enter the number of seconds in the range of 0 to 64000 seconds.

Command Default

By default, the *timervalue* is 120 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Specifies the default time interval between ASA attempts to set up new SXP connections between SXP peers. The ASA continues to make connection attempts until a successful connection is made.

The retry timer is triggered as long as there is one SXP connection on the ASA that is not up.

If you specify 0 seconds, the timer never expires and the ASA will not attempt to connect to SXP peers.

When the retry timer expires, the ASA goes through the connection database and if the database contains any connections that are off or in a “pending on” state, the ASA restarts the retry timer.

We recommend you configure the retry timer to a different value from its SXP peer devices.

Examples

The following example shows how to set default values for all SXP connections, including a default retry period:

```
ciscoasa(config)# cts sxp enable

ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

Related Commands

Command	Description
cts sxp connection peer	Configures an SXP connection for the ASA to an SXP peer.
cts sxp enable	Enables the SXP protocol on the ASA.

customization

To specify the customization to use for a tunnel group, group, or user, use the **customization** command in tunnel-group webvpn-attributes configuration mode or webvpn configuration mode. To not specify a customization, use the **no** form of this command.

customization*name*
no customization *name*
customization { **none** | **value** *name* }
no customization { **none** | **value** *name* }

Syntax Description

name	Specifies the name of the WebVPN customization to apply to a group or user.
none	Disables customization for the group or user, and prevents the customization from being inherited.
value *name*	Specifies the name of a customization to apply to the group policy or user.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn-attributes configuration	• Yes	—	• Yes	—	—
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Before entering the **customization** command in tunnel-group webvpn-attributes configuration mode, you must name and configure the customization using the **customization** command in webvpn configuration mode.

Mode-Dependent Command Options

The keywords available with the **customization** command differ depending on the mode you are in. In group-policy attributes configuration mode and username attributes configuration mode, the additional keywords **none** and **value** appear.

For example, if you enter the **customization none** command from username attributes configuration mode, the ASA will not look for the value in the group policy or tunnel group.

Examples

The following example shows a command sequence that first establishes a WebVPN customization named “123” that defines a password prompt. The example then defines a WebVPN tunnel group named “test” and uses the **customization** command to specifies the use of the WebVPN customization named “123”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization 123
ciscoasa(config-webvpn-custom)# password-prompt Enter password
ciscoasa(config-webvpn)# exit
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# customization 123
ciscoasa(config-tunnel-webvpn)#
```

The following example shows the customization named “cisco” applied to the group policy named “cisco_sales.” Note that the additional command option **value** is required with the **customization** command entered in group-policy attributes configuration mode via webvpn configuration mode:

```
ciscoasa(config)# group-policy
 cisco_sales attributes
ciscoasa(config-group-policy)#  webvpn
ciscoasa(config-group-webvpn)# customization value cisco
```

Related Commands

Command	Description
clear configure tunnel-group	Removes all tunnel group configuration.
show running-config tunnel-group	Displays the current tunnel group configuration.
tunnel-group webvpn-attributes	Enters the webvpn configuration mode for configuring WebVPN tunnel group attributes.

cxsc

To redirect traffic to the ASA CX module, use the **cxsc** command in class configuration mode. To remove the ASA CX action, use the **no** form of this command.

cxsc { **fail-close** | **fail-open** } [**auth-proxy** | **monitor-only**]
no cxsc { **fail-close** | **fail-open** } [**auth-proxy** | **monitor-only**]

Syntax Description

auth-proxy	(Optional) Enables the authentication proxy, which is required for active authentication.
fail-close	Sets the ASA to block all traffic if the ASA CX module is unavailable.
fail-open	Sets the ASA to allow all traffic through, uninspected, if the ASA CX module is unavailable.
monitor-only	For demonstration purposes only, specify **monitor-only** to send a read-only copy of traffic to the ASA CX module. When you configure this option, you see a warning message similar to the following: `WARNING: Monitor-only mode should be used for demonstrations and evaluations only. This mode prevents CXSC from denying or altering traffic.`

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(4.1)	This command was added.
9.1(2)	We added the **monitor-only** keyword to support demonstration functionality.
9.1(3)	You can now configure ASA CX policies per context.

Usage Guidelines

You can access the class configuration mode by first entering the policy-map command.

Before or after you configure the **cxsc** command on the ASA, configure the security policy on the ASA CX module using Cisco Prime Security Manager (PRSM).

To configure the **cxsc** command, you must first configure the **class-map** command, **policy-map** command, and the **class** command.

Traffic Flow

The ASA CX module runs a separate application from the ASA. It is, however, integrated into the ASA traffic flow. When you apply the **cxsc** command for a class of traffic on the ASA, traffic flows through the ASA and the ASA CX module in the following way:

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the ASA CX module over the backplane.
5. The ASA CX module applies its security policy to the traffic and takes appropriate actions.
6. Valid traffic is sent back to the ASA over the backplane; the ASA CX module might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the ASA.

Information About Authentication Proxy

When the ASA CX needs to authenticate an HTTP user (to take advantage of identity policies), you must configure the ASA to act as an authentication proxy: the ASA CX module redirects authentication requests to the ASA interface IP address/proxy port. By default, the port is 885 (user configurable with the **cxsc auth-proxy port** command). Configure this feature as part of the service policy to divert traffic from the ASA to the ASA CX module. If you do not enable the authentication proxy, only passive authentication is available.

Compatibility with ASA Features

The ASA includes many advanced application inspection features, including HTTP inspection. However, the ASA CX module provides more advanced HTTP inspection than the ASA provides, as well as additional features for other applications, including monitoring and controlling application usage.

To take full advantage of the ASA CX module features, see the following guidelines for traffic that you send to the ASA CX module:

- Do not configure ASA inspection on HTTP traffic.
- Do not configure Cloud Web Security (ScanSafe) inspection. If you configure both the ASA CX action and Cloud Web Security inspection for the same traffic, the ASA only performs the ASA CX action.
- Other application inspections on the ASA are compatible with the ASA CX module, including the default inspections.
- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA CX module.
- Do not enable ASA clustering; it is not compatible with the ASA CX module.
- If you enable failover, when the ASA fails over, any existing ASA CX flows are transferred to the new ASA, but the traffic is allowed through the ASA without being acted upon by the ASA CX module. Only new flows recieved by the new ASA are acted upon by the ASA CX module.

Monitor-Only Mode

For testing and demonstration purposes, you can configure the ASA to send a duplicate stream of read-only traffic to the ASA CX module using the **monitor-only** keyword, so you can see how the module inspects the

traffic without affecting the ASA traffic flow. In this mode, the ASA CX module inspects the traffic as usual, makes policy decisions, and generates events. However, because the packets are read-only copies, the module actions do not affect the actual traffic. Instead, the module drops the copies after inspection.

See the following guidelines:

- You cannot configure both monitor-only mode and normal inline mode at the same time on the ASA. Only one type of security policy is allowed.
- The following features are not supported in monitor-only mode:
  - Deny policies
  - Active authentication
  - Decryption policies
- The ASA CX does not perform packet buffering in monitor-only mode, and events will be generated on a best effort basis. For example, some events, such as ones with long URLs spanning packet boundaries, may be impacted by the lack of buffering.
- Be sure to configure both the ASA policy and the ASA CX to have matching modes: both in monitor-only, or both in normal inline mode.

Examples

The following example diverts all HTTP traffic to the ASA CX module and blocks all HTTP traffic if the ASA CX module card fails for any reason:

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the ASA CX module and allows all traffic through if the ASA CX module fails for any reason:

```
ciscoasa(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list my-cx-acl
ciscoasa(config)# class-map my-cx-class2
ciscoasa(config-cmap)# match access-list my-cx-acl2
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap)# class my-cx-class2
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy interface outside
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.

Command	Description
cxsc auth-proxy port	Sets the authentication proxy port.
debug cxsc	Enables ASA CX debugging messages.
hw-module module password-reset	Resets the module password to the default.
hw-module module reload	Reloads the module.
hw-module module reset	Performs a reset and then reloads the module.
hw-module module shutdown	Shuts down the module.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
session do get-config	Gets the module configuration.
session do password-reset	Resets the module password to the default.
session do setup host ip	Configures the module management address.
show asp table classify domain cxsc	Shows the NP rules created to send traffic to the ASA CX module.
show asp table classify domain cxsc-auth-proxy	Shows the NP rules created for the authentication proxy for the ASA CX module.
show module	Shows the module status.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Shows service policy statistics.

cxsc auth-proxy port

To set the authentication proxy port for ASA CX module traffic, use the **cxsc auth-proxy port** command in global configuration mode. To set the port to the default, use the **no** form of this command.

cxsc auth-proxy port *port*
no cxsc auth-proxy port [*port*]

Syntax Description

port *port*	Sets the authentication proxy port to a value higher than 1024. The default is 885.

Command Default

The default port is 885.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(4.1)	This command was added.
9.1(3)	You can now configure ASA CX policies per context.

Usage Guidelines

If you enable the authentication proxy when you configure the **cxsc** command, you can change the port using this command.

When the ASA CX needs to authenticate an HTTP user (to take advantage of identity policies), you must configure the ASA to act as an authentication proxy: the ASA CX module redirects authentication requests to the ASA interface IP address/proxy port. By default, the port is 885. Configure this feature as part of the service policy to divert traffic from the ASA to the ASA CX module. If you do not enable the authentication proxy, only passive authentication is available.

Examples

The following example enables the authentication proxy for ASA CX traffic, then changes the port to 5000:

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
```

```
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
ciscoasa(config)# cxsc auth-port 5000
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
cxsc	Redirects traffic to the ASA CX module.
debug cxsc	Enables ASA CX debug messages.
hw-module module password-reset	Resets the module password to the default.
hw-module module reload	Reloads the module.
hw-module module reset	Performs a reset, and then reloads the module.
hw-module module shutdown	Shuts down the module.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
session do get-config	Gets the module configuration.
session do password-reset	Resets the module password to the default.
session do setup host ip	Configures the module management address.
show asp table classify domain cxsc	Shows the NP rules created to send traffic to the ASA CX module.
show asp table classify domain cxsc-auth-proxy	Shows the NP rules created for the authentication proxy for the ASA CX module.
show module	Shows the module status.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Shows service policy statistics.



PART III

D Commands

- da – dg, on page 1155
- dh – dm, on page 1219
- dn – dz, on page 1313



da – dg

- database path, on page 1156
- data-plane quick-reload, on page 1158
- ddns, on page 1159
- ddns update, on page 1161
- ddns update method, on page 1163
- debug, on page 1166
- default (crl configure), on page 1168
- default (interface), on page 1169
- default (ipv6 router ospf), on page 1170
- default (parameters), on page 1172
- default (time-range), on page 1174
- default-acl, on page 1176
- default-domain, on page 1178
- default enrollment, on page 1180
- default-group-policy (imap4s, pop3s, smtps) (Deprecated), on page 1181
- default-group-policy (tunnel-group general-attributes), on page 1184
- default-idle-timeout, on page 1186
- default-information, on page 1188
- default-information originate, on page 1189
- default-information originate (address-family), on page 1193
- default-information originate (ipv6 router ospf, router ospf), on page 1195
- default-information originate (router rip), on page 1197
- default-language, on page 1198
- default-mapping-rule, on page 1199
- default-mcast-group, on page 1201
- default-metric, on page 1204
- default user group, on page 1206
- delay, on page 1208
- delete, on page 1210
- deny-message, on page 1212
- deny version, on page 1214
- description, on page 1216

database path

To specify a path or location for the local CA server database, use the **database** command in ca server configuration mode. To reset the path to flash memory, the default setting, use the **no** form of this command.

[**no**] **database path** *mount-name directory-path*

Syntax Description

directory-path	Specifies the path to a directory on the mount point where the CA files are stored.
mount-name	Specifies the mount name.

Command Default

By default, the CA server database is stored in flash memory.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The local CA files stored in the database include the certificate database, user database files, temporary PKCS12 files, and the current CRL file. The *mount-name* argument is the same as the *name* argument for the **mount** command that is used to specify a file system for the ASA.

Note These CA files are internal, stored files and should not be modified.

Examples

The following example defines the mount point for the CA database as cifs_share and the database files directory on the mount point as ca_dir/files_dir:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# database path cifs_share ca_dir/files_dir/
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows the user to configure and manage a local CA.
crypto ca server user-db write	Writes the user information configured in the local CA database to disk.
debug crypto ca server	Shows debugging messages when the user configures the local CA server.
mount	Makes the Common Internet File System (CIFS) and/or File Transfer Protocol file systems (FTPFS) accessible to the ASA.
show crypto ca server	Displays the characteristics of the CA configuration on the ASA.
show crypto ca server cert-db	Displays the certificates issued by the CA server.

data-plane quick-reload

To quickly reload the data-plane and resynchronize with adjacent processes, use the **data-plane quick-reload** command. To remove the quick reload option, use the **no** form of this command.

[**no**] **data-plane quick-reload**

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the quick reload of the data plane is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration Mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.20(2)	This command was added.

Usage Guidelines

When you want to reload the data plane process rather than a reboot of the device, you can use the **data-plane quick-reload** command. When data plane quick reload is enabled, it restarts the data plane and also the following processes:

- SNORT2/SNORT3/PDTS.
- SNMPD—Restarted if already running
- SYSLOGD—Restarted if already running
- LICENCE SMART AGENT—Restarted if already running
- OFFLOAD APP—Restarted and all flows are flushed
- SERVICE MANAGER—Re-registers with service manager

However, when lina crash occurs during a boot up, the device aborts the quick restart and instead follows the normal device reload/reboot sequence. This exception is done to avoid continuous looping of the quick restart process.

Related Commands

Command	Description
show data-plane quick-reload status	Displays the status of the reload of the data plan.

ddns

To specify a Dynamic DNS (DDNS) update method type, use the **ddns** command in ddns-update-method mode. To remove an update method type from the running configuration, use the **no** form of this command.

ddns [**both**]
no ddns [**both**]

Syntax Description

both	(Optional) Specifies updates to both the DNS A and PTR resource records (RRs).

Command Default

Update only the DNS A RRs.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ddns-update-method	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method in this release.

Name and address mappings are contained in two types of RRs:

- The A resource record contains domain name-to-IP address mapping.
- The PTR resource record contains IP address-to-domain name mapping.

DDNS updates can be used to maintain consistent information between the DNS A and PTR RR types.

When issued in ddns-update-method configuration mode, the **ddns** command defines whether the update is just to a DNS A RR, or to both DNS A and PTR RR types.

Examples

The following example configures updates to both the DNS A and PTR RRs for the DDNS update method named ddns-2:

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# ddns both
```

Related Commands

Command	Description
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update

To associate a dynamic DNS (DDNS) update method with an ASA interface or an update hostname, use the **ddns update** command in interface configuration mode. To remove the association between the DDNS update method and the interface or the hostname from the running configuration, use the **no** form of this command.

ddns update [*method-name* | **hostname** *hostname*]
no ddns update [*method-name* | **hostname** *hostname*]

Syntax Description

hostname	Specifies that the next term in the command string is a hostname.
hostname	Specifies a hostname to be used for updates.
method-name	Specifies a method name for association with the interface being configured.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

After defining a DDNS update method, you must associate it with an ASA interface to trigger DDNS updates.

A hostname could be a Fully Qualified Domain Name (FQDN) or just a hostname. If just a hostname, the ASA appends a domain name to the hostname to create a FQDN.

Examples

The following example associates the interface GigabitEthernet0/2 with the DDNS update method named ddns-2 and the hostname hostname1.example.com:

```
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname hostname1.example.com
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.

Command	Description
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update method

To create a method for dynamically updating DNS resource records (RRs), use the **ddns update method** command in global configuration mode. To remove a dynamic DNS (DDNS) update method from the running configuration, use the **no** form of this command.

ddns update method *name* [**web** { **reference-identity** *name* | **update-type** { **ipv4** | **ipv6** } | **update-url** *url* }]
no ddns update method *name*

Syntax Description

name	Specifies the name of a method for dynamically updating DNS records.
reference-identity	Specifies the reference-identity name to validate server identity.
update-type	Specifies the type of update to be sent—ipv4 or ipv6.
update-url	Specifies the update URL for DDNS update.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.18(1)	The option to specify the reference identity name that is configured to match server certificate identity was added.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. The update method configured by the **ddns update method** command determines what and how often DDNS updates are performed. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method in this release.

Name and address mapping is contained in two types of resource records (RRs):

- The A resource record contains domain name-to IP-address mapping.
- The PTR resource record contains IP address-to-domain name mapping.

DDNS updates can be used to maintain consistent information between the DNS A and PTR RR types.



Note Before the **ddns update method** command will work, you must configure a reachable default DNS server using the **dns** command with domain lookup enabled on the interface.

Examples

The following example configures the DDNS update method named ddns-2:

```
ciscoasa(config)# ddns update method ddns-2
```

To validate connecting to DDNS server with reference-identity object, use **reference-identity** *ref_id_name*. A reference-identity object is created using **crypto ca reference-identity refidname** with a matching criteria. When reference-identity is configured, while attempting to connect to ddns server, ASA validates server certificate identity with a matching hostname. Failure to resolve the host or when no match is found, the connection is terminated with an error message.

```
asa(config-aaa-server-host)# ddns update method tempddns
asa(DDNS-update-method)# web ?

dynupd-method mode commands/options:
  reference-identity  Enter Reference-identity name to validate server identity
  update-type         Configure the type of update to be sent
  update-url          Configure Update URL for DDNS update
```

The configured reference-identity is displayed in the show running-config command:

```
asa(DDNS-update-method)# web reference-identity dyndns
asa(DDNS-update-method)# show running-config ddns
ddns update method tempddns
web update-url
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
web update-type ipv4
web reference-identity dyndns
interval maximum 0 0 2 0
!
asa(DDNS-update-method)#

asa(DDNS-update-method)# sh ddns update method
Dynamic DNS Update Method: dyndns
Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
  Update type configured: ipv4
  Configured reference-identity name: dyndns
  Maximum update interval: 0 days 0 hours 2 minutes 0 seconds
asa(DDNS-update-method)#
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.

Command	Description
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform dynamic DNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

debug

To show debugging messages for a given feature, use the **debug** command in privileged EXEC mode. To disable the display of debug messages, use the **no** form of this command.

debug feature [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

level	(Optional) Specifies the debugging level. The level may not be available for all features.
feature	Specifies the feature for which you want to enable debugging. To see available features, use the **debug ?** command for CLI help.
subfeature	(Optional) Depending on the feature, you can enable debug messages for one or more subfeatures.

Command Default

The default debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	The **debug crypto ca** command was modified to reduce the options and to restrict the debugging level to 14.
9.18(1)	This command was modified to include the debug for path monitoring.
9.20(1)	This command was modified to include the debug for EIGRP IPv6.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

From version 9.13(1), the options to the **debug crypto ca** command, namely **debug crypto ca transactions** and **debug crypto ca messages** are consolidated to provide all applicable content into the **debug crypto ca** command itself. Also, the number of available debugging levels were reduced to 14.

Examples

The following is sample output from the **debug aaa internal** command:

```
ciscoasa(config)# debug aaa internal
debug aaa internal enabled at level 1
ciscoasa(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

The following is the modified **debug crypto ca** command:

```
(config)# debug crypto ca ?
exec mode commands/options:
  <1-14>                   Specify an optional debug level (default is 1)
  cluster                  debug PKI cluster
  cmp                      debug the CMP transactions
  periodic-authentication  debug PKI peroidic authentication
  <cr>
```

default (crl configure)

To return all CRL parameters to their system default values, use the **default** command in crl configure configuration mode.

default

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crl configure configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Invocations of this command do not become part of the active configuration. The crl configure configuration mode is accessible from the crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them.

Examples

The following example enters ca-crl configuration mode and returns CRL command values to their defaults:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# default
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters crl configure configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

default (interface)

To return an interface command to its system default value, use the **default** command in interface configuration mode.

default*command*

Syntax Description

command Specifies the command that you want to set to the default. For example:

```
default activation key
```

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is a runtime command; when you enter it, it does not become part of the active configuration.

Examples

The following example enters interface configuration mode and returns the security level to its default:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# default security-level
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

default (ipv6 router ospf)

To return an OSPFv3 parameter to its default value, use the **default** command in ipv6 router ospf configuration mode.

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

Syntax Description

area	(Optional) Specifies the OSPFv3 area parameters.
auto-cost	(Optional) Specifies the OSPFv3 interface cost according to the bandwidth.
default-information	(Optional) Distributes default information.
default-metric	(Optional) Specifies the metric for a redistributed route.
discard-route	(Optional) Enables or disables discard-route installation.
distance	(Optional) Specifies the administrative distance.
distribute-list	(Optional) Filters networks in routing updates.
ignore	(Optional) Ignores a specific event.
log-adjacency-changes	(Optional) Logs changes in the adjacency state.
maximum-paths	(Optional) Forwards packets over multiple paths.
passive-interface	(Optional) Suppresses routing updates on an interface.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
router-id	(Optional) Specifies the router ID for the specified routing process.
summary-prefix	(Optional) Specifies the OSPFv3 summary prefix.
timers	(Optional) Specifies the OSPFv3 timers.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to reset OSPFv3 parameter default values.

Examples

The following example resets OSPFv3 timer parameters to their default values:

```
ciscoasa(config-router)# d
efault timers spf
```

Related Commands

Command	Description
distance	Specifies the administrative distance for OSPFv3 routing processes.
default-information originate	Generates a default external route into an OSPFv3 routing domain.
log-adjacency-changes	Configures the router to send a syslog message when an OSPFv3 neighbor goes up or down.

default (parameters)

To define the default action for options for which specific actions are not specified during IP Options inspection, use the **default** command in parameters configuration mode. To return to system defaults, use the **no** form of this command.

default action { **allow** | **clear** }
no default action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing options not explicitly identified in the IP options inspection policy map.
clear	Remove options not explicitly identified in the IP options inspection policy map from packet headers and then allow the packets.

Command Default

By default, IP Options inspection allows the router-alert option but drops packets containing any other IP option.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action clear
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

default (time-range)

To restore default settings for the **absolute** and **periodic** commands, use the **default** command in time-range configuration mode.

default { **absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time* }

Syntax Description

absolute	Defines an absolute time when a time range is in effect.
days-of-the-week	The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
periodic	Specifies a recurring (weekly) time range for functions that support the time range feature.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the absolute start time is reached, and are not further evaluated after the absolute end time is reached.

The time-range feature relies on the system clock of the ASA; however, the feature works best with NTP synchronization.

Examples

The following example shows how to restore the default behavior of the **absolute** keyword:

```
ciscoasa(config-time-range)# default absolute
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
periodic	Specifies a recurring (weekly) time range for functions that support the time range feature.
time-range	Defines access control to the ASA based on time.

default-acl

To specify the ACL to be used as the default ACL for NAC Framework sessions that fail posture validation, use the **default-acl** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC policy, use the **no** form of the command.

[**no**] **default-acl** *acl-name*

Syntax Description

acl-name	Names the access control list to be applied to the session.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nac-policy-nac-framework configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	"nac-" was removed from the command name. The command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.

Usage Guidelines

Each group policy points to a default ACL to be applied to hosts that match the policy and are eligible for NAC. The ASA applies the NAC default ACL before posture validation. After posture validation, the ASA replaces the default ACL with the one obtained from the Access Control Server for the remote host. It retains the default ACL if posture validation fails.

The ASA also applies the NAC default ACL if clientless authentication is enabled (which is the default setting).

Examples

The following example identifies acl-1 as the ACL to be applied before posture validation succeeds:

```
ciscoasa(config-group-policy)# default-acl acl-1
ciscoasa(config-group-policy)
```

The following example inherits the ACL from the default group policy:

```
ciscoasa(config-group-policy)# no default-acl
ciscoasa(config-group-policy)
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
nac-settings	Assigns a NAC policy to a group policy.
debug nac	Enables logging of NAC Framework events.
show vpn-session_summary.db	Displays the number of IPsec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

default-domain

To set a default domain name for users of the group policy, use the **default-domain** command in group-policy configuration mode. To delete a domain name, use the **no** form of this command.

default-domain { **value** *domain-name* | **none** }
no default-domain [*domain-name*]

Syntax Description

none	Indicates that there is no default domain name. Sets a default domain name with a null value, thereby disallowing a default domain name. Prevents inheriting a default domain name from a default or specified group policy.
value *domain-name*	Identifies the default domain name for the group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To prevent users from inheriting a domain name, use the **default-domain none** command.

The ASA passes the default domain name to the Secure Client or the legacy VPN client (IPsec/IKEv1) to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. When there are no default domain names, users inherit the default domain name in the default group policy.

You can use only alphanumeric characters, hyphens (-), and periods (.) in default domain names.

Examples

The following example shows how to set a default domain name of FirstDomain for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# default-domain value FirstDomain
```

Related Commands

Command	Description
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in clear text form.

default enrollment

To return all enrollment parameters to their system default values, use the **default enrollment** command in crypto ca trustpoint configuration mode.

default enrollment

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Invocations of this command do not become part of the active configuration.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and returns all enrollment parameters to their default values within trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# default enrollment
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

default-group-policy (imap4s, pop3s, smtps) (Deprecated)

Note The last supported release of this command was 7.5(1).

To specify the name of the group policy to use when e-mail proxy configuration does not specify a group policy, use the **default-group-policy** command in various configuration modes. To remove the attribute from the configuration, use the **no** form of this command.

default-group-policy*groupname*
nodefault-group-policy

Syntax Description

groupname	Identifies the previously configured group policy to use as the default group policy. Use the **group-policy** command to configure a group policy.

Command Default

A default group policy, named *DfltGrpPolicy*, always exists on the ASA. This **default-group-policy** command lets you substitute a group policy that you create as the default group policy e-mail proxy sessions. An alternative is to edit the DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—

Command History

Version	Modification
7.0(1)	This command was added.
7.5(2)	This command was deprecated.

Usage Guidelines

IMAP4S, POP3S, and SMTPS sessions require either a specified or a default group policy. Use this command in the applicable e-mail proxy mode.

You can edit, but not delete the system DefaultGroupPolicy. It has the following AVPs:

Attribute	Default Value
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none

Attribute	Default Value
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled

Examples

The following example shows how to specify a default group policy called pop3s for POP3S:

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-webvpn)# default-group-policy pop3s
```

default-group-policy (tunnel-group general-attributes)

To specify the set of attributes that the user inherits by default, use the **default-group-policy** command in tunnel-group general-attributes configuration mode. To eliminate a default group policy name, use the **no** form of this command.

default-group-policy*group-name*
no default-group-policy *group-name*

Syntax Description

group-name	Specifies the name of the default group.

Command Default

The default group name is DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Version	Modification
7.0(1)	This command was added.
7.1(1)	The **default-group-policy** command in webvpn configuration mode was deprecated. The **default-group-policy** command in tunnel-group general-attributes mode replaced it.

Usage Guidelines

In Version 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

The default group policy DfltGrpPolicy comes with the initial configuration of the ASA. You can apply this attribute to all tunnel group types.

Examples

The following example entered in config-general configuration mode, specifies a set of attributes for users to inherit by default for an IPsec LAN-to-LAN tunnel group named “standard-policy.” This set of commands defines the accounting server, the authentication server, the authorization server, and the address pools.

```
ciscoasa(config)# tunnel-group standard-policy type ipsec-ra
ciscoasa(config)# tunnel-group standard-policy general-attributes
ciscoasa(config-tunnel-general)# default-group-policy first-policy
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
```

```
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
group-policy	Creates or edits a group policy
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

default-idle-timeout

To set a default idle timeout value for WebVPN users, use the **default-idle-timeout** command in webvpn configuration mode. To remove the default idle timeout value from the configuration and reset the default, use the **no** form of this command.

default-idle-timeout*seconds*
no default-idle-timeout

Syntax Description

seconds	Specifies the number of seconds for the idle time out. The minimum is 60 seconds, maximum is 1 day (86400 seconds).

Command Default

1800 seconds (30 minutes).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA uses the value you set here if there is no idle timeout defined for a user, if the value is 0, or if the value does not fall into the valid range. The default idle timeout prevents stale sessions.

We recommend that you set this command to a short time period, because a browser set to disable cookies (or one that prompts for cookies and then denies them) can result in a user not connecting but nevertheless appearing in the sessions database. If the maximum number of connections permitted is set to one (via the **vpn-simultaneous-logins** command), the user cannot log back in because the database indicates that the maximum number of connections already exists. Setting a low idle timeout removes such phantom sessions quickly, and lets a user log in again.

Examples

The following example shows how to set the default idle timeout to 1200 seconds (20 minutes):

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# default-idle-timeout 1200
```

Related Commands

Command	Description
vpn-simultaneous-logins	Sets the maximum number of simultaneous VPN sessions permitted.

default-information

To control the candidate default route information for the EIGRP routing process, use the **default-information** command in router eigrp configuration mode. To suppress EIGRP candidate default route information in incoming or outbound updates, use the **no** form of this command.

default-information { **in** | **out** } [*acl-name*]
no default-information { **in** | **out** }

Syntax Description

acl-name	(Optional) Specifies the named standard access list.
in	Configures EIGRP to accept exterior default routing information.
out	Configures EIGRP to advertise external routing information.

Command Default

Exterior routes are accepted and sent.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router eigrp configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Only the **no** form of the command or **default-information** commands with an access list specified will appear in the running configuration because, by default, the candidate default routing information is accepted and sent. The **no** form of the command does not take an *acl-name* argument.

Examples

The following example disables the receipt of exterior or candidate default route information:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no default-information in
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

default-information originate

To generate a default route into an IS-IS routing domain, use the **default-information originate** command in router isis configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]
no default-information originate [**route-map** *map-name*]

Syntax Description

route-map	(Optional) Routing process generates the default route if the route map is satisfied.
map-name	Name of the route map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If an ASA configured with this command has a route to 0.0.0.0 in the routing table, IS-IS originates an advertisement for 0.0.0.0 in its LSPs.

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached-bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the ASA generate default in its Level 1 LSPs.
- Advertise 0/0 conditionally.

With a **match ip address standard-access-list** command, you can specify one or more IP routes that must exist before the router will advertise 0/0.

Examples

The following example forces the software to generate a default external route into an IS-IS domain:

```
router isis
! ISIS routes will be distributed into IS-IS
```

```
redistribute isis 120 metric
! access list 2 is applied to outgoing routing updates
default-information originate
! access list 2 defined as giving access to network 10.105.0.0
access-list 2 permit 10.105.0.0 0.0.255.255
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.

Command	Description
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.

Command	Description
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

default-information originate (address-family)

To configure a Border Gateway Protocol (BGP) routing process to distribute a default route (network 0.0.0.0), use the default-information originate command in address-family configuration mode. To disable the advertisement of a default route, use the no form of this command.

default-informationoriginate
no default-information originate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The default-information originate command is used to configure a BGP routing process to advertise a default route (network 0.0.0.0). A redistribution statement must also be configured to complete this configuration or the default route will not be advertised.

The configuration of the default-information originate command in BGP is similar to the configuration of the network (BGP) command. The default-information originate command, however, requires explicit redistribution of the route 0.0.0.0. The network command requires only that the route 0.0.0.0 is present in the Interior Gateway Protocol (IGP) routing table. For this reason, the network command is preferred.

Note The default-information originate command should not be configured with the neighbor default-originate command on the same router. You should configure one or the other.

Examples

In the following example, the router is configured to redistribute a default route from OSPF into the BGP routing process:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# default-information originate
ciscoasa(config-router-af)# redistribute ospf 100
```

Related Commands

Command	Description
network	Specifies the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.

default-information originate (ipv6 router ospf, router ospf)

To generate a default external route into an OSPFv2 or OSPFv3 routing domain, use the **default-information originate** command in router configuration mode or IPv6 router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**metric** *value*] [**metric-type** { **1** | **2** }] [**route-map** *map-name*]
no default-information originate [**always**] [**metric** *value*] [**metric-type** { **1** | **2** }] [**route-map** *map-name*]

Syntax Description

always	(Optional) Always advertises the default route whether or not the software has a default route.
metric *value*	(Optional) Specifies the OSPF default metric value, from 0 to 16777214.
metric-type {**1** | **2**}	(Optional) Specifies the external link type associated with the default route advertised into the OSPF routing domain. Valid values are as follows: • **1**—Type 1 external route. • **2**—Type 2 external route.
route-map *map -name*	(Optional) Specifies the name of the route map to apply.

Command Default

The default values are as follows:

- **metric** *value* is 10.
- **metric-type** is 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—
Router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

Using the **no** form of this command with optional keywords and arguments only removes the optional information from the command. For example, entering the **no default-information originate metric** *3* command removes the **metric** *3* option from the command in the running configuration. To remove the complete command from the running configuration, use the **no** form of the command without any options: **no default-information originate**.

Examples

The following example shows how to use the **default-information originate** command with an optional metric and metric type:

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the OSPFv2 commands in the global router configuration.
ipv6 router ospf	Enters IPv6 router configuration mode.
show running-config ipv6 router	Displays the OSPFv3 commands in the global router configuration.

default-information originate (router rip)

To generate a default route into RIP, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *name*]
no default-information originate [**route-map** *name*]

Syntax Description

route-map *name*	(Optional) Name of the route map to apply. The routing process generates the default route if the route map is satisfied.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router rip configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The route map referenced in the **default-information originate** command cannot use an extended access list; it can use only a standard access list.

Examples

The following example shows how to generate a default route into RIP:

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# default-information originate
```

Related Commands

Command	Description
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.

default-language

To set the default language displayed on the Clientless SSL VPN pages, use the **default-language** command in webvpn configuration mode.

default-language*language*

Syntax Description

language	Specifies the name of a previously imported translation table.

Command Default

The default language is en-us (English spoken in the United States).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The ASA provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users. The language parameter must use the format defined in RFC-1766 in order to be in proper compliance.

The default language is displayed to Clientless SSL VPN users when they initially connect to the ASA, before logging in. Thereafter, the language displayed is affected by the tunnel group or group policy settings and any customization that they reference.

Examples

The following example changes the default language to Chinese *with the name >Sales:*

```
ciscoasa(config-webvpn)# default-language zh
```

Related Commands

Command	Description
import webvpn translation-table	Imports a translation table.
revert	Removes translation tables from cache memory.
show import webvpn translation-table	Displays information about imported translation tables.

default-mapping-rule

To configure the default mapping rule in a Mapping Address and Port (MAP) domain, use the **default-mapping-rule** command in MAP domain configuration mode. Use the **no** form of this command to delete the basic mapping rule.

default-mapping-rule *ipv6_prefix / prefix_length*
no default-mapping-rule *ipv6_prefix / prefix_length*

Syntax Description

ipv6_prefix/prefix_length	The IPv6 prefix to be used to embed IPv4 destination addresses per RFC 6052. The prefix length should normally be 64, but allowed values are 32, 40, 48, 56, 64 or 96. Any trailing bits after the embedded IPv4 address are set to 0.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The border relay (BR) device uses this rule to translate all IPv4 addresses outside the MAP domain to an IPv6 address that works within the MAP domain. The MAP-T customer edge (CE) devices within the MAP domain install an IPv4 default route using this rule.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0

ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64

ciscoasa(config-map-domain-bmr)# start-port 1024
```

```
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

default-mcast-group

To specify a default multicast group for all VXLAN VNI interfaces associated with the VTEP source interface, use the **default-mcast-group** command in nve configuration mode. To remove the default group, use the **no** form of this command.

default-mcast-group*mcast_ip*
no default-mcast-group

Syntax Description

mcast_ip	Sets the default multicast group IP address, IPv4 or IPv6.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nve configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.
9.20(1)	This command now supports IPv6.

Usage Guidelines

When the ASA sends a packet to a device behind a peer VTEP, the ASA needs two important pieces of information:

- The destination MAC address of the remote device
- The destination IP address of the peer VTEP

There are two ways in which the ASA can find this information:

- A single peer VTEP IP address can be statically configured on the ASA.

You cannot manually define multiple peers.

The ASA then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC address.

- A multicast group can be configured on each VNI interface (or on the VTEP as a whole with the **default-mcast-address** command).

The ASA sends a VXLAN-encapsulated ARP broadcast packet within an IP multicast packet through the VTEP source interface. The response to this ARP request enables the ASA to learn both the remote VTEP IP address along with the destination MAC address of the remote end node.

The ASA maintains a mapping of destination MAC addresses to remote VTEP IP addresses for the VNI interfaces.

If you do not configure the multicast group per VNI interface, then the default group is used. If you configure a group at the VNI interface level, then that group overrides this setting.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and specifies a default multicast group of 236.0.0.100:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.

Command	Description
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

default-metric

To specify the EIGRP metrics for redistributed routes, use the **default-metric** command in router configuration mode. To restore the default values, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*
no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

bandwidth	The minimum bandwidth of the route in kilobytes per second. Valid values are from 1 to 4294967295.
delay	The route delay in tens of microseconds. Valid values are 1 to any positive number that is a multiple of 39.1 nanoseconds.
loading	The effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
mtu	The smallest allowed value for the MTU, expressed in bytes. Valid values are from 1 to 65535.
reliability	The likelihood of successful packet transmission expressed as a number from 0 through 255. The value 255 means 100 percent reliability; 0 means no reliability.

Command Default

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to the metric of the interface. The metric of redistributed static route with exit interface is the metric of the exit interface. The metric of another EIGRP instance is copied from that instance.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for EIGRP Ipv6 routing was added.

Usage Guidelines

You must use a default metric to redistribute a protocol into EIGRP unless you use the **metric** keyword and attributes in the **redistribute** command. Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values. Keeping the same metrics is supported only when you are redistributing from static routes.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

Examples

The following example shows how the redistributed RIP route metrics are translated into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters router configuration mode for that process.
redistribute (EIGRP)	Redistributes routes into the EIGRP routing process.

default user group

For Cloud Web Security, to specify the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA, use the **default user group** command in parameters configuration mode. To remove the default user or group, use the **no** form of this command. You can access the parameters configuration mode by first entering the **policy-map type inspect scansafe** command.

default { [**user** *username* [**group** *groupname*]] }
no default [**user** *username* [**group** *groupname*]

Syntax Description

username	Specifies the default username.
groupname	Specifies the default group name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If the ASA cannot determine the identity of the user coming into the ASA, then the default user and/or group is included in the HTTP header.

Examples

The following example sets a default name as “Boulder” and a group name as “Cisco”:

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default name Boulder group Cisco
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.

Command	Description
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

delay

To set a delay value for an interface, use the **delay** command in interface configuration mode. To restore the default delay value, use the **no** form of this command.

delay*delay-time*
no delay

Syntax Description

delay-time	The delay time in tens of microseconds. Valid values are from 1 to 16777215.

Command Default

The default delay depends upon the interface type. Use the **show interface** command to see the delay value for an interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.1(6)	Support for multiple context mode was added.

Usage Guidelines

The value entered is in tens of microseconds. The delay value displayed in the **show interface** output is in microseconds.

Examples

The following example changes the delay on an interface from the default 1000 to 2000. Truncated **show interface** command output is included before and after the **delay** command to show how the command affects the delay values. The delay value is noted in the second line of the **show interface** output, after the DLY label.

Notice that the command entered to change the delay value to 2000 is **delay 200**, not **delay 2000**. This is because the value entered with the **delay** command is in tens of microseconds, and the **show interface** output displays microseconds.

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# show interface Ethernet0/0
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0! Remainder of the output
```

```
removedciscoasa(config-if)# delay 200
ciscoasa(config-if)# show interface Ethernet0/0
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
       IP address 10.86.194.224, subnet mask 255.255.254.0! Remainder of the output removed
```

Related Commands

Command	Description
show interface	Displays interface statistics and settings.

delete

To delete a file from flash memory, use the **delete** command in privileged EXEC mode.

delete [**/noconfirm**] [**/replicate**] [**disk0:| disk1:| flash:**] [*path* /] *filename*

Syntax Description

/noconfirm	(Optional) Does not prompt for confirmation.
/**recursive**	(Optional) Deletes the specified file recursively in all subdirectories.
/replicate	(Optional) Deletes the specified file on the standby unit.
disk0:	(Optional) Specifies the internal flash memory.
disk1:	(Optional) Specifies the external flash memory card.
filename	Specifies the name of the file to delete.
flash:	(Optional) Specifies the internal flash memory. This keyword is the same as **disk0**.
path/	(Optional) Specifies to the path to the file.

Command Default

If you do not specify a directory, the directory is the current working directory by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The file is deleted from the current working directory if a path is not specified. Wildcards are supported when deleting files. When deleting files, you are prompted with the filename and must confirm the deletion.

Examples

The following example shows how to delete a file named test.cfg in the current working directory:

```
ciscoasa# delete test.cfg
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
rmdir	Removes a file or directory.
show file	Displays the specified file.

deny-message

To change the message delivered to a remote user who logs into WebVPN successfully, but has no VPN privileges, use the **deny-message value** command in group-webvpn configuration mode. To remove the string so that the remote user does not receive a message, use the **no** form of this command.

deny-message value *string*
no deny-message value

Syntax Description

string	Allows up to 491 alphanumeric characters, including special characters, spaces, and punctuation.

Command Default

The default deny message is: "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command moved from tunnel-group webvpn configuration mode to group-webvpn configuration mode.

Usage Guidelines

Before entering this command, you must enter the **group-policy** *name* **attributes** command in global configuration mode, then the **webvpn** command. (This step assumes you already have created the policy name.)

The **no deny-message none** command removes the attribute from the group-webvpn configuration. The policy inherits the attribute value.

When typing the string in the **deny-message value** command, continue typing even if the command wraps.

The text appears on the remote user's browser upon login, independent of the tunnel policy used for the VPN session.

Examples

The following example shows the first command that creates an internal group policy named group2. The subsequent commands modify the deny message associated with that policy:

```
ciscoasa(config)# group-policy group2 internal
ciscoasa(config)# group-policy group2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator for
more information."
ciscoasa(config-group-webvpn)
```

Related Commands

Command	Description
clear configure group-policy	Removes all group policy configuration.
group-policy	Creates a group policy.
group-policy attributes	Enters the group-policy attribute configuration mode.
show running-config group-policy	Displays the running group policy configuration for the policy named.
webvpn	Enters group-policy webvpn configuration mode.

deny version

To deny a specific version of SNMP traffic, use the **deny version** command in snmp-map configuration mode. To disable this command, use the **no** form of this command.

deny version *version*
no deny version *version*

Syntax Description

version Specifies the version of SNMP traffic that the ASA drops. The permitted values are **1**, **2**, **2c**, and **3**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Snmp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **deny version** command to restrict SNMP traffic to specific versions of SNMP. Earlier versions of SNMP were less secure, so restricting SNMP traffic to Version 2 may be specified by your security policy. You use the **deny version** command within an SNMP map, which you configure using the **snmp-map** command, which is accessible by entering the **snmp-map** command in global configuration mode. After creating the SNMP map, you enable the map using the **inspect snmp** command, and then apply it to one or more interfaces using the **service-policy** command.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface:

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
```

```
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect snmp	Enables SNMP application inspection.
policy-map	Associates a class map with specific security actions.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
service-policy	Applies a policy map to one or more interfaces.

description

To add a description for a named configuration unit (for example, for a context or for an object group, or for a DAP record), use the **description** command in various configuration modes. To remove the description, use the **no** form of this command.

description *text*
no description

Syntax Description

text Sets the description as a text string of up to 200 characters in length. The description adds helpful notes in your configuration.

For dynamic-access-policy-record mode, the maximum length is 80 characters. For event manager applets, the maximum length is 256 characters.

If you want to include a question mark (?) in the string, you must type **Ctrl-V** before typing the question mark so you do not inadvertently invoke CLI help.

Command Default

No default behavior or values.

Command Modes

This command is available in various configuration modes.

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	Support was added for the dynamic-access-policy-record configuration mode.
9.2(1)	Support for the event manager applet configuration mode was added.

Examples

The following example adds a description to the "Administration" context configuration:

```
ciscoasa(config)# context administrator
ciscoasa(config-context)# description This is the admin context.
ciscoasa(config-context)
# allocate-interface gigabitethernet0/0.1
ciscoasa(config-context)
# allocate-interface gigabitethernet0/1.1
ciscoasa(config-context)
# config-url flash://admin.cfg
```

Related Commands

Command	Description
class-map	Identifies traffic to which you apply actions in the **policy-map** command.
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.

Command	Description
object-group	Identifies traffic to include in the **access-list** command.
policy-map	Identifies actions to apply to traffic identified by the **class-map** command.



dh – dm

- dhcp-client broadcast-flag, on page 1221
- dhcp-client client-id, on page 1223
- dhcp client route distance, on page 1225
- dhcp client route track, on page 1227
- dhcp-client update dns, on page 1229
- dhcp-network-scope, on page 1231
- dhcp-server, on page 1233
- dhcpd address, on page 1235
- dhcpd auto_config, on page 1237
- dhcpd dns, on page 1239
- dhcpd domain, on page 1241
- dhcpd enable, on page 1243
- dhcpd lease, on page 1245
- dhcpd option, on page 1247
- dhcpd ping_timeout, on page 1250
- dhcpd reserve-address, on page 1252
- dhcpd update dns, on page 1254
- dhcpd wins, on page 1256
- dhcprelay enable, on page 1258
- dhcprelay information trust-all, on page 1260
- dhcprelay information trusted, on page 1262
- dhcprelay server (global), on page 1264
- dhcprelay server (interface), on page 1266
- dhcprelay server (vti tunnel), on page 1268
- dhcprelay setroute, on page 1270
- dhcprelay timeout, on page 1272
- dialog, on page 1274
- diameter, on page 1276
- dir, on page 1278
- director-localization, on page 1280
- disable (cache), on page 1282
- disable (privileged EXEC), on page 1284
- disable service-settings (Deprecated), on page 1286

- display, on page 1288
- distance, on page 1289
- distance bgp, on page 1293
- distance eigrp, on page 1295
- distance ospf (ipv6 router ospf), on page 1297
- distance ospf (router ospf), on page 1299
- distribute-list, on page 1301
- distribute-list prefix-list (eigrp), on page 1303
- distribute-list in (address-family), on page 1305
- distribute-list in (router), on page 1307
- distribute-list out (address-family), on page 1309
- distribute-list out (router), on page 1311

dhcp-client broadcast-flag

To allow the ASA to set the broadcast flag in the DHCP client packet, use the **dhcp-client broadcast-flag** command in global configuration mode. To disallow the broadcast flag, use the **no** form of this command.

dhcp-client broadcast-flag
no dhcp-client broadcast-flag

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the broadcast flag is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address.

The DHCP client can receive both broadcast and unicast offers from the DHCP server.

Examples

The following example enables the broadcast flag:

```
ciscoasa(config)# dhcp-client broadcast-flag
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client for an interface.
interface	Enters interface configuration mode so you can set the IP address.
dhcp-client client-id	Sets DHCP request packet option 61 to include the interface MAC address.

Command	Description
dhcp-client update dns	Enables DNS updates for the DHCP client.

dhcp-client client-id

To force a MAC address to be stored inside a DHCP request packet for option 61 instead of the default internally generated string, use the **dhcp-client client-id** command in global configuration mode. To disallow the MAC address, use the **no** form of this command.

dhcp-client client-id interface *interface_name*
no dhcp-client client-id interface *interface_name*

Syntax Description

interface *interface_name*	Specifies the interface on which you want to enable the MAC address for option 61.

Command Default

By default, an internally-generated ASCII string is used for option 61.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use the **dhcp-client client-id** command to include the interface MAC address for option 61.

Examples

The following example enables the MAC address for option 61 for the outside interface:

```
ciscoasa(config)# dhcp-client client-id interface outside
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client for an interface.
interface	Enters interface configuration mode so you can set the IP address.
dhcp-client broadcast-flag	Sets the broadcast flag in the DHCP client packet.

Command	Description
dhcp-client update dns	Enables DNS updates for the DHCP client.

dhcp client route distance

To configure an administrative distance for routes learned through DHCP, use the **dhcp client route distance** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

dhcp client route distance *distance*
no dhcp client route distance *distance*

Syntax Description

distance	The administrative distance to apply to routes learned through DHCP. Valid values are from 1 to 255.

Command Default

Routes learned through DHCP are given an administrative distance of 1 by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **dhcp client route distance** command is checked only when a route is learned from DHCP. If the **dhcp client route distance** command is entered after a route is learned from DHCP, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option in the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route track	Associates routes learned through DHCP with a tracking entry object.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp client route track

To configure the DHCP client to associate added routes with a specified tracked object number, use the **dhcp client route track** command in interface configuration mode. To disable DHCP client route tracking, use the **no** form of this command.

dhcp client route track *number*
no dhcp client route track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **dhcp client route track** command is checked only when a route is learned from DHCP. If the **dhcp client route track** command is entered after a route is learned from DHCP, the existing learned routes are not associated with a tracking object. You must put the following two commands in the correct order. Make sure that you always enter the **dhcp client route track** command first, followed by the **ip address dhcp setroute** command, If you have already entered the **ip address dhcp setroute** command, then remove it and reenter it in the order previously described. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option in the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
ciscoasa(config)# sla monitor 123
```

```
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route distance	Assigns an administrative distance to routes learned through DHCP.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp-client update dns

To configure the update parameters that the DHCP client passes to the DHCP server, use the **dhcp-client update dns** command in global configuration mode. To remove the parameters that the DHCP client passes to the DHCP server, use the **no** form of this command.

dhcp-client update dns [**server** { **both** | **none** }]
no dhcp-client update dns [**server** { **both** | **none** }]

Syntax Description

both	The client requests that the DHCP server update both the DNS A and PTR resource records.
none	The client requests that the DHCP server perform no DDNS updates.
server	Specifies the DHCP server to receive the client requests.

Command Default

By default, the ASA requests that the DHCP server perform PTR RR updates only. The client does not send the FQDN option to the server.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can also be entered in interface configuration mode, but it is not hyphenated. See the **dhcp client update dns** command. When entered in interface mode, the **dhcp client update dns** command overrides settings configured by this command in global configuration mode.

Examples

The following example configures the client to request that the DHCP server update neither the A and the PTR RRs:

```
ciscoasa(config)# dhcp-client update dns server none
```

The following example configures the client to request that the server update both the A and PTR RRs:

ciscoasa(config)# **dhcp-client update dns server both**

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a DDNS update method with a ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

dhcp-network-scope

To specify the range of IP addresses the DHCP server should use to assign addresses to users of this group policy, use the **dhcp-network-scope** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

dhcp-network-scope { *ip_address* | **none** }
no dhcp-network-scope

Syntax Description

ip_address	Specifies a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.
none	Sets the DHCP scope to a null value, thereby allowing no IP addresses. Prevents inheriting a value from a default or specified group policy.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same subnet identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group.

If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

To specify a scope, enter a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.

We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the DHCP scope. Do not use the network number. You can use DHCP for IPv4 addressing only. If the address you choose is not an interface address, you might need to create a static route for the scope address.

This command allows inheritance of a value from another group policy. To prevent inheriting a value, use the **dhcp-network-scope none** command.

Examples

The following example shows how to set an IP subnetwork of 10.10.85.1 for the group policy named First Group:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dhcp-network-scope 10.10.85.1
```

dhcp-server

To configure support for DHCP servers that assign IP addresses to clients as a VPN tunnel is established, use the **dhcp-server** command in tunnel-group general-attributes configuration mode. To return this command to the default, use the **no** form of this command.

dhcp-server [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]
[**no**] **dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

Syntax Description

ip1	Address of a DHCP server
ip2-ip10	(Optional) Addresses of additional DHCP servers. Up to ten may be specified in the same command or spread over multiple commands.
link-selection	(Optional) Specifies that the ASA should send DHCP suboption 5, the Link Selection Suboption for the Relay Information Option 82, defined by RFC 3527. This should only be used with servers that support this RFC.
subnet-selection	(Optional) Specifies that the ASA should send DHCP Option 118, the IPv4 Subnet Selection Option, defined by RFC 3011. This should only be used with servers that support this RFC.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(5)	The **link-selection** and **subnet-selection** keywords were added.

Usage Guidelines

You can apply this attribute to remote access tunnel group types only.

Examples

The following command, entered in config-general configuration mode, adds three DHCP servers (dhcp1, dhcp2, and dhcp3) to the IPsec remote access tunnel group “remotegrp”:

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
ciscoasa(config-tunnel-general)
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

dhcpd address

To define the IP address pool used by the DHCP server, use the **dhcpd address** command in global configuration mode. To remove an existing DHCP address pool, use the **no** form of this command.

dhcpd address *ip_address 1* [- *ip_address 2*] *interface_name*
no dhcpd address *interface_name*

Syntax Description

interface_name	Interface to which the address pool is assigned. In transparent mode, specify a bridge group member interface. In routed mode, specify a routed interface or a BVI; do not specify the bridge group member interface.
ip_address1	Start address of the DHCP address pool.
ip_address2	End address of the DHCP address pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	You can now configure this command on a BVI in routed mode when using Integrated Routing and Bridging.

Usage Guidelines

The address pool of an ASA DHCP server must be within the same subnet of the ASA interface on which it is enabled, and you must specify the associated ASA interface using *interface_name*.

The size of the address pool is limited to 256 addresses per pool on the ASA. If the address pool range is larger than 253 addresses, the netmask of the ASA interface cannot be a Class C address (for example, 255.255.255.0) and needs to be something larger, for example, 255.255.254.0.

DHCP clients must be physically connected to the subnet of the ASA DCHP server interface.

The **dhcpd address** command cannot use interface names with a "-" (dash) character because this character is interpreted as a range specifier instead of as part of the object name.

The **no dhcpd address** *interface_name* command removes the DHCP server address pool that you configured for the specified interface.

See the CLI configuration guide for information about how to implement the DHCP server feature in the ASA.

Examples

The following example shows how to configure an address pool and DNS server for the DHCP clients on the DMZ interface of the ASA:

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 209.165.200.226
ciscoasa(config)# dhcpd enable dmz
```

The following example shows how to configure a DHCP server on the inside interface. The **dhcpd address** command assigns a pool of 10 IP addresses to the DHCP server on that interface.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd enable	Enables the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd auto_config

To enable the ASA to automatically configure DNS, WINS and domain name values for the DHCP server based on the values obtained from an interface running a DHCP or PPPoE client, or from a VPN server, use the **dhcpd auto_config** command in global configuration mode. To discontinue the automatic configuration of DHCP parameters, use the **no** form of this command.

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]
no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

Syntax Description

client_if_name	Specifies the interface running the DHCP client that supplies the DNS, WINS, and domain name parameters.
interface *if_name*	Specifies the interface to which the action will apply.
vpnclient-wins-override	Overrides the interface DHCP or PPPoE client WINS parameter with the vpnclient parameter.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you specify DNS, WINS, or domain name parameters using the CLI commands, then the CLI-configured parameters overwrite the parameters obtained by automatic configuration.

Examples

The following example shows how to configure DHCP on the inside interface. The **dhcpd auto_config** command is used to pass DNS, WINS, and domain information obtained from the DHCP client on the outside interface to the DHCP clients on the inside interface.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd auto_config outside
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd enable	Enables the DHCP server on the specified interface.
show ip address dhcp server	Displays detailed information about the DHCP options provided by a DHCP server to an interface acting as a DHCP client.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd dns

To define the DNS servers for DHCP clients, use the **dhcpd dns** command in global configuration mode. To clear defined servers, use the **no** form of this command.

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]
no dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

Syntax Description

dnsip1	Specifies the IP address of the primary DNS server for the DHCP client.
dnsip2	(Optional) Specifies the IP address of the alternate DNS server for the DHCP client.
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd dns** command lets you specify the IP address or addresses of the DNS server(s) for the DHCP client. You can specify two DNS servers. The **no dhcpd dns** command lets you remove the DNS IP address(es) from the configuration.

Examples

The following example shows how to configure an address pool and DNS server for the DHCP clients on the DMZ interface of the ASA.

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 192.168.1.2
ciscoasa(config)# dhcpd enable dmz
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.

Command	Description
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd enable	Enables the DHCP server on the specified interface.
dhcpd wins	Defines the WINS servers for DHCP clients.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd domain

To define the DNS domain name for DHCP clients, use the **dhcpd domain** command in global configuration mode. To clear the DNS domain name, use the **no** form of this command.

dhcpd domain *domain_name* [**interface** *if_name*]
no dhcpd domain [*domain_name*] [**interface** *if_name*]

Syntax Description

domain_name	Specifies the DNS domain name (example.com).
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd domain** command lets you specify the DNS domain name for the DHCP client. The **no dhcpd domain** command lets you remove the DNS domain server from the configuration.

Examples

The following example shows how to configure the domain name supplied to DHCP clients by the DHCP server on the ASA:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.

Command	Description
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd enable

To enable the DHCP server, use the **dhcpd enable** command in global configuration mode. To disable the DHCP server, use the **no** form of this command.

dhcpd enable *interface*
no dhcpd enable *interface*

Syntax Description

interface	Specifies the interface on which to enable the DHCP server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The DHCP server provides network configuration parameters to DHCP clients. Support for the DHCP server within the ASA means that the ASA can use DHCP to configure connected clients. The **dhcpd enable** *interface* command lets you enable the DHCP daemon to listen for the DHCP client requests on the DHCP-enabled interface. The **no dhcpd enable** command disables the DHCP server feature on the specified interface.

Note For multiple context mode, you cannot enable the DHCP server on an interface that is used by more than one context (a shared VLAN).

When the ASA responds to a DHCP client request, it uses the IP address and subnet mask of the interface at which the request was received as the IP address and subnet mask of the default gateway in the response.

Note The ASA DHCP server daemon does not support clients that are not directly connected to an ASA interface.

See the CLI configuration guide for information about how to implement the DHCP server feature in the ASA.

Examples

The following example shows how to enable the DHCP server on the inside interface:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
debug dhcpd	Displays debugging information for the DHCP server.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd lease

To specify the DHCP lease length, use the **dhcpd lease** command in global configuration mode. To restore the default value for the lease, use the **no** form of this command.

dhcpd lease *lease_length* [**interface** *if_name*]
no dhcpd lease [*lease_length*] [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
lease_length	Specifies the length of the IP address lease, in seconds, granted to the DHCP client from the DHCP server. Valid values are from 300 to 1048575 seconds.

Command Default

The default *lease_length* is 3600 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd lease** command lets you specify the length of the lease, in seconds, that is granted to the DHCP client. This lease indicates how long the DHCP client can use the assigned IP address that the DHCP server granted.

The **no dhcpd lease** command lets you remove the lease length that you specified from the configuration and replaces this value with the default value of 3600 seconds.

Examples

The following example shows how to specify the length of the lease of DHCP information for DHCP clients:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd option

To configure DHCP options, use the **dhcpd option** command in global configuration mode. To clear the option, use the **no** form of this command.

dhcpd option *code* { **ascii** *string* } | { **ip** *IP_address* [*IP_address*] } | { **hex** *hex_string* } [**interface** *if_name*]
no dhcpd option *code* [**interface** *if_name*]

Syntax Description

ascii *string*	Specifies that the option parameter is an ASCII character string without spaces.
code	Specifies a number representing the DHCP option being set. Valid values are 0 to 255 with several exceptions. See the Usage Guidelines section for the list of DHCP option codes that are not supported.
hex *hex_string*	Specifies that the option parameter is a hexadecimal string with an even number of digits and no spaces. You do not need to use a 0x prefix.
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
ip	Specifies that the option parameter is an IP address. You can specify a maximum of two IP addresses with the **ip** keyword.
IP_address	Specifies a dotted-decimal IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can use the **dhcpd option** command to provide TFTP server information to Cisco IP Phones and routers.

When a DHCP option request arrives at the ASA DHCP server, the ASA places the value or values that are specified by the **dhcpd option** command in the response to the client.

The **dhcpd option 66** and **dhcpd option 150** commands specify TFTP servers that Cisco IP Phones and routers can use to download configuration files. Use these commands as follows:

- **dhcpd option 66 ascii** *string*, where *string* is either the IP address or hostname of the TFTP server. Only one TFTP server can be specified for option 66.
- **dhcpd option 150 ip** *IP_address* [*IP_address*], where *IP_address* is the IP address of the TFTP server. You can specify a maximum of two IP addresses for option 150.

Note The **dhcpd option 66** command only takes an **ascii** parameter, and the **dhcpd option 150** only takes an **ip** parameter.

Use the following guidelines when specifying an IP address for the **dhcpd option 66 | 150** commands:

- If the TFTP server is located on the DHCP server interface, use the local IP address of the TFTP server.
- If the TFTP server is located on a less secure interface than the DHCP server interface, then general outbound rules apply. Create a group of NAT, global, and access list entries for the DHCP clients, and use the actual IP address of the TFTP server.
- If the TFTP server is located on a more secure interface, then general inbound rules apply. Create a group of static and access list statements for the TFTP server and use the global IP address of the TFTP server.

For information about other DHCP options, see RFC 2132.

Note The ASA does not verify that the option type and value that you provide match the expected type and value for the option code as defined in RFC 2132. For example, you can enter the **dhcpd option 46 ascii hello** command, and the ASA accepts the configuration although option 46 is defined in RFC 2132 as a single-digit, hexadecimal value.

You cannot configure the following DHCP options with the **dhcpd option** command:

Option Code	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER

Option Code	Description
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

Examples

The following example shows how to specify a TFTP server for DHCP option 66:

```
ciscoasa(config)# dhcpd option 66 ascii MyTftpServer
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd ping_timeout

To change the default timeout for DHCP ping, use the **dhcpd ping_timeout** command in global configuration mode. To return to the default value, use the **no** form of this command.

dhcpd ping_timeout *number* [**interface** *if_name*]
no dhcpd ping_timeout [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
number	The timeout value of the ping, in milliseconds. The minimum value is 10, the maximum is 10000. The default is 50.

Command Default

The default number of milliseconds for *number* is 50.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To avoid address conflicts, the DHCP server sends two ICMP ping packets to an address before assigning that address to a DHCP client. The ASA waits for both ICMP ping packets to time out before assigning an IP address to a DHCP client. For example, if the default value is used, the ASA waits for 1500 milliseconds (750 milliseconds for each ICMP ping packet) before assigning an IP address.

A long ping timeout value can adversely affect the performance of the DHCP server.

Examples

The following example shows how to use the **dhcpd ping_timeout** command to change the ping timeout value for the DHCP server:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd reserve-address

To reserve a DHCP address for an interface, use the **dhcpd reserve-address** command in global configuration mode. To remove an existing DHCP address reservation, use the **no** form of this command.

dhcpd reserve-address *ip_address mac_address if_name*
no dhcpd reserve_address *ip_address mac_address if_name*

Syntax Description

ip_address	The IP address from the address pool assigned to the DHCP client, based on the client's MAC address.
mac_address	The client MAC address.
if_name	The interface on which you want to reserve an IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was added.

Usage Guidelines

The reserved address must come from the configured address pool, and the address pool must be on the same subnet as the ASA interface. In transparent mode, specify a bridge group member interface. In routed mode, specify a routed interface or a BVI; do not specify the bridge group member interface.

Examples

The following example shows how to use the **dhcpd reserve-address** command to assign a specific address from the address pool to client based on the client's MAC address:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd enable inside
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

Related Commands

Command	Description
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.

Command	Description
dhcpd enable	Enables the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd update dns

To enable a DHCP server to perform DDNS updates, use the **dhcpd update dns** command in global configuration mode. To disable DDNS by a DHCP server, use the **no** form of this command.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]
no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

Syntax Description

both	Specifies that the DHCP server updates both A and PTR DNS RRs.
interface	Specifies the ASA interface to which the DDNS updates apply.
override	Specifies that the DHCP server overrides DHCP client requests.
srv_ifc_name	Specifies an interface to apply this option to.

Command Default

By default, the DHCP server performs PTR RR updates only.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. Updates are performed in conjunction with a DHCP server. The **dhcpd update dns** command enables updates by the server.

Name and address mapping is contained in two types of RRs:

- The A resource record contains domain name-to IP-address mapping.
- The PTR resource record contains IP address- to-domain name mapping.

DDNS updates can be used to maintain consistent information between the A and PTR RR types.

Using the **dhcpd update dns** command, the DHCP server can be configured to perform both A and PRT RR updates or PTR RR updates only. It can also be configured to override update requests from the DHCP client.

Examples

The following example configures the DDNS server to perform both A and PTR updates and override requests from the DHCP client:

```
ciscoasa(config)# dhcpd update dns both override
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

dhcpd wins

To define the WINS server IP addresses for DHCP clients, use the **dhcpd wins** command in global configuration mode. To remove the WINS server IP addresses from the configuration, use the **no** form of this command.

dhcpd wins *server1* [*server2*] [**interface** *if_name*]
no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
server1	Specifies the IP address of the primary Microsoft NetBIOS name server (WINS server).
server2	(Optional) Specifies the IP address of the alternate Microsoft NetBIOS name server (WINS server).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcpd wins** command lets you specify the addresses of the WINS servers for the DHCP client. The **no dhcpd wins** command removes the WINS server IP addresses from the configuration.

Examples

The following example shows how to specify WINS server information that is sent to DHCP clients:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd dns	Defines the DNS servers for DHCP clients.
show dhcpd	Displays DHCP binding, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcprelay enable

To enable the DHCP relay agent, use the **dhcprelay enable** command in global configuration mode. To disable the DHCP relay agent, use the **no** form of this command.

dhcprelay enable *interface_name*
no dhcprelay enable *interface_name*

Syntax Description

interface_name	Name of the interface on which the DHCP relay agent accepts client requests.

Command Default

The DHCP relay agent is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server.

For the ASA to start the DHCP relay agent with the **dhcprelay enable** *interface_name* command, you must have a **dhcprelay server** command already in the configuration. Otherwise, the ASA displays an error message similar to the following:

```
DHCPRA: Warning - There are no DHCP servers configured!
No relaying can be done without a server!
Use the 'dhcprelay server <server_ip> <server_interface>' command
```

You cannot enable DHCP relay under the following conditions:

- You cannot enable DHCP relay and the DHCP relay server on the same interface.
- You cannot enable DCHP relay and a DHCP server (**dhcpd enable**) on the same interface.
- The DHCP relay agent cannot be enabled if the DHCP server is also enabled.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context (a shared VLAN).

The **no dhcprelay enable** *interface_name* command removes the DHCP relay agent configuration for the interface that is specified by the *interface_name* argument only.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value up to 90 seconds:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

The following example shows how to disable the DHCP relay agent:

```
ciscoasa(config)# no dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcp relay	Displays debugging information for the DHCP relay agent.
dhcprelay server	Specifies the DHCP server to which the DHCP relay agent forwards DHCP requests.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay information trust-all

To configure a specified interface as trusted, use the **dhcprelay information trust-all** command in global configuration mode.

dhcprelay information trust-all

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command configures a given interface as trusted. To view the interface-specific trusted configuration, use the **show running-config dhcprelay interface** command in interface configuration mode. To configure a given interface as trusted in interface configuration mode, use the **dhcprelay information trusted** command. To view a given interface as trusted in global configuration mode, use the **show running-config dhcprelay** command.

Examples

The following example shows how to configure a specified interface as trusted in global configuration mode:

```
ciscoasa(config-if)# interface vlan501
ciscoasa(config-if)# nameif inside
ciscoasa(config)# dhcprelay information trust-all
ciscoasa(config)# show running-config dhcprelay
dhcprelay information trust-all
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.

Command	Description
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay information trusted

To configure a specified interface as trusted, use the **dhcprelay information trusted** command in interface configuration mode.

dhcprelay information trusted

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command configures a given interface as trusted. To view the interface-specific trusted configuration, use the **show running-config dhcprelay interface** command in interface configuration mode. To configure a given interface as trusted in global configuration mode, use the **dhcprelay information trust-all** command. To view a given interface as trusted in global configuration mode, use the **show running-config dhcprelay** command.

Examples

The following example shows how to configure a specified interface as trusted:

```
ciscoasa(config-if)# interface gigabitEthernet 0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay information trusted
ciscoasa(config)# show running-config dhcprelay
interface gigabitEthernet 0/0
nameif inside
dhcprelay information trusted
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.

Command	Description
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay server (global)

To specify the DHCP server to which DHCP requests are forwarded, use the **dhcpreplay server** command in global configuration mode. To remove the DHCP server from the DHCP relay configuration, use the **no** form of this command.

dhcprelay server [*interface_name*]
no dhcprelay server [*interface_name*]

Syntax Description

interface_name	Specifies the name of the ASA interface on which the DHCP server resides.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server. You can add up to ten DHCP relay servers per interface. You must add at least one **dhcprelay server** command to the ASA configuration before you can enter the **dhcprelay enable** command. You cannot configure a DHCP client on an interface that has a DHCP relay server configured.

The **dhcprelay server** command opens UDP port 67 on the specified interface and starts the DHCP relay task as soon as the **dhcprelay enable** command is added to the configuration.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value of up to 90 seconds:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay server (interface)

To specify the DHCP relay interface server to which DHCP requests are forwarded, use the **dhcpreplay server** command in interface configuration mode. To remove the DHCP relay interface server from the DHCP relay configuration, use the **no** form of this command.

dhcprelay server ip_address
no dhcprelay server ip_address

Syntax Description

ip_address	Specifies the IP address of the DHCP relay interface server to which the DHCP relay agent forwards client DHCP requests.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server. You can add up to four DHCP relay servers per interface. You must add at least one **dhcprelay server** command to the ASA configuration before you can enter the **dhcprelay enable** command. You cannot configure a DHCP client on an interface that has a DHCP relay server configured.

The **dhcprelay server** command opens UDP port 67 on the specified interface and starts the DHCP relay task as soon as the **dhcprelay enable** command is added to the configuration.

In the interface configuration mode, you can use the **dhcprelay server** *ip_address* command to configure a DHCP relay server (called a helper) address on a per-interface basis. This means that when a DHCP request is received on an interface and it has helper addresses configured, then the request is forwarded to only those servers.

When you use the **no dhcprelay server** *ip_address* command, the interface stops forwarding DHCP packets to that server and removes the DHCP relay agent configuration for the DHCP server that is specified by the *ip_address* argument only.

This command takes precedence over a DHCP relay server that has been configured in global configuration mode. This means that the DHCP relay agent forwards the client discovery message first to the DHCP relay interface server, then to the DHCP global relay server.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP relay interface server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value of up to 90 seconds:

```
ciscoasa(config)# interface vlan 10
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay server 10.1.1.1
ciscoasa(config-if)# exit
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay enable inside
dhcprelay timeout 90
interface vlan 10
nameif inside
dhcprelay server 10.1.1.1
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay server (vti tunnel)

To reach a dhcp relay server through a VTI tunnel interface, use the **dhcpreplay server** command in global configuration mode.

dhcprelay server *ip_address vti-ifc-name*

Syntax Description

ip_address	Specifies the IP address of the DHCP relay server that forwards client DHCP requests.
vti-ifc-name	Specify the name of the VTI interface that you want the DHCP relay agent forward the DHCP packets to the DHCP server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.14(1)	This command was added.

Usage Guidelines

The DHCP relay agent allows DHCP requests to be forwarded from a specified ASA interface to a specified DHCP server. However, the relay agent could be configured only on physical interfaces. As VTI interface was a logical interface, the DHCP relay requests could not be forwarded through it.

From ASA 9.14(1), using this command, the DHCP relay server can forward the packets through a VTI tunnel interface.

Examples

The following example shows how to configure the DHCP relay agent on a VTI tunnel. First, create a VTI tunnel:

```
ciscoasa(config)# interface Tunnel100
ciscoasa(config-if)# nameif vti
ciscoasa(config-if)# ip address 10.1.1.10 255.255.255.0
ciscoasa(config-if)# tunnel source interface outside
ciscoasa(config-if)# tunnel destination 192.168.2.111
ciscoasa(config-if)# tunnel mode ipsec ipv4
ciscoasa(config-if)# tunnel protection ipsec profile PROFILE1
```

Now, configure the DHCP relay server with the tunnel name:

```
ciscoasa(config)# dhcprelay server 192.168.3.112 vti
```

dhcprelay setroute

To set the default gateway address in the DHCP reply, use the **dhcprelay setroute** command in global configuration mode. To remove the default router, use the **no** form of this command.

dhcprelay setroute *interface*
no dhcprelay setroute *interface*

Syntax Description

interface	Configures the DHCP relay agent to change the first default IP address (in the packet sent from the DHCP server) to the address of *interface*.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command causes the default IP address of the DHCP reply to be substituted with the address of the specified ASA interface. The **dhcprelay setroute** *interface* command lets you enable the DHCP relay agent to change the first default router address (in the packet sent from the DHCP server) to the address of *interface*.

If there is no default router option in the packet, the ASA adds one containing the address of *interface*. This action allows the client to set its default route to point to the ASA.

When you do not configure the **dhcprelay setroute** *interface* command (and there is a default router option in the packet), it passes through the ASA with the router address unaltered.

Examples

The following example shows how to set the default gateway in the DHCP reply from the external DHCP server to the inside interface of the ASA:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay setroute inside
ciscoasa(config)# dhcprelay enable inside
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay timeout

To set the DHCP relay agent timeout value, use the **dhcprelay timeout** command in global configuration mode. To restore the timeout value to its default value, use the **no** form of this command.

dhcprelay timeout *seconds*
no dhcprelay timeout

Syntax Description

seconds	Specifies the number of seconds that are allowed for DHCP relay address negotiation.

Command Default

The default value for the DHCP relay timeout is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dhcprelay timeout** command lets you set the amount of time, in seconds, allowed for responses from the DHCP server to pass to the DHCP client through the relay binding structure.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the ASA, client requests on the inside interface of the ASA, and a timeout value up to 90 seconds:

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.

Command	Description
dhcprelay server	Specifies the DHCP server to which the DHCP relay agent forwards DHCP requests.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dialog

To customize dialog box messages displayed to WebVPN users, use the **dialog** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

dialog { **title** | **message** | **border** } **style** *value*
no dialog { **title** | **message** | **border** } **style** *value*

Syntax Description

border	Specifies a change to the border.
message	Specifies a change to the message.
style	Specifies a change to the style.
title	Specifies a change to the title.
value	The actual text or or CSS parameters to display (the maximum is 256 characters).

Command Default

The default title style is background-color:#669999;color:white.

The default message style is background-color:#99CCCC;color:black.

The default border style is border:1px solid black;border-collapse:collapse.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid CSS parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

- The RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma-separated entry indicates the level of intensity of each color to combine with the others.
- The HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.



Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the dialog box message, changing the foreground color to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# dialog message style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

diameter

To create a custom Diameter attribute-value pair (AVP) for use in a Diameter inspection class or policy map, use the **diameter** command in global configuration mode. To remove an existing custom AVP, use the **no** form of this command.

diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]
no diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

Syntax Description

name	The name of the custom AVP you are creating, up to 32 characters. You would refer to this name on the **match avp** command in a Diameter inspection policy map or class map.
code *value*	The custom AVP code value, from 256-4294967295. You cannot enter a code and vendor-id combination that is already defined in the system.
data-type *type*	The data type of the AVP. You can define AVP of the following types. If the new AVP is of a different type, you cannot create a custom AVP for it. • **address**—For IP addresses. • **diameter-identity**—Diameter identity data. • **diameter-uri**—Diameter uniform resource identifier (URI). • **float32**—32-bit floating point number. • **float64**—64-bit floating point number. • **int32**—32-bit integer. • **int64**—64-bit integer. • **octetstring**—Octet string. • **time**—Time value. • **uint32**—32-bit unsigned integer. • **uint64**—64-bit unsigned integer.
vendor-id *id_number*	(Optional.) The ID number of the vendor who defined the AVP, from 0-4294967295. For example, the 3GPP vendor ID is 10415, the IETF is 0.
description *text*	(Optional.) A description of the AVP, up to 80 characters. Enclose the description in quotation marks if you include spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

As new attribute-value pairs (AVP) are defined and registered, you can create custom Diameter AVP to define them and use them in your Diameter inspection policy map. You would get the information you need to create the AVP from the RFC or other source that defines the AVP.

Create custom AVP only if you want to use them in a Diameter inspection policy map or class map for AVP matching.

Examples

The following example shows how to create a custom AVP and then use it in a Diameter inspection policy map.

```
ciscoasa(config)# diameter avp eg_custom_avp code 9999 data-type int32
ciscoasa(config)# policy-map type inspect diameter avp-filter-pmap
asa3(config-pmap)# match avp eg_custom_avp
```

Related Commands

Command	Description
class-map type inspect diameter	Creates a Diameter inspection class map.
match avp	Matches Diameter attribute-value pairs (AVP).
policy-map type inspect diameter	Creates a Diameter inspection policy map.

dir

To display the directory contents, use the **dir** command in privileged EXEC mode.

dir [**/all**] [**all-filesystems**] [**/recursive**] [**disk0:** | **flash:** | **system:**] [*path*]

Syntax Description

/all	(Optional) Displays all files.
/recursive	(Optional) Displays the directory contents recursively.
all-filesystems	(Optional) Displays the files of all filesystems.
disk0:	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Displays the directory contents of the default flash partition.
path	(Optional) Specifies a specific path.
system:	(Optional) Displays the directory contents of the file system.

Command Default

If you do not specify a directory, the directory is the current working directory by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **dir** command without keywords or arguments displays the directory contents of the current directory.

Examples

The following example shows how to display the directory contents:

```
ciscoasa# dir
Directory of disk0:/
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

The following example shows how to display recursively the contents of the entire file system:

```
ciscoasa# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

The following example shows how to display the contents of the flash partition:

```
ciscoasa# dir flash:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
pwd	Displays the current working directory.
mkdir	Creates a directory.
rmdir	Removes a directory.

director-localization

To enable director localization to improve performance and reduce round-trip time latency for inter-site clustering for data centers, use the **director-localization** command in cluster group configuration mode. To disable director localization, use the **no** form of this command.

director-localization
no director-localization

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

New connections are typically load-balanced and owned by cluster members within a given site. However, the ASA assigns the director role to a member at any site. Director localization enables additional director roles: a local director at the same site as the owner, and a global director that can be at any site. Keeping the owner and director at the same site improves performance. Also, if the original owner fails, the local director chooses a new connection owner at the same site. The global director is used if a cluster member receives packets for a connection that is owned on a different site.

Set the site ID for the cluster member in the bootstrap configuration.

The following traffic types do not support localization: NAT or PAT traffic; SCTP-inspected traffic; Fragmentation owner query.

Examples

The following example enables director localization for cluster1:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# director-localization
ciscoasa(cfg-cluster)# enable noconfirm
```

Related Commands

Command	Description
cluster group	Enters cluster group configuration mode.
show asp table cluster chash	Shows local cHash tables.
show conn	The conn flag "l" indicates the stub flow is local director "Yl" or local backup "yl".
site-id	Sets the cluster unit site ID for use with inter-site clustering.

disable (cache)

To disable caching for WebVPN, use the **disable** command in cache configuration mode. To reenable caching, use the **no** version of this command.

disable
no disable

Command Default

Caching is enabled with default settings for each cache attribute.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cache Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, with the result that many applications run much more efficiently.

Examples

The following example shows how to disable caching, and then how to reenable it.

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# disable
ciscoasa(config-webvpn-cache)# no disable
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters webvpn cache configuration mode.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.

Command	Description
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum size of an object to cache.

disable (privileged EXEC)

To exit privileged EXEC mode and return to unprivileged EXEC mode, use the **disable** command in privileged EXEC mode.

disable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **enable** command to enter privileged mode. The **disable** command allows you to exit privileged mode and returns you to an unprivileged mode.

Note If you are logged into the ASA with a username, then entering **disable** will change your user identity to the default enable_1 username.

Examples

The following example shows how to enter privileged mode:

```
ciscoasa
>
enable
ciscoasa#
```

The following example shows how to exit privileged mode:

```
ciscoasa#

disable
ciscoasa
>
```

Related Commands

Command	Description
enable	Enables privileged EXEC mode.

disable service-settings (Deprecated)

To disable the service settings on IP phones when using the Phone Proxy feature, use the **disable service-settings** command in phone-proxy configuration mode. To preserve the settings on the IP phones, use the **no** form of this command.

disable service-settings
no disable service-settings

Syntax Description

There are no arguments or keywords for this command.

Command Default

The service settings are disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

By default, the following settings are disabled on the IP phones:

- PC Port
- Gratuitous ARP
- Voice VLAN access
- Web Access
- Span to PC Port

To preserve the settings configured on the CUCM for each IP phone configured, configure the **no disable service-settings** command.

Examples

The following example shows how to preserve the settings of the IP phones that use the Phone Proxy feature on the ASA:

```
ciscoasa
(config-phone-proxy)# no disable service-settings
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
show phone-proxy	Displays Phone Proxy specific information.

display

To display attribute value pairs that the ASA writes to the DAP attribute database, enter the **display** command in dap test attributes mode.

display

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap test attributes	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Normally the ASA retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The ASA writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record. The **display** command lets you display these attributes to the console.

Related Commands

Command	Description
attributes	Enters attributes configuration mode, in which you can set attribute value pairs.
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes submode.
test dynamic-access-policy execute	Executes the logic that generates DAP and displays the resulting access policies to the console.

distance

To define the administrative distance assigned to routes discovered by the IS-IS protocol, use the **distance** command in router isis configuration mode. To remove the distance command from the configuration file and restore the system to its default condition in which the software removes a distance definition, use the **no** form of this command.

distance*weight***ip**
no distance *weight* **ip**

Syntax Description

weight	The administrative distance to be assigned to IS-IS routes. The range is 1 to 255.
ip	The distance applied for IP-derived routes.

Command Default

The default is 115.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

An administrative distance is a number from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

Use the **distance** command to configure the administrative distances applied to IS-IS routes when they are inserted into the Routing Information Base (RIB), and influence the likelihood of these routes being preferred over routes to the same destination addresses discovered by other protocols.

Examples

In the following example, a distance of 20 is assigned to all ISIS routes:

```
ciscoasa(config)#
router isis
ciscoasa(config-router)#
distance 20 ip
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

distance bgp

To configure the administrative distance for BGP routes, use the distance bgp command in address family configuration mode. To return the administrative distance to the default value, use the no form of this command.

distancebgp*external-distanceinternal-distancelocal-distance*
no distance bgp

Syntax Description

external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.

Command Default

The following values are used if this command is not configured or if the no form is entered:

external-distance: 20 internal-distance: 200 local-distance: 200

Note Routes with a distance of 255 are not installed in the routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The distance bgp command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255.

In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.



Caution Changing the administrative distance of internal BGP routes is considered dangerous and is not recommended. Improper configuration can introduce routing table inconsistencies and break routing.

The distance bgp command replaces the distance mbgp command.

Examples

In the following example, the external distance is set to 10, the internal distance is set to 50, and the local distance is set to 100:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# distance bgp 10 50 100
ciscoasa(config-router-af)# end
```

distance eigrp

To configure the administrative distances of internal and external EIGRP routes, use the **distance eigrp** command in router configuration mode. To restore the default values, use the **no** form of this command.

distanceeigrp*internal-distanceexternal-distance*
no distance eigrp

Syntax Description

external-distance	Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. Valid values are from 1 to 255.
internal-distance	Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. Valid values are from 1 to 255.

Command Default

The default values are as follows:

- *external-distance* is 170
- *internal-distance* is 90

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Because every routing protocol has metrics based on algorithms that are different from the other routing protocols, it is not always possible to determine the “best path” for two routes to the same destination that were generated by different routing protocols. Administrative distance is a route parameter that the ASA uses to select the best path when there are two or more different routes to the same destination from two different routing protocols.

If you have more than one routing protocol running on the ASA, you can use the **distance eigrp** command to adjust the default administrative distances of routes discovered by the EIGRP routing protocol in relation to the other routing protocols. <xref> lists the default administrative distances for the routing protocols supported by the ASA.

Table 7: Default Administrative Distances

Route Source	Default Administrative Distance
Connected interface	0
Static route	1
EIGRP summary route	5
Internal EIGRP	90
OSPF	110
RIP	120
EIGRP external route	170
Unknown	255

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for both internal and external EIGRP routes.

Examples

The following example uses the **distance eigrp** command to set the administrative distance of all EIGRP internal routes to 80 and all EIGRP external routes to 115. Setting the EIGRP external route administrative distance to 115 would give routes discovered by EIGRP to a specific destination preference over the same routes discovered by RIP but not by OSPF.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.7.0
ciscoasa(config-router)# network 172.16.0.0

ciscoasa(config-router)# distance eigrp 90 115
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

distance ospf (ipv6 router ospf)

To define OSPFv3 route administrative distances based on route type, use the **distance** command in ipv6 router ospf configuration mode. To restore the default values, use the **no** form of this command.

distance [**ospf** { **external** | **intra-area** / **inter-area** }] *distance*
no distance [**ospf** { **external** | **intra-area** / **inter-area** }] *distance*

Syntax Description

distance	Specifies the administrative distance. Valid values range from 10 to 254.
external	(Optional) Specifies external type 5 and type 7 routes for OSPFv3 routes.
inter-area	(Optional) Specifies the inter-area routes for OSPFv3 routes.
intra-area	(Optional) Specifies the intra-area routes for OSPFv3 routes.
ospf	(Optional) Specifies the administrative distance for OSPFv3 routes.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to set the administrative distance for OSPFv3 routes.

Examples

The following example sets the administrative distance for external type 5 and type 7 routes for OSPFv3 to 200:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# distance ospf external 200
```

Related Commands

Command	Description
default-information originate	Generates a default external route into an OSPFv3 routing domain.

Command	Description
redistribute	Redistributes IPv6 routes from one routing domain into another routing domain.

distance ospf (router ospf)

To define OSPFv2 route administrative distances based on route type, use the **distance ospf** command in router ospf configuration mode. To restore the default values, use the **no** form of this command.

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]
no distance ospf

Syntax Description

d1, *d2*, and *d3*	Specifies the distance for each route type. Valid values range from 1 to 255.
external	(Optional) Sets the distance for routes from other routing domains that are learned by redistribution.
inter-area	(Optional) Sets the distance for all routes from one area to another area.
intra-area	(Optional) Sets the distance for all routes within an area.

Command Default

The default values for *d1*, *d2*, and *d3* are 110.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf configuratio	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must specify at least one keyword and argument. You can enter the commands for each type of administrative distance separately, however they appear as a single command in the configuration. If you reenter an administrative distance, the administrative distance for only that route type changes; the administrative distances for any other route types remain unaffected.

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for all of the route types. If you want to restore the default administrative distance for a single route type when you have multiple route types configured, you can do one of the following:

- Manually set that route type to the default value.
- Use the **no** form of the command to remove the entire configuration and then reenter the configurations for the route types that you want to keep.

Examples

The following example sets the administrative distance of external routes to 150:

```
ciscoasa(config-router)# distance ospf external 105
ciscoasa(config-router)#
```

The following example shows how entering separate commands for each route type appears as a single command in the router configuration:

```
ciscoasa(config-rtr)# distance ospf intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf intra-area 105
ciscoasa(config-rtr)# distance ospf external 105
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
ciscoasa(config)#
```

The following example shows how to set each administrative distance to 105, and then change only the external administrative distance to 150. The **show running-config router ospf** command shows how only the external route type value changed, while the other route types retained the value previously set.

```
ciscoasa(config-rtr)# distance ospf external 105 intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf external 150
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
ciscoasa(config)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode for OSPFv2.
show running-config router	Displays the OSPFv2 commands in the global router configuration.

distribute-list

To filter networks received or transmitted in Open Shortest Path First (OSPF) updates, use the distribute-list command in the router ospf configuration mode. To change or cancel the filter, use the no form of this command.

distribute-list *access-list name* [**in** | **out**] [**interface** *if_name*]
no distribute-list *access-list name* [**in** | **out**]

Syntax Description

access-list name	Standard IP access list name. The list defines which networks are to be received and which are to be suppressed in routing updates.
in	Applies the access list or route-policy to incoming routing updates.
out	Applies the access list or route-policy to outgoing routing updates.The out keyword is available only in router configuration mode.
interface *if_name*	(Optional) The interface on which to apply the routing updates. Specifying an interface causes the access list to be applied only to routing updates received on that interface.

Command Default

Networks are not filtered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

If no interface is specified, the access list will be applied to all incoming updates.

Examples

The following example filters OSPF routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
ciscoasa(config)# access-list ospf_filter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ospf_filter deny any
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ospf_filter in interface outside
```

Related Commands

Command	Description
distribute-list in	Filters incoming routing updates.
router ospf	Enters router configuration mode for the OSPF routing process.
show running-config router	Displays the commands in the global router configuration.

distribute-list prefix-list (eigrp)

To apply a prefix list to EIGRP for IPv6 routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command

distribute-list prefix-list *list_name* [**in** | **out**] [*if_name*]
no distribute-list prefix-list *list_name* [**in** | **out**] [*if_name*]

Syntax Description

list_name	Name of a prefix list.
in	Applies the prefix list to incoming routing updates.
out	Applies the prefix list to outgoing routing updates.The out keyword is available only in router configuration mode.
if_name	(Optional) The interface on which to apply the routing updates. Specifying an interface causes the prefix list to be applied only to routing updates received on that interface.

Command Default

Networks are not filtered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was added.

Usage Guidelines

The specified prefix list defines which EIGRP for IPv6 networks to be accepted in incoming routing updates and which networks are to be advertised in the outgoing routing updates, based upon the matching network prefixes. If no interface is specified, the list will be applied to all incoming updates.

Examples

The following example filters EIGRP routing updates received on the *a2* interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
ciscoasa(config)# access-list abc deny any
ciscoasa(config)# ipv6 router eigrp 1
ciscoasa(config-rtr)# distribute-list prefix-list abc in a2
```

Related Commands

Command	Description
ipv6 router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.
show running-config router	Displays the commands in the global router configuration.

distribute-list in (address-family)

To filter routes or networks received in incoming Border Gateway Protocol (BGP) updates; use the distribute-list in command in address-family configuration mode. You can access the address-family configuration mode by first entering the **router bgp** command. To delete the distribute list and remove it from the running configuration file, use the no form of this command.

distribute-list { *acl-name* | **prefix** *list-name* } **in**
no distribute-list { *acl-name* | **prefix** *list-name* } **in**

Syntax Description

acl-name	Standard IP access list name. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix list-name	Name of a prefix list. The prefix list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes.

Command Default

If this command is configured without a predefined access list or prefix list, the distribute list will default to permitting all traffic.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The distribute-list in command is used to filter incoming BGP updates. An access list or prefix list must be defined prior to configuration of this command. Standard and expanded access lists are supported. IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribute list. The session must be reset with the clear bgp command before the distribute list will take effect.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to accept traffic from only network 10.1.1.0/24, network 192.168.1.0, and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# ip prefix-list RED permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list RED permit 10.108.0.0/16
ciscoasa(config)# ip prefix-list RED permit 192.168.1.0/24
```

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list prefix RED in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

In the following example, an access list and distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.1.0 255.255.255.0

ciscoasa(config)# access-list distribute-list-acl permit 10.108.0.0 255.255.0.0

ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list distribute-list-acl in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

Related Commands

Command	Description
clear bgp	Resets BGP connections using hard or soft reconfigurations.
ip prefix-list	Creates a prefix list or adds a prefix list entry.

distribute-list in (router)

To filter incoming routing updates, use the **distribute-list in** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **in** [**interface** *if_name*]
no distribute-list *acl* **in** [**interface** *if_name*]

Syntax Description

acl	Name of a standard access list.
interface *if_name*	(Optional) The interface on which to apply the incoming routing updates. Specifying an interface causes the access list to be applied only to routing updates received on that interface.

Command Default

Networks are not filtered in incoming updates.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

If no interface is specified, the access list will be applied to all incoming updates.

Examples

The following example filters RIP routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
ciscoasa(config)# access-list ripfilter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter deny any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter in interface outside
```

The following example filters EIGRP routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
ciscoasa(config)# access-list eigrp_filter permit 10.0.0.0 255.0.0.0
```

```
ciscoasa(config)# access-list eigrp_filter deny any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter in interface outside
```

Related Commands

Command	Description
distribute-list out	Filters outgoing routing updates.
router eigrp	Enters router configuration mode for the EIGRP routing process.
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.

distribute-list out (address-family)

To suppress networks from being advertised in outbound Border Gateway Protocol (BGP) updates, use the distribute-list out command in address-family configuration mode. You can access the address-family configuration mode by first entering the **router bgp** command. To delete the distribute list and remove it from the running configuration file, use the no form of this command.

distribute-list { *acl-name* | **prefix** *list-name* } **out** [*protocol process-number* | **connected** | **static**]
no distribute-list { *acl-name* | **prefix** *list-name* } **out** [*protocol process-number* | **connected** | **static**]

Syntax Description

acl-name	Standard IP access list name. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix list-name	Name of a prefix list. The prefix list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes.
protocol process-number	Specifies the routing protocol to apply the distribution list. BGP, EIGRP, OSPF, and RIP are supported. The process number is entered for all routing protocols, except RIP. The process number is a value from 1 to 65.
connected	Specifies peers and networks learned through connected routes.
static	Specifies peers and networks learned through static routes.

Command Default

If this command is configured without a predefined access list or prefix list, the distribute list will default to permitting all traffic.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The distribute-list out command is used to filter outbound BGP updates. An access list or prefix list must be defined prior to configuration of this command. Only standard access lists are supported.

IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribute list. The session must be reset with the clear bgp command before the distribute list will take effect.

Entering a protocol and/or process-number arguments causes the distribute list to be applied to only routes derived from the specified routing process. Addresses not specified in the distribute-list command will not be advertised in outgoing routing updates after a distribute list is configured.

To suppress networks or routes from being received in inbound updates, use the distribute-list in command.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# ip prefix-list BLUE permit 192.168.0.0/16
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list prefix BLUE out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

In the following example, an access list and a distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.0.0 255.255.0.0
ciscoasa(config)# access-list distribute-list-acl deny 0.0.0.0 0.0.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list distribute-list-acl out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

Related Commands

Command	Description
clear bgp	Resets BGP connections using hard or soft reconfigurations.
ip prefix-list	Creates a prefix list or adds a prefix list entry.

distribute-list out (router)

To filter outgoing routing updates, use the **distribute-list out** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]
no distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

Syntax Description

acl	Name of a standard access list.
connected	(Optional) Filters only connected routes.
eigrp *as_number*	(Optional) Filters only EIGRP routes from the specified autonomous system number. The *as_number* argument is the autonomous system number of the EIGRP routing process on the ASA.
interface *if_name*	(Optional) The interface on which to apply the outgoing routing updates. Specifying an interface causes the access list to be applied only to routing updates received on that interface.
ospf *pid*	(Optional) Filters only OSPF routes discovered by the specified OSPF process.
rip	(Optional) Filters only RIP routes.
static	(Optional) Filters only static routes.

Command Default

Networks are not filtered in sent updates.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The **eigrp** keyword was added.

Usage Guidelines

If no interface is specified, the access list will be applied to all outgoing updates.

Examples

The following example prevents the 10.0.0.0 network from being advertised in RIP updates sent out of any interface:

```
ciscoasa(config)# access-list ripfilter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter permit any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter out
```

The following example prevents the EIGRP routing process from advertising the 10.0.0.0 network on the outside interface:

```
ciscoasa(config)# access-list eigrp_filter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list eigrp_filter permit any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter out interface outside
```

Related Commands

Command	Description
distribute-list in	Filters incoming routing updates.
router eigrp	Enters router configuration mode for the EIGRP routing process.
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.



dn – dz

- dnscrypt, on page 1315
- dns domain-lookup, on page 1317
- dns expire-entry-timer, on page 1319
- dns-group, on page 1321
- dns-group-map, on page 1323
- dns-guard, on page 1325
- dns-id, on page 1326
- dns name-server, on page 1328
- dns poll-timer, on page 1330
- dns-server (group-policy), on page 1331
- dns-server (ipv6 dhcp pool), on page 1333
- dns server-group, on page 1336
- dns-to-domain, on page 1338
- dns trusted-source, on page 1340
- dns update, on page 1342
- domain, on page 1344
- domain-name (dns server-group), on page 1346
- domain-name (global), on page 1347
- domain-name (ipv6 dhcp pool), on page 1348
- domain-password, on page 1351
- downgrade, on page 1355
- download-max-size, on page 1357
- drop, on page 1359
- drop-connection, on page 1361
- dtls port, on page 1363
- duplex, on page 1364
- dynamic-access-policy-config, on page 1366
- dynamic-access-policy-record, on page 1368
- dynamic-authorization, on page 1370
- dynamic-filter ambiguous-is-black, on page 1372
- dynamic-filter blacklist, on page 1375
- dynamic-filter database fetch, on page 1378
- dynamic-filter database find, on page 1380

- dynamic-filter database purge, on page 1383
- dynamic-filter drop blacklist, on page 1385
- dynamic-filter enable, on page 1388
- dynamic-filter updater-client enable, on page 1391
- dynamic-filter use-database, on page 1394
- dynamic-filter whitelist, on page 1397

dnscrypt

To enable DNScrypt to encrypt connections between the device and Cisco Umbrella, use the **dnscrypt** command in DNS inspection policy map parameters configuration mode. To disable DNScrypt, use the **no** form of this command.

dnscrypt
no dnscrypt

Syntax Description

This command has no arguments or keywords.

Command Default

DNScrypt is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

Use this command when configuring a DNS inspection policy map.

Enabling DNScrypt starts the key-exchange thread with the Umbrella resolver. The key-exchange thread performs the handshake with the resolver every hour and updates the device with a new secret key.

Because DNScrypt uses UDP/443, you must ensure that the class map used for DNS inspection includes that port. Note that the default inspection class already includes UDP/443 for DNS inspection.

Examples

The following example enables Umbrella using the default policy, and also enables DNScrypt, in the default inspection policy map used in global DNS inspection. The global DNS inspection already applies to UDP/443.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

Related Commands

Commands	Description
inspect dns	Enables DNS inspection.
policy-map type inspect dns	Creates a DNS inspection policy map.
public-key	Configures the public key used with Cisco Umbrella.
token	Identifies the API token that is needed to register with Cisco Umbrella.
timeout edns	Configures the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.
umbrella-global	Configures the Cisco Umbrella global parameters.
umbrella	Enables the DNS inspection engine to redirect DNS lookup requests to Cisco Umbrella.

dns domain-lookup

To enable the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands, use the **dns domain-lookup** command in global configuration mode. To disable DNS requests, use the **no** form of this command.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

dns domain-lookup *interface_name*
no dns domain-lookup *interface_name*

Syntax Description

interface_name	Specifies the name of the configured interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Make sure to enable DNS lookup on all interfaces that will be used to access DNS servers.

After you enable DNS lookup, specify DNS servers for the default server group using the **dns server-group DefaultDNS** server group command, and then the **name-server** command. You can change the default server group using the **dns-group** command.

Other server groups can be associated with specific domains. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface. Other DNS server groups can be configured for VPN tunnel groups. See the **tunnel-group** command for more information.

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database; and Cisco Smart Software Licensing needs DNS to resolve the License Authority address. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

Examples

The following example enable the ASA to send DNS requests to a DNS server to perform a name lookup for the management, inside, and dmz interfaces.

```
ciscoasa(config)# dns domain-lookup management
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup dmz
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 management
ciscoasa(config-dns-server-group)# name-server 10.10.1.1 10.20.2.2
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns expire-entry-timer

To remove the IP address of a resolved FQDN after its TTL expires, use the **dns expire-entry-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

dns expire-entry-timer minutes *minutes*
no dns expire-entry-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer time in minutes. Valid values range from 1 to 65535 minutes.

Command Default

By default, the DNS expire-entry-timer value is 1 minute.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The command specifies the time to remove the IP address of a resolved FQDN after its TTL expires. When the IP address is removed, the ASA recompiles the tmatch lookup table.

Specifying this command is only effective when the associated network object for the DNS is activated.

The default DNS expire-entry-timer value is 1 minute, which means that IP addresses are removed 1 minute after the TTL of the DNS entry expires.

Note The default setting might result in frequent recompilation of the tmatch lookup table when the resolved TTL of common FQDN hosts, such as www.sample.com, is a short time period. You can specify a long DNS expire-entry timer value to reduce the frequency of recompilation of the tmatch lookup table while maintaining security.

Examples

The following example removes resolved entries after 240 minutes:

```
ciscoasa(config)# dns expire-entry-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns-group

To specify the default DNS group, use the **dns-group** command in global configuration mode. To specify the DNS server group per tunnel group, use the **dns-group** command in tunnel-group webvpn-attributes configuration mode. To restore the default DNS group, use the **no** form of this command.

dns-group*name*
no dns-group

Syntax Description

name	Specifies the name of the default DNS server group. The default group cannot have any associated domains in the **dns-group-map**.

Command Default

The default value is DefaultDNS.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Tunnel-group webvpn-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

You configure the default DNS group using the **dns server-group** command.

Examples

The following example shows a customization command that specifies the use of the DNS group named “dnsgroup1”:

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# dns-group dnsgroup1
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.

Command	Description
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel group attributes.

dns-group-map

To map DNS server groups to specific domains, use the **dns-group-map** command in global configuration mode. To remove the DNS group map, use the **no** form of this command.

dns-group-map
no dns-group-map

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	Added this command.

Usage Guidelines

After you enter the **dns-group-map** command, add server-group-to-domain mappings using the **dns-to-domain** command. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface.

Examples

The following example configures three mappings:

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns server-group mode, in which you can configure a DNS servers.

Command	Description
dns-to-domain	Maps a DNS server group to a domain.
name-server	Adds a DNS server to a group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns-guard

To enable the DNS guard function, which enforces one DNS response per query, use the **dns-guard** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

dns-guard
no dns-guard

Syntax Description

This command has no arguments or keywords.

Command Default

DNS guard is enabled by default. This feature can be enabled when the **inspect dns** command is configured even if a **policy-map type inspect dns** command is not defined. To disable, the **no dns-guard** command must explicitly be stated in the policy map configuration. If the **inspect dns** command is not configured, the behavior is determined by the global dns-guard command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The identification field in the DNS header is used to match the DNS response with the DNS header. One response per query is allowed through the ASA.

Examples

The following example shows how to enable DNS guard in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# dns-guard
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

dns-id

To configure a dns-id in a reference-identity object, use the **dns-id** command in ca-reference-identity mode. To delete a dns-id, use the **no** form of this command. You can access the *ca-reference-identity* mode by first entering the **crypto ca reference-identity** command to configure a reference-identity object..

dns-id*value*
no dns-id *value*

Syntax Description

value	Value of each reference-id.
dns-id	A subjectAltName entry of type dNSName. This is a DNS domain name. A DNS-ID reference identifier does not identify an application service.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ca-reference-identity	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity.

The reference identifiers **cn-id** and **dns-id** MAY NOT contain information identifying the application service and MUST contain information identifying the DNS domain name.

Examples

The following example creates a reference-identity for a syslog server:

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Related Commands

Command	Description
crypto ca reference-identity	Configures a reference identity object.
cn-id	Configures a Common Name Identifier in the reference-identity object.

Command	Description
srv-id	Configures a SRV-ID identifier in a reference identity object.
uri-id	Configures a URI identifier in a reference identity object.
logging host	Configures a logging server that can use a reference-identity object for a secure connection.
call-home profile destination address http	Configures a Smart Call Home server that can use a reference-identity object for a secure connection.

dns name-server

To configure a DNS server for the *default* DNS server group, use the **dns name-server** command in global configuration mode. To remove the configuration, use the **no** form of this command. This command is equivalent to the **name-server** command.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]
no dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

Syntax Description

ip_address Specifies the IPv4 or IPv6 address of the DNS server. You can specify up to 6 addresses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	This command was changed to add the DNS servers under the **dns server-group DefaultDNS** server group.
9.0(1)	Support for IPv6 addresses was added.

Usage Guidelines

To enable DNS lookup for an interface, configure the **dns domain-lookup** command. If you do not enable DNS lookup, the DNS servers are not used on that interface.

This command adds servers to the default DNS server group. By default, the default group is called **DefaultDNS**. You can change the default group using the **dns-group** command. See the following resulting configuration:

```
ciscoasa(config)# dns name-server 10.1.1.1
ciscoasa(config)# show running-config dns
```

```
dns server-group DefaultDNS
name-server ip_address
```

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database; and Cisco Smart Software Licensing needs DNS to resolve the License Authority address. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

Examples

The following example configures a DNS server with an IPv6 address:

```
ciscoasa(config)# dns domain-lookup
ciscoasa(config)# dns name-server 8080:1:2::2
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns server-group mode, in which you can configure a DNS servers.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns poll-timer

To specify the timer during which the ASA queries the DNS server to resolve fully qualified domain names (FQDN) that are defined in a network object group, use the **dns poll-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

dns poll-timer minutes *minutes*
no dns poll-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer in minutes. Valid values are from 1 to 65535 minutes.

Command Default

By default, the DNS timer is 240 minutes or 4 hours.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command specifies the timer during which the ASA queries the DNS server to resolve the FQDN that was defined in a network object group. A FQDN is resolved periodically when the poll DNS timer has expired or when the TTL of the resolved IP entry has expired, whichever comes first.

This command has effect only when at least one network object group has been activated.

Examples

The following example sets the DNS poll timer to 240 minutes:

```
ciscoasa(config)# dns poll-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server-group configurations.

dns-server (group-policy)

To set the IP address of the primary and secondary DNS servers, use the **dns-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

dns-server { **value** *ip_address* [*ip_address*] | **none** }
no dns-server

Syntax Description

none	Sets the **dns-server** command to a null value, thereby allowing no DNS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary DNS servers.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command allows inheritance of a DNS server from another group policy. To prevent inheriting a server, use the **dns-server none** command.

Each time you issue the **dns-server** command, you overwrite the existing setting. For example, if you configure DNS server x.x.x.x and then configure DNS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole DNS server. The same holds true for multiple servers. To add a DNS server rather than overwrite previously configured servers, include the IP addresses of all DNS servers when you enter this command.

Examples

The following example shows how to configure DNS servers with the IP addresses 10.10.10.15 and 10.10.10.45 for the group policy named FirstGroup.

```
ciscoasa
(config)#
group-policy FirstGroup attributes
ciscoasa
```

```
(config-group-policy)#
 dns-server value 10.10.10.15 10.10.10.45
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
show running-config dns server-group	Shows the current running DNS server group configuration.

dns-server (ipv6 dhcp pool)

To provide the DNS server IP address to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **dns-server** command in ipv6 dhcp pool configuration mode. To remove the DNS server, use the **no** form of this command.

dns-server*dns_ipv6_address*
no dns-server *dns_ipv6_address*

Syntax Description

dns_ipv6_address	Specifies the DNS server IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the DNS server, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
```

```
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.

Command	Description
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

dns server-group

To create and configure a group of DNS servers, use the **dns server-group** command in global configuration mode. To remove a particular DNS server group, use the **no** form of this command.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

dns server-group *name*
nodnsserver-group

Syntax Description

name Specifies the name of the DNS server group. The default group name used for ASA lookups is **DefaultDNS**.

Command Default

The default active server group for the ASA is DefaultDNS.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

To enable DNS lookup, configure the **dns domain-lookup** command. If you do not enable DNS lookup, the DNS servers are not used.

The ASA uses the **dns server-group DefaultDNS** server group for outgoing requests. You can change the active server group using the **dns-group** command. Other DNS server groups can be configured for VPN tunnel groups or other purposes. See the **tunnel-group** command for more information.

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database; and Cisco Smart Software Licensing needs DNS to resolve the License Authority address. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

Examples

The following example configures a DNS server group named “DefaultDNS”:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# domain-name cisco.com
ciscoasa(config-dns-server-group)# name-server 192.168.10.10
ciscoasa(config-dns-server-group)# retries 5
ciscoasa(config-dns-server-group)# timeout 7
ciscoasa(config-dns-server-group)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
expire-entry-timer	Only available for DefaultDNS. Sets the time added to the TTL value returned by the DNS server to calculate the delete timer.
poll-timer	Only available for DefaultDNS. Specifies the timer to periodically resolve an FQDN defined in a network object.
retries	Specifies the number of times to retry the list of DNS servers when the ASA does not receive a response.
show running-config dns server-group	Shows the current running DNS server group configuration.
timeout	Specifies the amount of time to wait before trying the next DNS server.

dns-to-domain

To map a DNS server groups to a specific domain, use the **dns-to-domain** command in dns-group-map configuration mode. To remove the mapping, use the **no** form of this command.

dns-to-domain *dns_group_name domain*
no dns-to-domain *dns_group_name domain*

Syntax Description

dns_group_name	Specifies the DNS group name from the **dns server-group** command that you want to use for the associated domain. Do not map any domains to the group you want to use for the default (for example, DefaultDNS).
domain	Specifies the domain for which you want to use the associated DNS server group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dns-group-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	Added this command.

Usage Guidelines

By default, there is a default DNS server group called DefaultDNS. You can create multiple DNS server groups: one group is the default, while other groups can be associated with specific domains by using the **dns-group-map** and **dns-to-domain** commands. A DNS request that matches a domain associated with a DNS server group will use that group. You can create up to 30 mappings.

For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface.

Examples

The following example configures three mappings:

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
```

```
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns server-group mode, in which you can configure a DNS servers.
dns-group-map	Maps DNS server groups to domains.
name-server	Adds a DNS server to a group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns trusted-source

To define the DNS servers that can be trusted to resolve domain names in a network-service object, use the **dns trusted-source** command in global configuration mode. To remove a type of DNS server from the trusted list, use the **no** form of the command.

dns trusted-source { **configured-servers** | **dhcp-client** | **dhcp-pools** | **dhcp-relay** | *ip_list* }

Syntax Description

configured-servers	Specifies that servers configured in DNS server groups should be trusted. A configured server is any server specified in DNS groups or name-server commands.
dhcp-client	Specifies that the servers that are learned by snooping messages between a DHCP client and DHCP server are considered trusted DNS servers. This option applies when you configure the **dhcpd auto_config** command to configure DHCP servers on inside interfaces using the information obtained from device interfaces that use DHCP client to obtain an IP address.
dhcp-pools	Specifies that the DNS servers that are configured in the DHCP pools for clients that obtain addresses through DHCP servers running on the device interfaces should be trusted. These are the servers that are configured on the **dhcpd dns** command, and thus are IPv4 only.
dhcp-relay	Specifies that the servers that are learned by snooping DHCP relay messages between a DHCP client and DHCP server are considered trusted DNS servers.
ip_list	A space separated list of the IP addresses of DNS servers that should be trusted. You can list up to 12 IPv4 and IPv6 addresses. Specify **any** to cover all DNS servers. Use the **no** form of the command to remove a server.

Command Default

By default, all configured and learned DNS servers are trusted (that is, all of these options). You need to change this only if you want to limit the trusted list.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was introduced.

Usage Guidelines

If you configure domain names in network-service objects, the system snoops DNS request/response traffic to gather IP addresses for DNS domain names and caches the results. Any DNS request/response can be snooped.

The records snooped are A, AAAA, and MX. The time-to-live (TTL) of each resolved name is honored within limits: the minimum TTL is 2 minutes, the maximum is 24 hours. This ensures that the cache does not become stale.

For security reasons, you can limit the scope of DNS snooping by defining which DNS servers should be trusted. Any DNS traffic to non-trusted DNS servers is ignored and not used to obtain mappings for network-service objects. By default, all configured and learned DNS servers are trusted; you need to change this only if you want to limit the trusted list.

Example

The following example explicitly trusts the DNS servers at 10.100.10.1 and 10.100.10.2.

```
ciscoasa(config)# dns trusted-source 10.100.10.1 10.100.10.2
```

The following example removes DNS relay servers from the trusted server configuration.

```
ciscoasa(config)# no dns trusted-source dhcp-relay
```

Related Commands

Command	Description
show dns trusted-source	Shows the trusted DNS configuration.

dns update

To start DNS lookup to resolve the designated hostnames without waiting for the expiration of the DNS poll timer, use the **dns update** command in privileged EXEC mode.

dns update [**host** *fqdn_name*] [**timeout seconds** *seconds*]

Syntax Description

host *fqdn_name*	Specifies the fully qualified domain name of the host on which to run DNS updates.
timeout seconds *seconds*	Specifies the timeout in seconds.

Command Default

By default, the timeout is 30 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command immediately starts a DNS lookup to resolve the designated hostnames without waiting for the expiration of the DNS poll timer. When you run DNS update without specifying an option, all activated host groups and FQDN hosts are selected for DNS lookup. When the command finishes running, the ASA displays [Done] at the command prompt and generates a syslog message.

When the update operation starts, a starting update log is created. When the update operation finishes or is aborted after the timer has expired, another syslog message is generated. Only one outstanding DNS update operation is allowed.

Examples

The following example performs a DNS update:

```
ciscoasa# dns update
ciscoasa# ...
ciscoasa# [Done] dns update
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.

Command	Description
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

domain

To configure a DNS domain name for a network-service object or object group, use the **domain** command in object configuration mode. Use the **no** form of this command to remove the domain from the configuration.

domain *domain_name* [*service*]
no domain *domain_name* [*service*]

Syntax Description

domain_name	The DNS name, up to 253 characters. This can be fully-qualified (such as www.example.com) or partial (such as example.com), in which case the object matches all subdomains, that is, servers with the partial name (such as www.example.com, www1.example.com, long.server.name.example.com, and so forth). Connections will be matched against the longest name if an exact match is available. The domain name can resolve to multiple IP addresses.
service	(Optional.) Specify the service only if you want to limit the scope of the connections matched. By default, any connection to the resolved IP addresses for the domain name matches the object. *protocol* [*operator port*] where: • *protocol* is the protocol used in the connection, such as tcp, udp, ip, and so forth. Use ? to see the list of protocols. • (TCP/UDP only.) *operator* is one of the following: • **eq** equals the port number specified. • **lt** means any port less than the specified port number. • **gt** means any port greater than the specified port number. • **range** means any port between the two ports specified. • (TCP/UDP only.) *port* is the port number, 1-65535 or a mnemonic, such as www. Use ? to see the mnemonics. For ranges, you must specify two ports, with the first port being a lower number than the second port.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network-service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was introduced.

Usage Guidelines

You must configure DNS servers and enable domain lookup services on the device interfaces so that the system can request IP addresses for the domain names.

Example

The following example creates several network-service objects that include domain names.

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

Related Commands

Command	Description
object network-service	Creates a network-service object.
object-group network-service	Creates a network-service object group.

domain-name (dns server-group)

To set the default domain name to append to unqualified hostnames, use the **domain-name** command in dns server-group configuration mode. To remove the domain name, use the **no** form of this command.

domain-name*name*
no domain-name [*name*]

Syntax Description

name	Sets the domain name, up to 63 characters.

Command Default

The default domain name is default.domain.invalid.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dns server-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name of “jupiter,” then the ASA qualifies the name to “jupiter.example.com.”

Examples

The following example sets the domain to “example.com” for “dnsgroup1”:

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# domain-name example.com
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group configuration mode, in which you can configure a DNS server group.
domain-name	Sets the default domain name globally.
show running-config dns-server group	Shows one or all the current DNS server group configurations.

domain-name (global)

To set the default domain name, use the **domain-name** command in global configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *name*
no domain-name [*name*]

Syntax Description

name	Sets the domain name, up to 63 characters.

Command Default

The default domain name is default.domain.invalid.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to "example.com" and specify a syslog server by the unqualified name of "jupiter," then the ASA qualifies the name to "jupiter.example.com." For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

Examples

The following example sets the domain to example.com:

```
ciscoasa(config)# domain-name example.com
```

Related Commands

Command	Description
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Identifies a DNS server for the ASA.
hostname	Sets the ASA hostname.
show running-config domain-name	Shows the domain name configuration.

domain-name (ipv6 dhcp pool)

To provide the domain name to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **domain-name** command in ipv6 dhcp pool configuration mode. To remove the domain name, use the **no** form of this command.

domain-name*domain_name*
no domain-name *domain_name*

Syntax Description

domain_name	Specifies the domain name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the domain name, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
```

```
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.

Command	Description
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

domain-password

To configure the IS-IS routing domain authentication password, use the **domain-password** command in router isis configuration mode. To disable a password, use the **no** form of this command.

domain-name *password* [**authenticate snp** { **validate** | **send-only** }]
no domain-name *password*

Syntax Description

password	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into SNP PDUs.
validate	(Optional) Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	(Optional) Causes the system only to insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Command Default

No domain password is specified and no authentication is enabled for exchange of Level 2 routing information.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 2 (area router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an authentication password to the routing domain and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.

Command	Description
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.

Command	Description
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

downgrade

To downgrade your software version, use the **downgrade** command in global configuration mode.

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

Syntax Description

activation-key *old_key*	(Optional) If you need to revert the activation key, then you can enter the old activation key.
old_config_url	Specifies the path to the saved, pre-migration configuration (by default this was saved on disk0).
old_image_url	Specifies the path to the old image on disk0, disk1, tftp, ftp, or smb.
/noconfirm	(Optional) Downgrades without prompting.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

This command is a shortcut for completing the following functions:

1. Clearing the boot image configuration (**clear configure boot**).
2. Setting the boot image to be the old image (**boot system**).
3. (Optional) Entering a new activation key (**activation-key**).
4. Saving the running configuration to startup (**write memory**). This sets the BOOT environment variable to the old image, so when you reload, the old image is loaded.
5. Copying the old configuration to the startup configuration (**copy** *old_config_url* **startup-config**).
6. Reloading (**reload**).

Examples

The following example downgrades without confirming:

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

Related Commands

Command	Description
activation-key	Enters an activation key.
boot system	Sets the image to boot from.
clear configure boot	Clears the boot image configuration.
copy startup-config	Copies a configuration to the startup configuration.

download-max-size

Note The **download-max-size** command does not work. Do not use it. However, you might see it in the running configuration, and it is available in the CLI.

To specify the maximum size allowed for an object to download, use the **download-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

download-max-size*size*
no download-max-size

Syntax Description

size	Specifies the maximum size allowed for a downloaded object. The range is 0 through 2147483647. Setting the size to 0 effectively disallows object downloading.

Command Default

The default size is 2147483647.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example sets the maximum size for a downloaded object to 1500 bytes:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
download-max-size 1500
```

Related Commands

Command	Description
post-max-size	Specifies the maximum size of an object to post.
upload-max-size	Specifies the maximum size of an object to upload.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

drop

To drop all packets that match the **match** command or **class** command, use the **drop** command in match or class configuration mode. To disable this action, use the no form of this command.

drop [**send-protocol-error**] [**log**]
no drop [**send-protocol-error**] [**log**]

Syntax Description

log	Logs the match. The syslog message number depends on the application.
send-protocol-error	Sends a protocol error message.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

When using the Modular Policy Framework, drop packets that match a **match** command or class map by using the **drop** command in match or class configuration mode. This drop action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action.

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop** command to drop all packets that match the **match** command or **class** command.

If you drop a packet, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example drops packets and sends a log when they match the HTTP traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

drop-connection

When using the Modular Policy Framework, drop packets and close the connection for traffic that matches a **match** command or class map by using the **drop-connection** command in match or class configuration mode. To disable this action, use the no form of this command.

drop-connection [**send-protocol-error**] [**log**]
no drop-connection [**send-protocol-error**] [**log**]

Syntax Description

send-protocol-error	Sends a protocol error message.
log	Logs the match. The system log message number depends on the application.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The connection will be removed from the connection database on the ASA. Any subsequent packets entering the ASA for the dropped connection will be discarded. This drop-connection action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop-connection** command to drop packets and close the connection for traffic that matches the **match** command or **class** command.

If you drop a packet or close a connection, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet and close the connection, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop-connection** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action. For example, enter the **inspect http http_policy_map** command, where http_policy_map is the name of the inspection policy map.

Examples

The following example drops packets, closes the connection, and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

dtls port

To specify a port for DTLS connections, use the **dtls port** command from webvpn configuration mode. To remove the command from the configuration, use the **no** form of this command:

dtls port *number*
no dtls port *number*

Syntax Description

number	The UDP port number, from 1 to 65535.

Command Default

The default port number is 443.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

This command specifies the UDP port to be used for SSL VPN connections using DTLS.

DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Examples

The following example enters webvpn configuration mode and specifies port 444 for DTLS:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# dtls port 444
```

Related Commands

Command	Description
dtls enable	Enables DTLS on an interface.
svc dtls	Enables DTLS for groups or users establishing SSL VPN connections.
vpn-tunnel-protocol	Specifies VPN protocols that the ASA allows for remote access, including SSL.

duplex

To set the duplex of a copper (RJ-45) Ethernet interface, use the **duplex** command in interface configuration mode. To restore the duplex setting to the default, use the **no** form of this command.

duplex { **auto** | **full** | **half** }
no duplex

Syntax Description

auto	Auto-detects the duplex mode.
full	Sets the duplex mode to full duplex.
half	Sets the duplex mode to half duplex.

Command Default

The default is auto detect.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

Set the duplex mode on the physical interface only.

The **duplex** command is not available for fiber media.

If your network does not support auto detection, set the duplex mode to a specific value.

For RJ-45 interfaces on the ASA 5500 series, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the duplex to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Examples

The following example sets the duplex mode to full duplex:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

dynamic-access-policy-config

To configure a DAP record and the access policy attributes associated with it, use the **dynamic-access-policy-config** command in global configuration mode. To remove an existing DAP configuration, use the **no** form of this command.

dynamic-access-policy-config *name* | *activate*
no dynamic-access-policy-config

Syntax Description

activate	Activates the DAP selection configuration file.
name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration (name)	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC (activate)	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **dynamic-access-policy-config** command in global configuration mode to create one or more DAP records. To activate a DAP selection configuration file, use the **dynamic-access-policy-config** command with the *activate* argument.

When you use this command, you enter dynamic-access-policy-record mode, in which you can set attributes for the named DAP record. The commands you can use in dynamic-access-policy-record mode include the following:

- **action**
- **description**
- **network-acl**

- **priority**
- **user-message**
- **webvpn**

Examples

The following example shows how to configure the DAP record named user1:

```
ciscoasa
(config)
# dynamic-access-policy-config user1
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Populates the DAP record with access policy attributes.
show running-config dynamic-access-policy-record	Displays the running configuration for all DAP records, or for the named DAP record.

dynamic-access-policy-record

To create a DAP record and populate it with access policy attributes, use the **dynamic-access-policy-record** command in global configuration mode. To remove an existing DAP record, use the **no** form of this command.

dynamic-access-policy-record*name*
no dynamic-access-policy-record *name*

Syntax Description

name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **dynamic-access-policy-record** command in global configuration mode to create one or more DAP records. When you use this command, you enter dynamic-access-policy-record mode, in which you can set attributes for the named DAP record. The commands you can use in dynamic-access-policy-record mode include the following:

- **action** (**continue**, **terminate**, or **quarantine**)
- **description**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

Examples

The following example shows how to create a DAP record named Finance.

```
ciscoasa
(config)
```

```
# dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
clear config dynamic-access-policy-record	Removes all DAP records or the named DAP record.
dynamic-access-policy-config url	Configures the DAP Selection Configuration file.
show running-config dynamic-access-policy-record	Displays the running configuration for all DAP records, or for the named DAP record.

dynamic-authorization

To enable RADIUS dynamic authorization (change of authorization) services for the AAA server group, use the **dynamic-authorization** command in aaa-server group configuration mode. To disable dynamic authorization, use the **no** form of this command.

dynamic-authorization [**port** *number*]
no dynamic-authorization [**port** *number*]

Syntax Description

port *number*	(Optional) Specifies the dynamic authorization port on the ASA. It can range from 1024 to 65535.

Command Default

The default listening port is 1700. By default dynamic-authorization is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to configure a RADIUS server group for ISE Change of Authorization (CoA). Once defined, the corresponding RADIUS server group will be registered for CoA notification and the ASA will listen to the port for the CoA policy updates from ISE.

The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is no longer required to apply access control lists (ACLs) for each VPN session established with the ASA.

When an end user requests a VPN connection, the ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network. An accounting start message is sent to the ISE to register the session. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA. The ISE sends a policy update to the ASA via a CoA “policy push.” This identifies a new user ACL that provides increased network access privileges. Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates.

Examples

The following example shows how to configure an ISE server group for dynamic authorization (CoA) updates and hourly periodic accounting. Included is the tunnel group configuration that configures password authentication with ISE.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE. In this case, you include the **authorize-only** command in the server group configuration, because the server group will not be used for authentication.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Related Commands

Command	Description
authorize-only	Enables authorize-only mode for the RADIUS server group.
interim-accounting-update	Enables the generation of RADIUS interim-accounting-update messages.
without-csd	Switches off hostscan processing for connections that are made to a specific tunnel-group.

dynamic-filter ambiguous-is-black

To treat Botnet Traffic Filter greylisted traffic as blacklisted traffic for dropping purposes, use the **dynamic-filter ambiguous-is-black** command in global configuration mode. To allow greylisted traffic, use the **no** form of this command.

dynamic-filter ambiguous-is-black
no dynamic-filter ambiguous-is-black

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

If you configured the **dynamic-filter enable** command and then the **dynamic-filter drop blacklist** command, this command treats greylisted traffic as blacklisted traffic for dropping purposes. If you do not enable this command, greylisted traffic will not be dropped.

Ambiguous addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. These addresses are on the greylist.

Examples

The following example monitors all port 80 traffic on the outside interface, and then drops blacklisted and greylisted traffic at a threat level of moderate or greater:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
ciscoasa(config)# dynamic-filter ambiguous-is-black
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.

Command	Description
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.

Command	Description
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter blacklist

To edit the Botnet Traffic Filter blacklist, use the **dynamic-filter blacklist** command in global configuration mode. To remove the blacklist, use the **no** form of this command.

dynamic-filter blacklist
no dynamic-filter blacklist

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

After you enter the dynamic-filter blacklist configuration mode, you can manually enter domain names or IP addresses (host or subnet) that you want to tag as bad names in a blacklist using the **address** and **name** commands. You can also enter names or IP addresses in a whitelist (see the **dynamic-filter whitelist** command), so that names or addresses that appear on both the dynamic blacklist and whitelist are identified only as whitelist addresses in syslog messages and reports. Note that you see syslog messages for whitelisted addresses even if the address is not also in the dynamic blacklist.

Static blacklist entries are always designated with a Very High threat level.

When you add a domain name to the static database, the ASA waits 1 minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the *DNS host cache* . (This action is a background process, and does not affect your ability to continue configuring the ASA). We recommend also enabling DNS packet inspection with Botnet Traffic Filter snooping (see the **inspect dns dynamic-filter-snooping** command). The ASA uses Botnet Traffic Filter snooping instead of the regular DNS lookup to resolve static blacklist domain names in the following circumstances:

- The ASA DNS server is unavailable.
- A connection is initiated during the 1-minute waiting period before the ASA sends the regular DNS request.

If DNS snooping is used, when an infected host sends a DNS request for a name on the static database, the ASA looks inside the DNS packets for the domain name and associated IP address and adds the name and IP address to the DNS reverse lookup cache.

The static database lets you augment the dynamic database with domain names or IP addresses that you want to blacklist.

If you do not enable Botnet Traffic Filter snooping, and one of the above circumstances occurs, then that traffic will not be monitored by the Botnet Traffic Filter.



Note This command requires ASA use of a DNS server; see the **dns domain-lookup** and **dns server-group** commands.

Examples

The following example creates entries for the blacklist and whitelist:

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.

Command	Description
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter database fetch

To test the download of the dynamic database for the Botnet Traffic Filter, use the **dynamic-filter database fetch** command in privileged EXEC mode.

dynamic-filter database fetch

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The actual database is not stored on the ASA; it is downloaded and then discarded. Use this command for testing purposes only.

Examples

The following example tests the download of the dynamic database:

```
ciscoasa# dynamic-filter database fetch
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.

Command	Description
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter database find

To check if a domain name or IP address is included in the dynamic database for the Botnet Traffic Filter, use the **dynamic-filter database find** command in privileged EXEC mode.

dynamic-filter database find *string*

Syntax Description

string	The *string* can be the complete domain name or IP address, or you can enter part of the name or address, with a minimum search string of 3 characters. Regular expressions are not supported for the database search.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

If there are multiple matches, the first two matches are shown. To refine your search for a more specific match, enter a longer string.

Examples

The following example searches on the string “example.com,” and finds one match:

```
ciscoasa# dynamic-filter database find bad.example.com
   bad.example.com
Found 1 matches
```

The following example searches on the string “bad,” and finds more than two matches:

```
ciscoasa# dynamic-filter database find bad
   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

Related Commands

Command	Description
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.

Command	Description
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.

Command	Description
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter database purge

To manually delete the Botnet Traffic Filter dynamic database from running memory, use the **dynamic-filter database purge** command in privileged EXEC mode.

dynamic-filter database purge

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The database files are stored in running memory; they are not stored in flash memory. If you need to delete the database, use the **dynamic-filter database purge** command.

Before you can purge the database files, disable use of the database using the **no dynamic-filter use-database** command.

Examples

The following example disables use of the database, and then purges the database:

```
ciscoasa(config)# no dynamic-filter use-database
ciscoasa(config)# dynamic-filter database purge
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.

Command	Description
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter drop blacklist

To automatically drop blacklisted traffic using the Botnet Traffic Filter, use the **dynamic-filter drop blacklist** command in global configuration mode. To disable the automatic dropping, use the **no** form of this command.

dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** { **eq** *level* | **range** *min max* }]
no dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** { **eq** *level* | **range** *min max* }]

Syntax Description

action-classify-list *sub_access_list*	(Optional) Identifies a subset of traffic that you want to drop . See the **access-list extended** command to create the access list. The dropped traffic must always be equal to or a subset of the monitored traffic identified by the **dynamic-filter enable** command. For example, if you specify an access list for the **dynamic-filter enable** command, and you specify the **action-classify-list** for this command, then it must be a subset of the **dynamic-filter enable** access list.
interface *name*	(Optional) Limits monitoring to a specific interface. The dropped traffic must always be equal to or a subset of the monitored traffic identified by the **dynamic-filter enable** command. Any interface-specific commands take precedence over the global command.
threat-level {**eq** *level* | **range** *min max* }	(Optional) Limits the traffic dropped by setting the threat level. If you do not explicitly set a threat level, the level used is **threat-level range moderate very-high**. **Note** We highly recommend using the default setting unless you have strong reasons for changing the setting. The *level* and *min* and *max* options are: • **very-low** • **low** • **moderate** • **high** • **very-high** **Note** Static blacklist entries are always designated with a Very High threat level.

Command Default

This command is disabled by default.

The default threat level is **threat-level range moderate very-high**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

Be sure to first configure a **dynamic-filter enable** command for any traffic you want to drop; the dropped traffic must always be equal to or a subset of the monitored traffic.

You can enter this command multiple times for each interface and global policy. Make sure you do not specify overlapping traffic in multiple commands for a given interface/global policy. Because you cannot control the exact order that commands are matched, overlapping traffic means you do not know which command will be matched. For example, do not specify both a command that matches all traffic (without the **action-classify-list** keyword) as well as a command with the **action-classify-list** keyword for a given interface. In this case, the traffic might never match the command with the **action-classify-list** keyword. Similarly, if you specify multiple commands with the **action-classify-list** keyword, make sure each access list is unique, and that the networks do not overlap.

Examples

The following example monitors all port 80 traffic on the outside interface, and then drops traffic at a threat level of moderate or greater:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.

Command	Description
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter enable

To enable the Botnet Traffic Filter, use the **dynamic-filter enable** command in global configuration mode. To disable the Botnet Traffic Filter, use the **no** form of this command.

dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]
no dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

Syntax Description

classify-list *access_list*	Identifies the traffic that you want to monitor using an extended access list (see the **access-list extended** command). If you do not create an access list, by default you monitor all traffic.
interface *name*	Limits monitoring to a specific interface.

Command Default

The Botnet Traffic Filter is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The Botnet Traffic Filter compares the source and destination IP address in each initial connection packet to the IP addresses in the dynamic database, static database, DNS reverse lookup cache, and DNS host cache, and sends a syslog message or drops any matching traffic.

Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity. You can also supplement the dynamic database with a static database by entering IP addresses or domain names in a local “blacklist” or “whitelist.”

The DNS snooping is enabled separately (see the **inspect dns dynamic-filter-snoop** command). Typically, for maximum use of the Botnet Traffic Filter, you need to enable DNS snooping, but you can use Botnet Traffic Filter logging independently if desired. Without DNS snooping for the dynamic database, the Botnet Traffic Filter uses only the static database entries, plus any IP addresses in the dynamic database; domain names in the dynamic database are not used.

Botnet Traffic Filter Address Categories

Addresses monitored by the Botnet Traffic Filter include:

- Known malware addresses—These addresses are on the "blacklist."
- Known allowed addresses—These addresses are on the "whitelist."
- Ambiguous addresses—These addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. These addresses are on the "greylist."
- Unlisted addresses—These addresses are unknown, and not included on any list.

Botnet Traffic Filter Actions for Known Addresses

You can configure the Botnet Traffic Filter to log suspicious activity using the **dynamic-filter enable** conmmand, and you can optionally configure it to block suspicious traffic automatically using the **dynamic-filter drop blacklist** command.

Unlisted addresses do not generate any syslog messages, but addresses on the blacklist, whitelist, and greylist generate syslog messages differentiated by type. The Botnet Traffic Filter generates detailed syslog messages numbered 338*nnn* . Messages differentiate between incoming and outgoing connections, blacklist, whitelist, or greylist addresses, and many other variables. (The greylist includes addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist.)

See the syslog messages guide for detailed information about syslog messages.

Device Support

You can enable the Botnet Traffic Filter on the following device models:

- ASA 5505
- ASA 5510, 5520, 5540, 5550
- ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X
- ASA 5580
- ASA 5585-X
- ASASM

Examples

The following example monitors all port 80 traffic on the outside interface, and then drops traffic at a threat level of moderate or greater:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.

Command	Description
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter updater-client enable

To enable downloading of the dynamic database from the Cisco update server for the Botnet Traffic Filter, use the **dynamic-filter updater-client enable** command in global configuration mode. To disable downloading of the dynamic database, use the **no** form of this command.

dynamic-filter updater-client enable
no dynamic-filter updater-client enable

Syntax Description

This command has no arguments or keywords.

Command Default

Downloading is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

If you do not have a database already installed on the ASA, it downloads the database after approximately 2 minutes. The update server determines how often the ASA polls the server for future updates, typically every hour.

The Botnet Traffic Filter can receive periodic updates for the dynamic database from the Cisco update server.

This database lists thousands of known bad domain names and IP addresses. When the domain name in a DNS reply matches a name in the dynamic database, the Botnet Traffic Filter adds the name and IP address to the *DNS reverse lookup cache* . When the infected host starts a connection to the IP address of the malware site, then the ASA sends a syslog message informing you of the suspicious activity.

To use the database, be sure to configure a domain name server for the ASA so that it can access the URL. To use the domain names in the dynamic database, you need to enable DNS packet inspection with Botnet Traffic Filter snooping; the ASA looks inside the DNS packets for the domain name and associated IP address.

In some cases, the IP address itself is supplied in the dynamic database, and the Botnet Traffic Filter logs any traffic to that IP address without having to inspect DNS requests.

The database files are stored in running memory; they are not stored in flash memory. If you need to delete the database, use the **dynamic-filter database purge** command.

Note This command requires ASA use of a DNS server; see the **dns domain-lookup** and **dns server-group** commands.

Examples

The following multiple mode example enables downloading of the dynamic database, and enables use of the database in context1 and context2:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

The following single mode example enables downloading of the dynamic database, and enables use of the database:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns name-server	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.

Command	Description
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter use-database

To enable use of the dynamic database for the Botnet Traffic Filter, use the **dynamic-filter use-database** command in global configuration mode. To disable use of the dynamic database, use the **no** form of this command.

dynamic-filter use-database
no dynamic-filter use-database

Syntax Description

This command has no arguments or keywords.

Command Default

Use of the database is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Disabling use of the downloaded database is useful in multiple context mode, so you can configure use of the database on a per-context basis. To enable downloading of the dynamic database, see the **dynamic-filter updater-client enable** command.

Examples

The following multiple mode example enables downloading of the dynamic database, and enables use of the database in context1 and context2:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

The following single mode example enables downloading of the dynamic database, and enables use of the database:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.

Command	Description
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter whitelist

To edit the Botnet Traffic Filter whitelist, use the **dynamic-filter whitelist** command in global configuration mode. To remove the whitelist, use the **no** form of this command.

dynamic-filter whitelist
no dynamic-filter whitelist

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The static database lets you augment the dynamic database with domain names or IP addresses that you want to whitelist. After you enter the dynamic-filter whitelist configuration mode, you can manually enter domain names or IP addresses (host or subnet) that you want to tag as good names in a whitelist using the **address** and **name** commands. Names or addresses that appear on both the dynamic blacklist and static whitelist are identified only as whitelist addresses in syslog messages and reports. Note that you see syslog messages for whitelisted addresses even if the address is not also in the dynamic blacklist. You can enter names or IP addresses in the static blacklist using the **dynamic-filter blacklist** command.

When you add a domain name to the static database, the ASA waits 1 minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the *DNS host cache* . (This action is a background process, and does not affect your ability to continue configuring the ASA). We recommend also enabling DNS packet inspection with Botnet Traffic Filter snooping (see the **inspect dns dynamic-filter-snooping** command). The ASA uses Botnet Traffic Filter snooping instead of the regular DNS lookup to resolve static blacklist domain names in the following circumstances:

- The ASA DNS server is unavailable.
- A connection is initiated during the 1 minute waiting period before the ASA sends the regular DNS request.

If DNS snooping is used, when an infected host sends a DNS request for a name on the static database, the ASA looks inside the DNS packets for the domain name and associated IP address and adds the name and IP address to the DNS reverse lookup cache.

If you do not enable Botnet Traffic Filter snooping, and one of the above circumstances occurs, then that traffic will not be monitored by the Botnet Traffic Filter.



Note This command requires ASA use of a DNS server; see the **dns domain-lookup** and **dns server-group** commands.

Examples

The following example creates entries for the blacklist and whitelist:

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.

Command	Description
dynamic-filter use-database	Enables use of the dynamic database.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.



PART IV

E - H Commands

- e, on page 1403
- fa – fd, on page 1519
- fe – fz, on page 1595
- g – h, on page 1683



e

- echo, on page 1405
- early-message, on page 1407
- eigrp log-neighbor-changes, on page 1409
- eigrp log-neighbor-warnings, on page 1410
- eigrp router-id, on page 1412
- eigrp stub, on page 1414
- eject, on page 1417
- email, on page 1419
- enable (cluster group), on page 1420
- enable (user EXEC), on page 1422
- enable e-mail proxy (Deprecated), on page 1424
- enable gprs, on page 1425
- enable password, on page 1426
- enable webvpn, on page 1429
- encapsulation, on page 1430
- encryption, on page 1432
- endpoint, on page 1434
- endpoint-mapper, on page 1435
- enforcenextupdate, on page 1436
- enrollment protocol scep cmp est acme url, on page 1437
- enrollment-retrieval, on page 1439
- enrollment retry count, on page 1441
- enrollment retry period, on page 1443
- enrollment terminal, on page 1444
- enrollment url (Deprecated), on page 1446
- eool, on page 1448
- eou allow (Deprecated), on page 1450
- eou clientless (Deprecated), on page 1452
- eou initialize (Deprecated), on page 1454
- eou max-retry (Deprecated), on page 1456
- eou port (Deprecated), on page 1458
- eou revalidate (Deprecated), on page 1460
- eou timeout (Deprecated), on page 1462

- erase, on page 1464
- esp, on page 1466
- established, on page 1468
- event crashinfo, on page 1471
- event manager applet, on page 1473
- event memory-logging-wrap, on page 1474
- event none, on page 1475
- event syslog id, on page 1476
- event timer, on page 1478
- exceed-mss, on page 1480
- exempt-list, on page 1482
- exit, on page 1484
- exp-flow-control, on page 1485
- expire-entry-timer, on page 1487
- expiry-time, on page 1489
- exp-measure, on page 1491
- export, on page 1493
- export webvpn AnyConnect-customization, on page 1495
- export webvpn customization, on page 1497
- export webvpn plug-in, on page 1499
- export webvpn mst-translation, on page 1501
- export webvpn translation-table, on page 1503
- export webvpn url-list, on page 1506
- export webvpn webcontent, on page 1508
- extended-security, on page 1510
- external-browser, on page 1512
- external-port, on page 1514
- external-segment-id, on page 1516

echo

To configure echo in a BFD single-hop template, use the echo command in BFD template configuration mode. To disable echo in BFD template for single-hop sessions, use the **no** form of this command.

echo
no echo

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
BFD configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to enable echo mode functionality in a single-hop template only. BFD echo is not supported for IPv6 BFD sessions.

Examples

The following example configures echo for a single-hop BFD template.

```
ciscoasa(config)# bfd-template single-hop template1
ciscoasa(config-bfd)# echo
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.

Command	Description
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

early-message

To allow messages before the H.255 SETUP message during H.323 inspection, use the **early-message** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

early-message*message_type*
no early-message *message_type*

Syntax Description

message_type	The type of message to allow before the H.225 SETUP message. You can enter the following types: • **facility**

Command Default

The command is disabled. Messages before the H.225 SETUP message are not allowed, resulting in dropped connections.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was introduced.

Usage Guidelines

H.460.18 defines a method for traversal of H.323 signaling across network address translators and firewalls. This method allows the H.225 FACILITY message to be sent before the H.225 SETUP message. If you encounter call setup issues, where connections are being closed before being completed when using H.323/H.225, use this command to allow early messages.

Also, ensure that you enable inspection for both H.323 RAS and H.225 (they are both enabled by default).

Examples

The following example shows how to allow early messages:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# early-message FACILITY
```

Related Commands

Command	Description
policy-map type inspect	Creates an inspection policy map.

Command	Description
show running-config policy-map	Display all current policy map configurations.

eigrp log-neighbor-changes

To enable the logging of EIGRP neighbor adjacency changes, use the **eigrp log-neighbor-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-changes
no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for EIGRP IPv6 was added.

Usage Guidelines

The **eigrp log-neighbor-changes** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor changes:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-changes
```

Related Commands

Command	Description
eigrp log-neighbor-warnings	Enables logging of neighbor warning messages.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp log-neighbor-warnings

To enable the logging of EIGRP neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]
no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. Valid values are from 1 to 65535. Repeated warnings are not logged if they occur during this interval.

Command Default

This command is enabled by default. All neighbor warning messages are logged.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for EIGRP IPv6 was added.

Usage Guidelines

The **eigrp log-neighbor-warnings** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor warning messages:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-warnings
```

The following example logs EIGRP neighbor warning messages and repeats the warning messages in 5-minute (300 seconds) intervals:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
eigrp log-neighbor-messages	Enables the logging of changes in EIGRP neighbor adjacencies.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp router-id

To specify router ID used by the EIGRP routing process, use the **eigrp router-id** command in router configuration mode. To restore the default value, use the **no** form of this command.

eigrp router-id *ip-address*
no eigrp router-id [*ip-address*]

Syntax Description

ip-address	Router ID in IP address (dotted-decimal) format. You cannot use 0.0.0.0 or 255.255.255.255 as the router ID.

Command Default

If not specified, the highest-level IP address on the ASA is used as the router ID.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for configuring EIGRP with IPv6 address was added.

Usage Guidelines

If the **eigrp router-id** command is not configured, EIGRP automatically selects the highest IP address on the ASA to use as the router ID when an EIGRP process is started. The router ID is not changed unless the EIGRP process is removed using the **no router eigrp** command or unless the router ID is manually configured with the **eigrp router-id** command.

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. To prevent this, use the **eigrp router-id** command to specify a global address for the router ID.

A unique value should be configured for each EIGRP router.

Examples

The following example configures 172.16.1.3 as a fixed router ID for the EIGRP routing process:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp stub

To configure the EIGRP routing process as a stub routing process, use the **eigrp stub** command in router configuration mode. To remove EIGRP stub routing, use the **no** form of this command.

eigrp stub [**receive-only**] | { [**connected**] [**redistributed**] [**static**] [**summary**] }
no eigrp stub [**receive-only**] | { [**connected**] [**redistributed**] [**static**] [**summary**] }

Syntax Description

connected	(Optional) Advertises connected routes.
receive-only	(Optional) Sets the ASA as a received-only neighbor.
redistributed	(Optional) Advertises routes redistributed from other routing protocols.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.

Command Default

Stub routing is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for IPv6 routing was added.

Usage Guidelines

Use the **eigrp stub** command to configure the ASA as a stub where the ASA directs all IP traffic to a distribution router.

Using the **receive-only** keyword restricts the ASA from sharing any of its routes with any other router in the autonomous system; the ASA only receives updates from the EIGRP neighbor. You cannot use any other keyword with the **receive-only** keyword.

You can specify one or more of the **connected**, **static**, **summary**, and **redistributed** keywords. If any of these keywords is used with the **eigrp stub** command, only the route types specified by the particular keyword are sent.

The **connected** keyword permits the EIGRP stub routing process to send connected routes. If the connected routes are not covered by a **network** statement, it may be necessary to redistribute connected routes with the **redistribute** command under the EIGRP process.

The **static** keyword permits the EIGRP stub routing process to send static routes. Without the configuration of this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. You must still redistribute static routes using the **redistribute static** command.

The **summary** keyword permits the EIGRP stub routing process to send summary routes. You can create summary routes manually with the **summary-address eigrp** command or automatically with the **auto-summary** command enabled (this command is enabled by default).

The **redistributed** keyword permits the EIGRP stub routing process to send routes redistributed into the EIGRP routing process from other routing protocols. If you do you configure this option, EIGRP does not advertise redistributed routes.

Examples

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that advertises connected and summary routes:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected summary
```

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that advertises connected and static routes. Sending summary routes is not permitted.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected static
```

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that only receives EIGRP updates. Connected, summary, and static route information is not sent.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 eigrp

ciscoasa(config-router)# eigrp stub receive-only
```

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that advertises routes redistributed into EIGRP from other routing protocols:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub redistributed
```

The following example uses the **eigrp stub** command without any of the optional arguments. When used without arguments, the **eigrp stub** commands advertises connected and static routes by default.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub
```

Related Commands

Command	Description
router eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

eject

To support the removal of an ASA external compact flash device, use the **eject** command in user EXEC mode.

eject [**/noconfirm**] *disk1:*

Syntax Description

disk1:	Specifies the device to eject.
/noconfirm	Specifies that you do not need to confirm device removal before physically removing the external flash device from the ASA.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **eject** command allows you to safely remove a compact flash device from an ASA 5500 series.

The following example shows how to use the **eject** command to shut down *disk1* gracefully before the device is physically removed from the ASA:

```
ciscoasa
#
eject /noconfig disk1:
It is now safe to remove disk1:
ciscoasa
#
show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34
Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"
wef5520 up 5 hours 36 mins
Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

Related Commands

Command	Description
show version	Displays information about the operating system software.

email

To include the indicated e-mail address in the Subject Alternative Name extension of the certificate during enrollment, use the **email** command in crypto ca-trustpoint configuration mode. To restore the default setting, use the **no** form of this command.

email*address*
no email

Syntax Description

address	Specifies the e-mail address. The maximum length is 64 characters.

Command Default

The default setting is not set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuratio	• Yes	• Yes	• Yes	• —	• —

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and includes the e-mail address user1@user.net in the enrollment request for the trustpoint central:

```
ciscoasa(config)# crypto ca-trustpoint central
ciscoasa(ca-trustpoint)# email user1@user.net
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca-trustpoint	Enters crypto ca-trustpoint configuration mode.

enable (cluster group)

To enable clustering, use the **enable** command in cluster group configuration mode. To disable clustering, use the **no** form of this command.

enable [**as-slave** | **noconfirm**]
no enable

Syntax Description

as-slave	(Optional) Enables clustering without checking the running configuration for incompatible commands and ensures that the slave joins the cluster with no possibility of becoming the master in any current election. Its configuration is overwritten with the one synced from the master unit.
noconfirm	(Optional) When you enter the **enable** command, the ASA scans the running configuration for incompatible commands for features that are not supported with clustering, including commands that may be present in the default configuration. You are prompted to delete the incompatible commands. If you respond **No**, then clustering is not enabled. Use the **noconfirm** keyword to bypass the confirmation and delete incompatible commands automatically.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

For the first unit enabled, a master unit election occurs. Because the first unit should be the only member of the cluster so far, it will become the master unit. Do not perform any configuration changes during this period.

If you already have a master unit, and are adding slave units to the cluster, you can avoid any configuration incompatibilities (primarily the existence of any interfaces not yet configured for clustering) by using the **enable as-slave** command.

To disable clustering, enter the **no enable** command.

Note If you disable clustering, all data interfaces are shut down, and only the management interface is active. If you want to remove the unit from the cluster entirely (and thus want to have active data interfaces), you need to remove the entire cluster group configuration.

Examples

The following example enables clustering and removes incopatible configuration:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y
INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

enable (user EXEC)

To enter privileged EXEC mode, use the **enable** command in user EXEC mode.

enable [*level*]

Syntax Description

level (Optional) The privilege level between 0 and 15. Not used with enable authentication (the **aaa authentication enable console** command).

Command Default

Enters privilege level 15 unless you are using enable authentication (using the **aaa authentication enable console** command), in which case the default level depends on the level configured for your username.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The default enable password is blank. See the **enable password** command to set the password.

Without enable authentication, when you enter the **enable** command, your username changes to enable_*level* , where the default level is 15. With enable authentication (using the **aaa authentication enable console** command), the username and associated level are preserved. Preserving the username is important for command authorization (the **aaa authorization command** command, using either local or TACACS+).

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode. To use levels in between, enable local command authorization (the **aaa authorization command LOCAL** command) and set the commands to different privilege levels using the **privilege** command. TACACS+ command authorization does not use the privilege levels configured on the ASA.

See the **show curpriv** command to view your current privilege level.

Enter the **disable** command to exit privileged EXEC mode.

Examples

The following example enters privileged EXEC mode:

```
ciscoasa> enable
Password: Pa$$w0rd
ciscoasa#
```

The following example enters privileged EXEC mode for level 10:

```
ciscoasa> enable 10
Password: Pa$$w0rd10
ciscoasa#
```

Related Commands

Command	Description
enable password	Sets the enable password.
disable	Exits privileged EXEC mode.
aaa authorization command	Configures command authorization.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.

enable e-mail proxy (Deprecated)



Note The last supported release for this command as 9.5(1).

To enable e-mail proxy access on a previously configured interface, use the **enable** command. For e-mail proxies (IMAP4S. POP3S, and SMTPS), use this command in the applicable e-mail proxy configuration mode. To disable e-mail proxy access on an interface, use the **no** form of the command.

enable*ifname*
no enable

Syntax Description

ifname Identifies the previously configured interface. Use the **nameif** command to configure interfaces.

Command Default

There are no default values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Examples

The following example shows how to configure POP3S e-mail proxy on the interface named Outside:

```
ciscoasa (config)# pop3s ciscoasa(config-pop3s)# enable Outside
```

enable gprs

To enable GPRS with RADIUS accounting, use the **enable gprs** command in radius-accounting parameter configuration mode. To disable this command, use the **no** form of this command.

enable gprs
no enable gprs

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Radius-accounting parameter configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command is accessed by using the **inspect radius-accounting** command. The ASA checks for the 3GPP VSA 26-10415 in the Accounting-Request Stop messages to correctly handle secondary PDP contexts. This option is disabled by default. A GTP license is required to enable this feature.

Examples

The following example shows how to enable GPRS with RADIUS accounting:

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# enable gprs
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

enable password

To set the enable password for privileged EXEC mode, use the **enable password** command in global configuration mode.

enable password *password* [**level** *level*] [**pbkdf2** | **encrypted**]

Syntax Description

encrypted	(Optional) For 9.6 and earlier, specifies that the password is in encrypted form for passwords 32 characters and fewer. When you define a password in the **enable password** command, the ASA creates an MD5 hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **enable password** command does not show the actual password; it shows the encrypted password followed by the **encrypted** keword. For example, if you enter the password "test," the **show running-config** command output would appear to be something like the following: `enable password rvEdRh0xPC8bel7s encrypted` The only time you would actually enter the **encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password. In 9.7 and later, passwords of all lengths use PBKDF2.
level *level*	(Optional) Sets a password for a privilege level between 0 and 15.
password	Sets the password as a case-sensitive string of 8 to 127 alphanumeric and special characters. You can use any character in the password with the following exceptions: • No spaces • No question marks • You cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected: • **abc**user1 • user**543** • user**aaaa** • user2**666**

pbkdf2 (Optional) Indicates that the password is encrypted. For 9.6 and earlier, the PBKDF2 (Password-Based Key Derivation Function 2) hash is used only when the password is more than 32 characters in length. In 9.7 and later, all passwords use PBKDF2. When you define a password in the **enable password** command, the ASA creates a PBKDF2 (Password-Based Key Derivation Function 2) hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **enable password** command does not show the actual password; it shows the encrypted password followed by the **pbkdf2** keyword. For example, if you enter a long password, the **show running-config** command output would appear to be something like the following:

```
username pat password rvEdRh0xPC8bel7s pbkdf2
```

The only time you would actually enter the **pbkdf2** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password.

Note that already existing passwords continue to use the MD5-based hash unless you enter a new password.

Command Default

The default password is blank. The default level is 15.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.6(1)	The password length was increased to 127 characters, and the **pbkdf2** keyword was added.
9.7(1)	Passwords of all lengths are now saved to the configuration using the PBKDF2 hash.
9.12(1)	The **no enable password** command is no longer supported.
9.17(1)	The minumum length was changed from 3 to 8 characters. Also you cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected: • **abc**user1 • user**543** • user**aaaa** • user2**666**

Usage Guidelines

The default password for enable level 15 (the default level) is blank, but you are prompted to change it the first time you enter the enable command. You cannot set the password to be blank.

At the CLI, you can access privileged EXEC mode using the **enable** command, the **login** command (with a user at privilege level 2+), or an SSH or Telnet session when you enable **aaa authorization exec auto-enable**. All of these methods require you to set the enable password.

This password change requirement is not enforced for ASDM logins. In ASDM, by default you can log in without a username and with the enable password.

For multiple context mode, you can create an enable password for the system configuration as well as for each context.

To use privilege levels other than the default of 15, configure local command authorization (see the **aaa authorization command** command and specify the **LOCAL** keyword), and set the commands to different privilege levels using the **privilege** command. If you do not configure local command authorization, the enable levels are ignored, and you have access to level 15 regardless of the level you set. See the **show curpriv** command to view your current privilege level.

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode.

Examples

The following example sets the enable password to Pa$$w0rd:

```
ciscoasa(config)# enable password Pa$$w0rd
```

The following example sets the enable password to Pa$$w0rd10 for level 10:

```
ciscoasa(config)# enable password Pa$$w0rd10 level 10
```

The following example sets the enable password to an encrypted password that you copied from another ASA:

```
ciscoasa(config)# enable password jMorNbK0514fadBh pbkdf2
```

Related Commands

Command	Description
aaa authorization command	Configures command authorization.
enable	Enters privileged EXEC mode.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config enable	Shows the enable passwords in encrypted form.

enable webvpn

To enable WebVPN access on a previously configured interface, use the **enable** command. Use this command in webvpn configuration mode.To disable WebVPN on an interface, use the **no** form of the command.

enable*ifname*
no enable

Syntax Description

ifname	Identifies the previously configured interface. Use the **nameif** command to configure interfaces.

Command Default

WebVPN is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to enable WebVPN on the interface named Outside:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# enable Outside
```

encapsulation

To set the Network Virtualization Endpoint (NVE) instance to use VXLAN or Geneve encapsulation, use the **encapsulation** command in nve configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation
{
vxlan
| **geneve** [**port** *port_number* }
no encapsulation vxlan

Syntax Description

Syntax Description

vxlan	Specifies VXLAN encapsulation.
geneve	Specifies Geneve encapsulation. Geneve is only supported by the ASA Virtual.
port *port_number*	For Geneve, sets the port number. The default is 6081.

Command Default

No default value.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nve configuration	• Yes	VXLAN: • Yes	• Yes	VXLAN: • Yes	—

Command History

Release	Modification
9.4(1)	This command was added.
9.17(1)	Added support for **geneve** for the ASA Virtual.

Examples

The following example creates NVE instance 1 and sets the encapsulation to VXLAN:

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# encapsulation vxlan
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

encryption

To specify the encryption algorithm in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the encryption command in ikev2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]
no encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

Syntax Description

des	Specifies 56-bit DES-CBC encryption for ESP.
3des	(Default) Specifies the triple DES encryption algorithm for ESP.
aes	Specifies AES with a 128-bit key encryption for ESP.
aes-192	Specifies AES with a 192-bit key encryption for ESP.
aes-256	Specifies AES with a 256-bit key encryption for ESP.
aes-gcm	Specifies AES-GCM algorithm for IKEv2 encryption.
aes-gcm-192	Specifies AES-GCM algorithm for IKEv2 encryption.
aes-gcm-256	Specifies AES-GCM algorithm for IKEv2 encryption.
null	Choose null integrity algorithm if AES-GCM/GMAC is configured as the encryption algorithm.

Command Default

The default is 3DES.

Usage Guidelines

An IKEv2 SA is a key used in Phase 1 to enable IKEv2 peers to communicate securely in Phase 2. After entering the crypto ikev2 policy command, you can use the **encryption** command to set the SA encryption algorithm.

When OSPFv3 encryption is enabled on an interface, a delay may occur when you establish adjacencies while the IPsec tunnel is configured. Use the **show crypto sockets**, **show ipsec policy**, and **show ipsec sa** commands to determine the underlying IPsec tunnel status and to confirm that processing is occurring.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ikev2-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	The AES-GCM algorithm to use for IKEv2 encryption was added.

Examples

The following example enters ikev2-policy configuration mode and sets the encryption to AES-256:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# encryption aes-256
```

Related Commands

Command	Description
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
integrity	Specifies the ESP integrity algorithm in an IKEv2 SA for AnyConnect IPsec connections.
prf	Specifies the pseudo-random function in an IKEv2 SA for AnyConnect IPsec connections.
lifetime	Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections.

endpoint

To add an endpoint to an HSI group for H.323 protocol inspection, use the **endpoint** command in hsi group configuration mode. To disable this feature, use the **no** form of this command.

endpoint*ip_addressif_name*
no endpoint *ip_address if_name*

Syntax Description

if_name	The interface through which the endpoint is connected to the ASA.
ip_address	The IP address of the endpoint to add. A maximum of ten endpoints per HSI group is allowed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Hsi-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to add endpoints to an HSI group in an H.323 inspection policy map:

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
hsi-group	Creates an HSI group.
hsi	Adds an HSI to the HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

endpoint-mapper

To configure endpoint mapper options for DCERPC inspection, use the **endpoint-mapper** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]
no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

Syntax Description

epm-service-only	Specifies to enforce endpoint mapper service during binding.
lookup-operation	Specifies to enable lookup operation of the endpoint mapper service.
timeout value	Specifies the timeout for pinholes from the lookup operation. The range is from 0:0:1 to 1193:0:0.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure the endpoint mapper in a DCERPC policy map:

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# endpoint-mapper epm-service-only
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **enforcenextupdate** command in ca-crl configuration mode. To permit a lapsed or missing NextUpdate field, use the **no** form of this command.

enforcenextupdate
no enforcenextupdate

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is enforced (on).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If set, this command requires CRLs to have a NextUpdate field that has not yet lapsed. If not used, the ASA allows a missing or lapsed NextUpdate field in a CRL.

Examples

The following example enters crypto ca-crl configuration mode and requires CRLs to have a NextUpdate field that has not expired for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# enforcenextupdate
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
cache-time	Specifies a cache refresh time in minutes.
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.

enrollment protocol scep cmp est acme url

To specify automatic enrollment (for SCEP, CMP, EST, or ACME) to enroll with this trustpoint and to configure the enrollment URL, use the **enrollment protocol scep| cmp |est |acme** *url* command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment protocol scep | **cmp** | **est** | **acme** *url*
no enrollment protocol scep | **cmp** | **est** | **acme** *url*

Syntax Description

protocol	Distinguishes between an ACME CA URL, an SCEP CA URL, a CMP CA URL, and an EST CA URL.

Command Default

The default setting is Off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-server configuration	• Yes	• Yes	• Yes	• Yes • No (for EST)	—

Command History

Release	Modification
9.7(1)	This command was added.
9.16(1)	This command was modified to include **est** as a valid protocol option.
9.22(3), 9.23(1)	This command was modified to include **acme** as a valid protocol option.

Usage Guidelines

In order to be positioned as a Security Gateway device in wireless LTE networks, ASA supports some certificate management functions using the Certificate Management Protocol (CMPv2) in addition to SCEP, Enrollment over Secure Transport (EST) , and Automated Certificate Management Environment (ACME). Using CMPv2 for enrollment of ASA device certificates, you can perform manual enrollment for the primary and secondary certificates from the CMPv2-enabled CA, or manual certificate updates for replacement of a previously issued certificate using the same key pair. The received certificates are stored outside the conventional configuration and are used in certificate-enabled IPsec configurations.

You can use ACME for automatic enrollment of ASA TLS device certificates. The ACME-enabled trustpoints also support manual certificate enrollment. ACME server validates domain ownership using ASA port 80. Hence, ensure that you configure the authentication method as **HTTP-01**. If you use the **Let's Encrypt** CA

option, the enrollment URL is automatically generated. ACME is supported only in nonclustered single-context ASA deployments.

Examples

The following example shows how to use the **crypto ca trustpoint** command to configure the enrollment URL:

```
ciscoasa(config)# crypto ca trustpoint new
ciscoasa(config-ca-trustpoint)# enrollment ?
crypto-ca-trustpoint mode commands/options:
 interface   Configure source interface
 protocol    Enrollment protocol
 retry       Polling parameters
 self        Enrollment will generate a self-signed certificate
 terminal    Enroll via the terminal (cut-and-paste)
asa(config-ca-trustpoint)# enrollment protocol ?

crypto-ca-trustpoint mode commands/options:
  acme  ACME enrollment
  cmp   Certificate Management Protocol Version 2
  est   Enrollment over Secure Transport
  scep  Simple Certificate Enrollment Protocol
asa(config-ca-trustpoint)# enrollment protocol est ?

crypto-ca-trustpoint mode commands/options:
  url CA server enrollment URL
asa(config-ca-trustpoint)# enrollment protocol est url ?

crypto-ca-trustpoint mode commands/options:
  LINE < 477 char  URL
asa(config-ca-trustpoint)# enrollment protocol est url https://xyz.com/est
```

The following example shows how to use the **crypto ca trustpoint** command for the enrollment of ACME CA:

Example:

```
ciscoasa(config)# crypto ca trustpoint my_acme_tp
ciscoasa(config-ca-trustpoint)# enrollment protocol ?
crypto-ca-trustpoint mode commands/options:
  acme  Automatic Certificate Management Environment
  cmp   Certificate Management Protocol Version 2
  est   Enrollment over Secure Transport
  scep  Simple Certificate Enrollment Protocol

ciscoasa(config-ca-trustpoint)# enrollment protocol acme ?
crypto-ca-trustpoint mode commands/options:
  authentication  ACME authentication method
  url             CA server enrollment URL
ciscoasa(config-ca-trustpoint)#  enrollment protocol acme url
https://mytest.com:8443/acme/acme/directory
```

The following example shows how automatic re-enrollment of the ACME certificate can be enabled using the **crypto ca trustpoint** command such that the certificate is automatically renewed when the expiration is approaching:

```
ciscoasa(config)# crypto ca trustpoint my_acme_tp
ciscoasa(config-ca-trustpoint)# auto-enroll 90 regenerate
ciscoasa(config-ca-trustpoint)#
```

enrollment-retrieval

To specify the time in hours that an enrolled user can retrieve a PKCS12 enrollment file, use the **enrollment-retrieval** command in local crypto ca-server configuration mode. To reset the time to the default number of hours (24), use the **no** form of this command.

enrollment-retrieval*timeout*
no enrollment-retrieval

Syntax Description

timeout	Specifies the number of hours users have to retrieve an issued certificate from the local CA enrollment web page. Valid timeout values range from 1 to 720 hours.

Command Default

By default, the PKCS12 enrollment file is stored and retrievable for 24 hours.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

A PKCS12 enrollment file contains an issued certificate and key pair. The file is stored on the local CA server and is available for retrieval from the enrollment web page for the time period specified with the **enrollment-retrieval** command.

When a user is marked as allowed to enroll, that user has the amount of time to enroll with that password specified in the **otp expiration** command. Once the user enrolls successfully, a PKCS12 file is generated, stored, and a copy is returned through the enrollment web page. The user can return for another copy of the file for any reason (such as when a download fails while trying enrollment) for the command time period specified in the **enrollment-retrieval** command.

Note This time is independent from the OTP expiration period.

Examples

The following example specifies that a PKCS12 enrollment file is available for retrieval from the local CA server for 48 hours after the certificate is issued:

```
ciscoasa(config)# crypto ca server
```

```
ciscoasa
(config-ca-server)
# enrollment-retrieval 48
ciscoasa
(config-ca-server)
#
```

The following example resets the retrieval time back to the default of 24 hours:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no enrollment-retrieval
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to ca-server configuration mode commands, which allow you to configure and manage the local CA.
OTP expiration	Specifies the duration in hours that an issued one-time password for the CA enrollment page is valid.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the CA server.
smtp subject	Specifies the text appearing in the subject field of all e-mails generated by the local CA server.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

enrollment retry count

To specify a retry count, use the **enrollment retry count** command in crypto ca-trustpoint configuration mode. To restore the default setting of the retry count, use the **no** form of the command.

enrollment retry count *number*
no enrollment retry count

Syntax Description

number	The maximum number of attempts to send an enrollment request. The valid values are 0, and 1-100 retries.

Command Default

The default setting for the *number* argument is 0 (unlimited).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

After requesting a certificate, the ASA waits to receive a certificate from the CA. If the ASA does not receive a certificate within the configured retry period, it sends another certificate request. The ASA repeats the request until either it receives a response or reaches the end of the configured retry period. This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and configures an enrollment retry count of 20 retries within the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry count 20
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

Command	Description
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

enrollment retry period

To specify a retry period, use the **enrollment retry period** command in crypto ca trustpoint configuration mode. To restore the default setting of the retry period, use the **no** form of the command.

enrollment retry period *minutes*
no enrollment retry period

Syntax Description

minutes	The number of minutes between attempts to send an enrollment request. The valid range is 1- 60 minutes.

Command Default

The default setting is 1 minute.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

After requesting a certificate, the ASA waits to receive a certificate from the CA. If the ASA does not receive a certificate within the specified retry period, it sends another certificate request. This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and configures an enrollment retry period of 10 minutes within the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry period 10
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns all enrollment parameters to their system default values.
enrollment retry count	Defines the number of retries to requesting an enrollment.

enrollment terminal

To specify cut and paste enrollment with this trustpoint (also known as manual enrollment), use the **enrollment terminal** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment terminal
no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and specifies the cut-and-paste method of CA enrollment for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

Command	Description
enrollment url	Specifies automatic enrollment (SCEP) with this trustpoint and configures the URL.

enrollment url (Deprecated)

To specify automatic enrollment (SCEP) to enroll with this trustpoint and to configure the enrollment URL, use the **enrollment url** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment url *url*
no enrollment url url

Syntax Description

url	Specifies the name of the URL for automatic enrollment. The maximum length is 1K characters (effectively unbounded).

Command Default

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and specifies SCEP enrollment at the URL https://enrollsite for trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url https://enrollsite
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

Command	Description
enrollment terminal	Specifies cut-and-paste enrollment with this trustpoint.

eool

To define an action when the End of Options List (EOOL) option occurs in a packet header with IP Options inspection, use the **eool** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

eool action { **allow** | **clear** }
no eool action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the End of Options List IP option.
clear	Remove the End of Options List option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the End of Options List IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

The End of Options List option, which contains just a single zero byte, appears at the end of all options to mark the end of a list of options. This might not coincide with the end of the header according to the header length.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

eou allow (Deprecated)



Note The last supported release for this command was Version 9.1(1).

To enable clientless authentication in a NAC Framework configuration, use the **eou allow** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

eou allow { **audit** | **clientless** | **none** }
no eou allow { **audit** | **clientless** | **none** }

Syntax Description

audit	Performs clientless authentication.
clientless	Performs clientless authentication.
none	Disables clientless authentication.

Command Default

The default configuration contains the **eou allow clientless** configuration.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The **audit** option was added.
9.1(2)	This command was deprecated.

Usage Guidelines

The ASA uses this command only if both of the following are true:

- The group policy is configured to use a NAC Framework NAC policy type.
- A host on the session does not respond to EAPoUDP requests.

Examples

The following example enables the use of an ACS to perform clientless authentication:

```
ciscoasa(config)# eou allow clientless
ciscoasa(config)#
```

The following example shows how to configure the ASA to use an audit server to perform clientless authentication:

```
ciscoasa(config)# eou allow audit
ciscoasa(config)#
```

The following example shows how to disable the use of an audit server:

```
ciscoasa(config)# no eou allow clientless
ciscoasa(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou clientless	Changes the username and password to be sent to the ACS for clientless authentication in a NAC Framework configuration.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou clientless (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the username and password to be sent to the Access Control Server for clientless authentication in a NAC Framework configuration, use the **eou clientless** command in global configuration mode. To use the default value, use the **no** form of this command.

eou clientless username *username* **password** *password*
no eou clientless username *username* **password** *password*

Syntax Description

password	Enter to change the password sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
password	Enter the password configured on the Access Control Server to support clientless hosts. Enter 4-32 ASCII characters.
username	Enter to change the username sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
username	Enter the username configured on the Access Control Server to support clientless hosts. Enter 1-64 ASCII characters, excluding leading and trailing spaces, pound signs (#), question marks (?), quotation marks ("), asterisks (*), and angle brackets (< and >).

Command Default

The default value for both the username and password attributes is clientless.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.

- Clientless authentication is enabled on the ASA.
- NAC is configured on the ASA.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the username for clientless authentication to sherlock:

```
ciscoasa(config)# eou clientless username sherlock
ciscoasa(config)#
```

The following example changes the username for clientless authentication to the default value, clientless:

```
ciscoasa(config)# no eou clientless username
ciscoasa(config)#
```

The following example changes the password for clientless authentication to secret:

```
ciscoasa(config)# eou clientless password secret
ciscoasa(config)#
```

The following example changes the password for clientless authentication to the default value, clientless:

```
ciscoasa(config)# no eou clientless password
ciscoasa(config)#
```

Related Commands

Command	Description
eou allow	Enables clientless authentication in a NAC Framework configuration.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.

eou initialize (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To clear the resources assigned to one or more NAC Framework sessions and initiate a new, unconditional posture validation for each of the sessions, use the **eou initialize** command in privileged EXEC mode.

eou initialize { **all** | **group** *tunnel-group* | **ip** *ip-address* }

Syntax Description

all	Revalidates all NAC Framework sessions on this ASA
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Command Default

No default behavior or values.

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

Use this command if a change occurs in the posture of the remote peers or if the assigned access policies (that is, the downloaded ACLs) change, and you want to clear the resources assigned to the sessions. Entering this command purges the EAPoUDP associations and access policies used for posture validation. The NAC default ACL is effective during the revalidations, so the session initializations can disrupt user traffic. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example initializes all NAC Framework sessions:

```
ciscoasa# eou
initialize all
ciscoasa
```

The following example initializes all NAC Framework sessions assigned to the tunnel group named tg1:

```
ciscoasa# eou
initialize group tg1
ciscoasa
```

The following example initializes the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
ciscoasa# eou
initialize
209.165.200.225
ciscoasa
```

Related Commands

Command	Description
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
debug nac	Enables logging of NAC Framework events.

eou max-retry (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the number of times the ASA resends an EAP over UDP message to the remote computer, use the **eou max-retry** command in global configuration mode. To use the default value, use the **no** form of this command.

eou max-retry *retries*
no eou max-retry

Syntax Description

retries	Limits the number of consecutive retries sent in response to retransmission timer expirations. Enter a value in the range of 1 to 3.

Command Default

The default value is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.
- Clientless authentication is enabled on the ASA.
- NAC is configured on the ASA.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example limits the number of EAP over UDP retransmissions to 1:

```
ciscoasa(config)# eou max-retry 1
ciscoasa(config)#
```

The following example changes the number of EAP over UDP retransmissions to its default value, 3:

```
ciscoasa(config)# no eou max-retry
ciscoasa(config)#
```

Related Commands

eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou port (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the port number for EAP over UDP communication with the Cisco Trust Agent in a NAC Framework configuration, use the eou port command in global configuration mode. To use the default value, use the **no** form of this command.

eou port *port_number*
no eou port

Syntax Description

port_number	Port number on the client endpoint to be designated for EAP over UDP communications. This number is the port number configured on the Cisco Trust Agent. Enter a value in the range of 1024 to 65535.

Command Default

The default value is 21862.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the port number for EAP over UDP communication to 62445:

```
ciscoasa(config)# eou port 62445
ciscoasa(config)#
```

The following example changes the port number for EAP over UDP communication to its default value:

```
ciscoasa(config)# no eou port
ciscoasa(config)#
```

Related Commands

debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
show vpn-session.db	Displays information about VPN sessions, including VLAN mapping and NAC results.
show vpn-session_summary.db	Displays the number IPsec, Cisco Secure Client, and NAC sessions, including VLAN mapping session data.

eou revalidate (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To force immediate posture revalidation of one or more NAC Framework sessions, use the **eou revalidate** command in privileged EXEC mode.

eou revalidate { **all** | **group** *tunnel-group* | **ip** *ip-address* }

Syntax Description

all	Revalidates all NAC Framework sessions on this ASA
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Command Default

No default behavior or values.

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

Use this command if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed. The command initiates a new, unconditional posture validation. The posture validation and assigned access policy that were in effect before you entered the command remain in effect until the new posture validation succeeds or fails. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example revalidates all NAC Framework sessions:

```
ciscoasa# eou
```

```
revalidate all
ciscoasa
```

The following example revalidates all NAC Framework sessions assigned to the tunnel group named tg-1:

```
ciscoasa# eou
revalidate group tg-1
ciscoasa
```

The following example revalidates the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
ciscoasa# eou
revalidate ip
209.165.200.225
ciscoasa
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.

eou timeout (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration, use the eou timeout command in global configuration mode. To use the default value, use the **no** form of this command.

eou timeout { **hold-period** | **retransmit** } *seconds*
no eou timeout { **hold-period** | **retransmit** }

Syntax Description

hold-period	Maximum time to wait after sending EAPoUDP messages equal to the number of EAPoUDP retries. The **eou initialize** or **eou revalidate** command also clears this timer. If this timer expires, the ASA initiates a new EAP over UDP association with the remote host.
retransmit	Maximum time to wait after sending an EAPoUDP message. A response from the remote host clears this timer. The **eou initialize** or **eou revalidate** command also clears this timer. If the timer expires, the ASA retransmits the EAPoUDP message to the remote host.
seconds	Number of seconds for the ASA to wait. Enter a value in the range of 60 to 86400 for the hold-period attribute, or the range of 1 to 60 for the retransmit attribute.

Command Default

The default value of the **hold-period** option is 180.

The default value of the **retransmit** option is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the wait period before initiating a new EAP over UDP association to 120 seconds:

```
ciscoasa(config)# eou timeout hold-period 120
ciscoasa(config)#
```

The following example changes the wait period before initiating a new EAP over UDP association to its default value:

```
ciscoasa(config)# no eou timeout hold-period
ciscoasa(config)#
```

The following example changes the retransmission timer to 6 seconds:

```
ciscoasa(config)# eou timeout retransmit 6
ciscoasa(config)#
```

The following example changes the retransmission timer to its default value:

```
ciscoasa(config)# no eou timeout retransmit
ciscoasa(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou max-retry	Changes the number of times the ASA resends an EAP over UDP message to the remote computer.

erase

To erase and reformat the file system, use the **erase** command in privileged EXEC mode. This command overwrites all files and erases the file system, including hidden system files, then reinstalls the file system.

erase [**disk0:** | **disk1:** | **flash:**]

Syntax Description

disk0: (Optional) Specifies the internal compact Flash memory card, followed by a colon.

disk1: (Optional) Specifies the external compact Flash memory card, followed by a colon.

flash: (Optional) Specifies the internal Flash memory, followed by a colon.

Caution
Erasing the flash memory also removes the licensing information, which is stored in flash memory. Save the licensing information before erasing the flash memory.

On the ASA 5500 series, the **flash** keyword is aliased to **disk0:**.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **erase** command erases all data in the flash memory using the 0xFF pattern and then rewrites an empty file system allocation table to the device.

To delete all visible files (excluding hidden system files), enter the **delete /recursive** command, instead of the **erase** command.

Note On the ASA 5500 series, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information.

Examples

The following example erases and reformats the file system:

```
ciscoasa# erase flash:
```

Related Commands

Command	Description
delete	Removes all visible files, excluding hidden system files.
format	Erases all files (including hidden system files) and formats the file system.

esp

To specify parameters for ESP and AH tunnels for IPsec Pass-Through inspection, use the **esp** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

{ **esp** | **ah** } [**per-client-max** *num*] [**timeout** *time*]
no { **esp** | **ah** } [**per-client-max** *num*] [**timeout** *time*]

Syntax Description

esp	Specifies parameters for the ESP tunnel.
ah	Specifies parameters for the AH tunnel.
per-client-max num	Specifies the maximum number of tunnels from one client.
timeout time	Specifies the idle timeout for the ESP tunnel.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to permit UDP 500 traffic:

```
ciscoasa(config)# access-list test-udp-acl extended permit udp any any eq 500
ciscoasa(config)# class-map test-udp-class
ciscoasa(config-pmap-c)# match access-list test-udp-acl
ciscoasa(config)# policy-map type inspect ipsec-pass-thru ipsec-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
ciscoasa(config-pmap-p)# ah per-client-max 16 timeout 00:05:00
ciscoasa(config)# policy-map test-udp-policy
ciscoasa(config-pmap)# class test-udp-class
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

established

To permit return connections on ports that are based on an established connection, use the **established** command in global configuration mode. To disable the established feature, use the **no** form of this command.

established est_protocol *dest_port* [**source_port**] [**permitto protocol port** [**-port**]] [**permitfrom protocol** *port* [**-port**]]
no established est_protocol *dest_port* [**source_port**] [**permitto protocol port** [**-port**]] [**permitfrom protocol** *port* [**-port**]]

Syntax Description

est_protocol	Specifies the IP protocol (UDP or TCP) to use for the established connection lookup.
dest_port	Specifies the destination port to use for the established connection lookup.
permitfrom	(Optional) Allows the return protocol connection(s) originating from the specified port.
permitto	(Optional) Allows the return protocol connections destined to the specified port.
port [-port]	(Optional) Specifies the (UDP or TCP) destination port(s) of the return connection.
protocol	(Optional) IP protocol (UDP or TCP) used by the return connection.
source_port	(Optional) Specifies the source port to use for the established connection lookup.

Command Default

The defaults are as follows:

- *dest_port*—0 (wildcard)
- *source_port*—0 (wildcard)

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The keywords **to** and **from** were removed from the CLI. Use the keywords **permitto** and **permitfrom** instead.

Usage Guidelines

The established command lets you permit return access for outbound connections through the ASA. This command works with an original connection that is outbound from a network and protected by the ASA and a return connection that is inbound between the same two devices on an external host. The established command

lets you specify the destination port that is used for connection lookups. This addition allows more control over the command and provides support for protocols where the destination port is known, but the source port is unknown. The permitto and permitfrom keywords define the return inbound connection.

Caution We recommend that you always specify the established command with the permitto and permitfrom keywords. Using the established command without these keywords is a security risk because when connections are made to external systems, those system can make unrestricted connections to the internal host involved in the connection. This situation can be exploited for an attack of your internal systems.

Examples

The following set of examples shows potential security violations could occur if you do not use the established command correctly.

This example shows that if an internal system makes a TCP connection to an external host on port 4000, then the external host could come back in on any port using any protocol:

```
ciscoasa(config)# established tcp 4000 0
```

You can specify the source and destination ports as **0** if the protocol does not specify which ports are used. Use wildcard ports (0) only when necessary.

```
ciscoasa(config)# established tcp 0 0
```

Note To allow the established command to work correctly, the client must listen on the port that is specified with the permitto keyword.

You can use the established command with the nat 0 command (where there are no global commands).

Note You cannot use the established command with PAT.

The ASA supports XDMCP with assistance from the **established** command.

Caution Using XWindows system applications through the ASA may cause security risks.

XDMCP is on by default, but it does not complete the session unless you enter the established command as follows:

```
ciscoasa(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

Entering the **established** command enables the internal XDMCP-equipped (UNIX or ReflectionX) hosts to access external XDMCP-equipped XWindows servers. UDP/177-based XDMCP negotiates a TCP-based XWindows session, and subsequent TCP back connections are permitted. Because the source port(s) of the return traffic is unknown, specify the *source_port* field as 0 (wildcard). The

dest_port should be 6000 + *n*, where *n* represents the local display number. Use this UNIX command to change this value:

```
ciscoasa(config)# setenv DISPLAY
 hostname:displaynumber.screennumber
```

The **established** command is needed because many TCP connections are generated (based on user interaction) and the source port for these connections is unknown. Only the destination port is static. The ASA performs XDMCP fixups transparently. No configuration is required, but you must enter the **established** command to accommodate the TCP session.

The following example shows a connection between two hosts using protocol A destined for port B from source port C. To permit return connections through the ASA and protocol D (protocol D can be different from protocol A), the source port(s) must correspond to port F and the destination port(s) must correspond to port E.

```
ciscoasa(config)# established A B C permitto D E permitfrom D F
```

The following example shows how a connection is started by an internal host to an external host using TCP destination port 6060 and any source port. The ASA permits return traffic between the hosts through TCP destination port 6061 and any TCP source port.

```
ciscoasa(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

The following example shows how a connection is started by an internal host to an external host using UDP destination port 6060 and any source port. The ASA permits return traffic between the hosts through TCP destination port 6061 and TCP source port 1024-65535.

```
ciscoasa(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

The following example shows how a local host starts a TCP connection on port 9999 to a foreign host. The example allows packets from the foreign host on port 4242 back to local host on port 5454.

```
ciscoasa(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

Related Commands

Command	Description
clear configure established	Removes all established commands.
show running-config established	Displays the allowed inbound connections that are based on established connections.

event crashinfo

To trigger an event manager applet when a crash occurs on the ASA, use the **event crashinfo** command in event manager applet configuration mode. To remove the crash event, use the **no** form of this command.

event crashinfo
no event crashinfo

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Regardless of the value of the **output** command, the **action** commands are directed to the crash information file. The output is generated before the **show tech** command.

Note The state of the ASA is generally unknown when it crashes. Some CLI commands may not be safe to run during this condition.

Examples

The following example triggers an applet when the ASA crashes:

```
ciscoasa(config-applet)# event crashinfo
```

Related Commands

Command	Description
event none	Invokes an event manager applet manually.
event syslog id	Adds a syslog event to an event manager applet.
event timer absolute time	Configures an absolute event timer.

Command	Description
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

event manager applet

To create or edit an event manager applet that links events with actions and output, use the event manager applet command in global configuration mode. To remove an event manager applet, use the **no** form of this command.

event manager applet *name*
no event manager applet *name*

Syntax Description

name Specifies the name of the event manager applet. The name can be up to 32 characters long.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use the **event manager applet** command to enter event manager applet configuration mode.

Examples

The following example creates an event manager applet and enters event manager applet configuration mode:

```
ciscoasa(config)# event manager applet appletexample1
ciscoasa(config-applet)#
```

Related Commands

Command	Description
description	Describes an applet.
event manager run	Runs an event manager applet.
show event manager	Shows statistical information for each configured event manager applet.
debug event manager	Manages debugging traces for the event manager.

event memory-logging-wrap

To configure a memory logging wrap event trigger, use the **event memory-logging-wrap** command in event manager applet configuration mode.

event memory-logging-wrap

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuratio	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

When wrap is enabled for memory logging, the memory logger sends an event to the event manager to trigger configured applets.

Examples

The following example shows an applet that records all memory allocations:

```
ciscoasa(config-applet)# event manager applet memlog
ciscoasa(config-applet)# event memory-logging-wrap
ciscoasa(config-applet)# action 0 cli command "show memory logging wrap"
ciscoasa(config-applet)# output file append disk0:/memlog.log
```

Related Commands

Command	Description
memory logging	Enables memory logging.
show memory logging	Shows the results of memory logging.

event none

To invoke an event manager applet manually, use the **event none** command in event manager applet configuration mode. To remove a manual invocation, use the **no** form of this command.

event none
no event none

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

You can configure any other event with the **event none** command.

Examples

The following example invokes an event manager applet manually:

```
ciscoasa(config-applet)# event none
```

Related Commands

Command	Description
event crashinfo	Triggers an event manager applet when a crash occurs on the ASA.
event syslog id	Adds a syslog event tor an event manager applet.
event timer absolute time	Configures an absolute event timer.
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

event syslog id

To add a syslog event to an event manager applet, use the **event syslog id** command in event manager applet configuration mode. To remove a syslog event from an event manager applet, use the **no** form of this command.

event syslog id *nnnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]
no event syslog id *nnnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

Syntax Description

nnnnnn	Identifies the syslog message ID.
occurs *n*	Indicates the number of times that the syslog message must occur for the applet to be invoked. The default is 1. Valid values are from 1 - 4294967295.
period *seconds*	Indicates the number of seconds in which the event must occur, and limits how frequently the applet is invoked to at most once in the configured period. Valid values are from 0 - 604800. A value of 0 means that no period is defined.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use the **event syslog id** command to identify a single syslog message or a range of syslog messages that trigger an applet.

Examples

The following example indicates that syslog message 106201 triggers an applet:

```
ciscoasa(config-applet)# event syslog id 106201
```

Related Commands

Command	Description
event crashinfo	Triggers an event manager applet when a crash occurs on the ASA.
event none	Invokes an event manager applet manually.

Command	Description
event timer absolute time	Configures an absolute event timer.
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

event timer

To configure timer events, use the **event timer** command in event manager applet configuration mode. To remove timer events, use the **no** form of this command.

event timer { **watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss* }
no event timer { **watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss* }

Syntax Description

absolute time	Specifies that an event occurs once a day at a specified time and restarts automatically.
countdown time	Specifies that an event occurs once and does not restart unless it is removed, then re-added.
hh:mm:ss	Specifies the time-of-day format. The time range is from 00:00:00 (midnight) to 23:59:59.
seconds	Specifies the number of seconds. Valid values range from 0 - 604800. A value of 0 disables the timer.
watchdog time	Specifies that an event occurs once per configured period and restarts automatically.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use the **event timer absolute time** command to cause an event to occur once a day at a specified time and restart automatically.

Use the **event timer countdown time** command to cause an event to occur once and not restart unless it is removed, then re-added.

Use the **event timer watchdog time** command to cause an event to occur once per configured period and restart automatically.

Examples

The following example causes an event to occur once a day at the specified time shown:

```
ciscoasa(config-applet)# event timer absolute time 10:30:20
```

The following example causes an event to occur once a day at the specified time shown:

```
ciscoasa(config-applet)# event timer countdown time 10:30:20
```

The following example causes an event to occur once a day and restart automatically:

```
ciscoasa(config-applet)# event timer watchdog time 30
```

Related Commands

Command	Description
event crashinfo	Triggers an event manager applet when a crash occurs on the ASA.
event none	Invokes an event manager applet manually.
event syslog id	Adds a syslog event to an event manager applet.
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

exceed-mss

To allow or drop packets whose data length exceeds the TCP maximum segment size (MSS) set by the peer during a three-way handshake, use the **exceed-mss** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

exceed-mss { **allow** | **drop** }
no exceed-mss { **allow** | **drop** }

Syntax Description

allow	Allows packets that exceed the MSS. This setting is the default.
drop	Drops packets that exceed the MSS.

Command Default

Packets are allowed by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)/8.0(4)	The default was changed from **drop** to **allow**.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **exceed-mss** command in tcp-map configuration mode to drop TCP packets whose data length exceed the TCP maximum segment size set by the peer during a three-way handshake.

Examples

The following example drops flows on port 21 if they are in excess of MSS:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# exceed-mss drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
```

```
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection advanced-options	Configures advanced connection features, including TCP normalization.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

exempt-list

To add an entry to the list of remote computer types that are exempt from posture validation, use the **exempt-list** command in nac-policy-nac-framework configuration mode. To remove an entry from the exemption list, use the **no** form of this command and name the operating system and ACL in the entry to be removed.

exempt-list os " *os-name* **"** [**disable** | **filter** *acl-name* [**disable**]]
no exempt-list os " *os-name* **"** [**disable** | **filter** *acl-name* [**disable**]]

Syntax Description

acl-name	Name of the ACL present in the ASA configuration. When specified, it must follow the **filter** keyword.
disable	Performs one of two functions, as follows: • If you enter it after the "os-name," the ASA ignores the exemption, and applies NAC posture validation to the remote hosts that are running that operating system. • If you enter it after the *acl-name* , ASA exempts the operating system, but does not assign the ACL to the associated traffic.
filter	Applies an ACL to filter the traffic if the computer's operating system matches the *os name* . The filter/*acl-name* pair is optional.
os	Exempts an operating system from posture validation.
os name	Operating system name. Quotation marks are required only if the name includes a space (for example, "Windows XP").

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nac-policy-nac-framework configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The command name was changed from **vpn-nac-exempt** to **exempt-list**. The command was moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.

Usage Guidelines

When the command specifies an operating system, it does not overwrite the previously added entry to the exception list; enter the command once for each operating system and ACL that you want to exempt.

The **no exempt-list** command removes all exemptions from the NAC Framework policy. Specifying an entry when issuing the **no** form of the command removes the entry from the exemption list.

To remove all entries from the exemption list associated with this NAC policy, use the **no** form of this command without specifying additional keywords.

Examples

The following example adds all hosts running Windows XP to the list of computers that are exempt from posture validation:

```
ciscoasa(config-group-policy)# exempt-list os "Windows XP"
ciscoasa(config-group-policy)
```

The following example exempts all hosts running Windows XP and applies the ACL acl-1 to traffic from those hosts:

```
ciscoasa(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

The following example removes the same entry from the exemption list:

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

The following example removes all entries from the exemption list:

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list
ciscoasa(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
debug nac	Enables logging of NAC Framework events.
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
nac-settings	Assigns a NAC policy to a group policy.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
show vpn-session_summary.db	Displays the number of IPsec, Cisco Secure Client, and NAC sessions.

exit

To exit the current configuration mode, or to logout from privileged or user EXEC modes, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can also use the key sequence **Ctrl+Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **exit** command in privileged or user EXEC modes, you log out from the ASA. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Examples

The following example shows how to use the **exit** command to exit global configuration mode, then log out from the session:

```
ciscoasa(config)# exit
ciscoasa# exit
Logoff
```

The following example shows how to use the **exit** command to exit global configuration mode, then use the **disable** command to exit privileged EXEC mode:

```
ciscoasa(config)# exit
ciscoasa# disable
ciscoasa#
```

Related Commands

Command	Description
quit	Exits a configuration mode or logs out of the privileged or user EXEC modes.

exp-flow-control

To define an action when the Experimental Flow Control (FINN) option occurs in a packet header with IP Options inspection, use the **exp-flow-control** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

exp-flow-control action { **allow** | **clear** }
no exp-flow-control action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Experimental Flow Control IP option.
clear	Remove the Experimental Flow Control option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Experimental Flow Control IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-flow-control action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

expire-entry-timer

To set the expiration timer for fully-qualified domain names (FQDN) specified in network objects, use the **expire-entry-timer** command in dns server-group configuration mode. To remove the timer, use the **no** form of this command.

expire-entry-timer minutes *minutes*
no expire-entry-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer time in minutes. Valid values range from 1 to 65535 minutes.

Command Default

By default, the DNS expire-entry-timer value is 1 minute.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
dns server-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.
9.17(1)	The behavior of the command was changed to set a minimum TTL, rather than extend the TTL, of DNS resolutions.

Usage Guidelines

This command is supported for the DefaultDNS server group, or the active server group, only. It sets the expiration timer for fully-qualified domain names (FQDN) specified in network objects. It applies only to these FQDN, and does not apply to any FQDN resolved for other purposes.

Up to version 9.16, the command specifies the time to remove the IP address of a resolved FQDN after its TTL expires. When the IP address is removed, the ASA recompiles the tmatch lookup table. The default DNS expire-entry-timer value is 1 minute, which means that IP addresses are removed 1 minute after the TTL (time to live) of the DNS entry expires.

Starting with 9.17, the command specifies a minimum TTL for the DNS entry. If the expiration timer is longer than the entry's TTL, the TTL is increased to the expire entry time value. If the TTL is longer than the expiration timer, the expire entry time value is ignored: no additional time is added to the TTL in this case.

Note The default setting might result in frequent recompilation of the tmatch lookup table when the resolved TTL of common FQDN hosts, such as www.example.com, is a short time period. You can specify a long DNS expire-entry timer value to reduce the frequency of recompilation of the tmatch lookup table while maintaining security.

Examples

The following example removes resolved entries after 240 minutes:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# expire-entry-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

expiry-time

To configure an expiration time for caching objects without revalidating them, use the **expiry-time** command in cache configuration mode. To remove the expiration time from the configuration and reset it to the default value, use the **no** form of this command.

expiry-time*time*
no expiry-time

Syntax Description

time	The amount of time in minutes that the ASA caches objects without revalidating them.

Command Default

The default is 1 minute.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cache configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The expiration time is the amount of time in minutes that the ASA caches an object without revalidating it. Revalidation consists of rechecking the content.

Examples

The following example shows how to set an expiration time with a value of 13 minutes:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)#expiry-time 13
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters webvpn cache configuration mode.
cache-compressed	Configures WebVPN cache compression.

Command	Description
disable	Disables caching.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum size of an object to cache.

exp-measure

To define an action when the Experimental Measurement (ZSU) option occurs in a packet header with IP Options inspection, use the **exp-measure** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

exp-measure action { **allow** | **clear** }
no exp-measure action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Experimental Measurement IP option.
clear	Remove the Experimental Measurement option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Experimental Measurement IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-measure action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

export

To specify the certificate to be exported to the client, use the export command in ctl-provider configuration mode. To remove the configuration, use the **no** form of this command.

export certificate *trustpoint_name*
no export certificate [*trustpoint_name*]

Syntax Description

certificate *trustpoint_name*	Specifies the certificate to be exported to the client.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl-provider configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the export command in ctl-provider configuration mode to specify the certificate to be exported to the client. The trustpoint name is defined by the crypto ca trustpoint command. The certificate will be added to the CTL file composed by the CTL client.

Examples

The following example shows how to create a CTL provider instance:

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in ctl-provider configuration mode.

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and the username and password for client authentication.
service	Specifies the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

export webvpn AnyConnect-customization

To export a customization object *that customizes the AnyConnect client GUI*, use the **export webvpn AnyConnect-customization** command in privileged EXEC mode:

export webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
type	The type of customization: • binary—An executable that replaces the Secure Client GUI. • transform—A transform that customizes the MSI.
url	Remote path and filename to export the XML customization object, in the form *URL/filename* (the maximum number is 255 characters).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An Secure Client customization object is an XML file that resides in cache memory, and customizes the GUI screens for Secure Client users. When you export a customization object, an XML file containing XML tags is created at the URL you specify.

The XML file created by the customization object named *Template* contains empty XML tags, and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory, but can be exported, edited, and imported back into the ASA as a new customization object.

The content of *Template* is the same as the initial DfltCustomization object state.

For a complete list of resource files used the Secure Client GUI and their filenames, see the AnyConnect VPN Client Administrator Guide.

Examples

The following example exports the Cisco logo used on the Secure Client GUI:

```
ciscoasa# export webvpn AnyConnect-customization type resource company_logo.bmp
tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn customization

To export a customization object *that customizes screens visible to Clientless SSL VPN users*, use the **export webvpn customization** command in privileged EXEC mode.

export webvpn customization *name url*

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
url	Remote path and filename to export the XML customization object, in the form *URL/filename* (the maximum number is 255 characters).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A customization object is an XML file that resides in cache memory, and customizes the screens visible to Clientless SSL VPN users, including login and logout screens, the portal page, and available languages. When you export a customization object, an XML file containing XML tags is created at the URL that you specify.

The XML file created by the customization object named *Template* contains empty XML tags, and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory, but can be exported, edited, and imported back into the ASA as a new customization object.

The content of *Template* is the same as the initial DfltCustomization object state.

You can export a customization object using the **export webvpn customization** command, make changes to the XML tags, and import the file as a new object using the **import webvpn customization** command.

Examples

The following example exports the default customization object (DfltCustomization) and creates the resulting XML file named dflt_custom:

```
ciscoasa# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
```

```
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn plug-in

To export a plug-in from the flash device of the ASA, enter the **export webvpn plug-in** command in privileged EXEC mode.

import webvpn plug-in protocol *protocol URL*

Syntax Description

protocol

- **citrix**

The Citrix plugin lets the remote user connect to a computer running Citrix Metaframe services.

- **rdp**

The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes. The web site containing the original is http://properjavardp.sourceforge.net/ .

- **ssh,telnet**

The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer. Cisco redistributes this plug-in without any changes. The web site containing the original is http://javassh.org/ .

Caution
The **export webvpn plug-in protocol ssh,telnet** *URL* command exports *both* the SSH and Telnet plug-ins. Do *not* enter this command once for SSH and once for Telnet. When typing the **ssh,telnet** string, do *not* insert a space.

- **vnc**

The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes. The web site containing the original is http://www.tightvnc.com/ .

URL — Path to the remote device.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Exporting a plug-in does not remove it from flash. Exporting creates a copy of the plug-in at the specified URL.

Examples

The following command adds WebVPN support for Citrix:

```
ciscoasa# import webvpn plug-in protocol citrix tftp://209.165.201.22/plugins/ica-plugin.zip
Accessing
tftp://209.165.201.22/plugins/ica-plugin.zip...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/citrix...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
554543 bytes copied in 13.270 secs (42657 bytes/sec)
```

The following command exports the RDP plugin:

```
ciscoasa# export webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
```

Related Commands

Command	Description
import webvpn plugin	Imports a specified plug-in from a local device to the ASA flash.
revert webvpn plug-in protocol	Removes the specified plug-in from the flash device of the ASA.
show import webvpn plug-in	Lists the plug-ins present on the flash device of the ASA.

export webvpn mst-translation

To export a Microsoft transform (MST) *that translates the AnyConnect installer program,* use the **export webvpn mst-translation** command in privileged EXEC mode:

export webvpn mst-translation *component* **language** *language* **URL**

Syntax Description

component	The component to which this MST applies. The only valid choice is Secure Client.
language	The language code of the MST exported. Use the code in the same format that the browser requires.
URL	The remote path and filename to export the transform to, in the form *URL/filename* (the maximum number is 255 characters).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

As with the Secure Client GUI, you can translate messages displayed by the client installer program. The ASA uses transforms to translate the messages displayed by the installer. The transform alters the installation, but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.

Each language has its own transform. You can edit a transform with a transform editor such as Orca, and make changes to the message strings. Then you import the transform to the ASA. When the user downloads the client, the client detects the preferred language of the computer (the locale specified during installation of the operating system) and applies the appropriate transform.

We currently offer transforms for 30 languages. These transforms are available in the following .zip file on the Secure Client software download page at cisco.com:

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

In this file, <VERSION> is the version of Secure Client release (for exmaple, 2.2.103).

Examples

The following example exports the English language transform as AnyConnect_Installer_English:

```
ciscoasa# export webvpn mst-translation AnyConnect language es tftp://209.165.200.225/
AnyConnect_Installer_English
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn translation-table

To export a translation table used to translate terms displayed to remote users establishing SSL VPN connections, use the **export webvpn translation-table** command in privileged EXEC mode.

export webvpn webvpn *translation_domain* { **language** *language* | **template** } *url*

Syntax Description

language	Specifies the name of a previously imported translation table. Enter the value in the manner expressed by your browser language options.
translation_domain	The functional area and associated messages. Table 14-1 lists available translation domains.
url	Specifies the URL of the object.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The ASA provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

Each functional area and its messages that are visible to remote users has its own translation domain, which are specified by the *translation_domain argument*. Table 14-1 shows the translation domains and the functional areas translated.

Table 8: Translation Domains and Functional Areas Affected

Translation Domain	Functional Areas Translated
AnyConnect	*Messages displayed on the user interface of the Cisco AnyConnect VPN Client.*
banners	Banners displayed to remote users and messages when VPN access is denied.

Translation Domain	Functional Areas Translated
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	*Messages on the login and logout pages, portal page, and all the messages customizable by the user.*
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA, and portal messages that are not customizable.

Usage Guidelines

A translation template is an XML file in the same format as the translation table, but has all the translations empty. The software image package for the ASA includes a template for each domain that is part of the standard functionality. Templates for plug-ins are included with the plug-ins and define their own translation domains. Because you can customize the *login and logout pages, portal page, and URL bookmarks for clientless users,* the ASA **generates the** customization and url-list translation domain templates dynamically, and the template automatically reflects your changes to these functional areas.

Exporting a previously-imported translation table creates an XML file of the table at the URL location. You can view a list of available templates and previously-imported tables using the **show import webvpn translation-table** command.

Download a template or translation table using the **export webvpn translation-table** command, make changes to the messages, and import the translation table using the **import webvpn translation-table** command.

Examples

The following example exports a template for the translation domain *customization* , which is used to translate the *login and logout pages, portal page, and all the messages customizable and visible to remote users establishing clientless SSL VPN connections. The* ASA *creates the XML file with the name >Sales:*

```
ciscoasa# export webvpn translation-table customization template tftp://209.165.200.225/Sales
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The following example exports a previously imported translation table for the Chinese language named *>zh* , an abbreviation compatible with the abbreviation specified for Chinese in the Internet Options of the Microsoft Internet Explorer browser. The ASA *creates the XML file with the name >Chinese* :

```
ciscoasa# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Related Commands

Command	Description
import webvpn translation-table	Imports a translation table.
revert	Removes translation tables from cache memory.
show import webvpn translation-table	Displays information about imported translation tables.

export webvpn url-list

To export a URL list to a remote location, use the **export webvpn url-list** command in privileged EXEC mode.

export webvpn url-list *name url*

Syntax Description

name	The name that identifies the URL list. The maximum number is 64 characters.
url	The remote path to the source of the URL list. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

No URL lists are present in WebVPN by default.

An object, Template, is available for downloading with the **export webvpn url-list** command. The Template object cannot be changed or deleted. The contents of the Template object can be edited and saved as a custom URL list, and imported with the **import webvpn url-list** command to add a custom URL list.

Exporting a previously imported URL list creates an XML file of the list at the URL location. You can view a list of available templates and previously imported tables using the **show import webvpn url-list** command.

Examples

The following example exports a URL list, *servers:*

```
ciscoasa# export webvpn url-list servers2 tftp://209.165.200.225
ciscoasa#
```

Related Commands

Command	Description
import webvpn url-list	Imports a URL list.

Command	Description
revert webvpn url-list	Removes URL lists from cache memory.
show import webvpn url-list	Displays information about imported URL lists.

export webvpn webcontent

To export previously imported content in flash memory that is visible to remote Clientless SSL VPN users, use the **export webvpn webcontent** command in privileged EXEC mode.

export webvpn webcontent *source url destination url*

Syntax Description

destination url	**The URL to export to**. The maximum number is 255 characters.
source url	The URL in the ASA flash memory in which the content resides. The maximum number is 64 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Content exported with the **webcontent** option is content visible to remote clientless users. This includes previously imported help content visible on the clientless portal and logos used by customization objects.

You can see a list of content available for export by entering a question mark (**?**) after the **export webvpn webcontent** command. For example:

```
ciscoasa# export webvpn webcontent ?
Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

Examples

The following example exports the file *logo.gif* , using TFTP, to 209.165.200.225, as the filename *logo_copy.gif* :

```
ciscoasa# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

Related Commands

Command	Description
import webvpn webcontent	Imports content visible to Clientless SSL VPN users.
revert webvpn webcontent	Removes content from flash memory.
show import webvpn webcontent	Displays information about imported content.

extended-security

To define an action when the Extended Security (E-SEC) option occurs in a packet header with IP Options inspection, use the **extended-security** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

extended-security action { **allow** | **clear** }
no extended-security action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Extended Security IP option.
clear	Remove the Extended Security option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Extended Security IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# extended-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

external-browser

To configure Secure Client single sign-on authentication using an external browser (default operating system browser) instead of a browser embedded in Secure Client, use the **external-browser** command in the config-tunnel-webvpn mode. Use the **no** form of the command to disable external browser for single sign-on authentication.

external-browser enable

no external-browser enable

Syntax Description

enable	Configures the default OS browser for single sing-on authentication.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
config-tunnel-webvpn	• Yes	• Yes	• Yes	• No	• No

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

The **external-browser** command allows you to configure the default operating system browser for SAML single sign-on authentication.

The following example shows how to use the**external-browser enable** command to use the default operating system browser for SAML single sign-on authentication.

```
ciscoasa
#
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
anyconnect external-browser-pkg	Configures the Secure Client external browser package file path.
tunnel-group	Creates a VPN connection profile or accesses the database of VPN connection profiles.

Command	Description
show webvpnanyconnect external-browser-pkg	Displays information about the specified single sing-on package file.

external-port

To specify the VXLAN external port for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **external-port** command in interface configuration mode. To remove the port, use the **no** form of this command.

external-port *port*
no external-port *port*

Syntax Description

port	Sets the port between 1024 and 65535.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-segment-id	Specifies the VXLAN external segment ID for a VNI interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-port	Sets the internal VXLAN port.
internal-segment-id	Specifies the VXLAN internal segment ID for a VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
proxy paired	Sets the interface to paired proxy mode.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

external-segment-id

To specify the VXLAN external segment ID for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **external-segment-id** command in interface configuration mode. To remove the ID, use the **no** form of this command.

external-segment-id *id*
no external-segment-id *id*

Syntax Description

id	Sets the ID between 1 and 16777215.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-port	Sets the external VXLAN port.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-port	Sets the internal VXLAN port.
internal-segment-id	Specifies the VXLAN internal segment ID for a VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
proxy paired	Sets the interface to paired proxy mode.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.



fa – fd

- failover, on page 1521
- failover active, on page 1523
- failover cloud authentication, on page 1524
- failover cloud peer, on page 1526
- failover cloud polltime, on page 1528
- failover cloud port, on page 1530
- failover cloud route-table, on page 1532
- failover cloud route-table rg, on page 1534
- failover cloud route-table route, on page 1536
- failover cloud subscription-id, on page 1538
- failover cloud unit, on page 1540
- failover exec, on page 1542
- failover group, on page 1548
- failover health-check bfd, on page 1550
- failover interface ip, on page 1552
- failover interface-policy, on page 1554
- failover ipsec pre-shared-key, on page 1556
- failover key, on page 1558
- failover lan interface, on page 1560
- failover lan unit, on page 1563
- failover link, on page 1565
- failover mac address, on page 1567
- failover polltime, on page 1569
- failover polltime interface, on page 1571
- failover poll-time link-state, on page 1573
- failover reload-standby, on page 1574
- failover replication http, on page 1575
- failover replication rate, on page 1576
- failover reset, on page 1577
- failover standby config-lock, on page 1578
- failover timeout, on page 1579
- failover trace, on page 1581
- failover wait-disable, on page 1582

- fallback (Deprecated), on page 1583
- fast-flood, on page 1585
- fault-monitor block-depletion, on page 1589
- fault-monitor mbuf-depletion, on page 1591

failover

To enable failover, use the **failover** command in global configuration mode. To disable failover, use the **no** form of this command.

failover
no failover

Syntax Description

This command has no arguments or keywords.

Command Default

Failover is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was limited to enable or disable failover in the configuration (see the **failover active** command).

Usage Guidelines

Use the **no** form of this command to disable failover.

In HA, when **no failover** is triggered during a healthy active/standby state, none of the interfaces on the standby unit are shut down. However, if this occurs while HA is in an active/failed state, all interfaces—including the management interface—are shut down on the failed unit, except for the failover LAN and state interfaces. This is done to prevent potential traffic issues if the failed interfaces become active after failover has been disabled. The failover LAN and state interfaces remain up to ensure ongoing failover communication.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

The ASA 5505 device allows only Stateless Failover, and only while not acting as an Easy VPN hardware client.

Examples

The following example disables failover:

```
ciscoasa(config)# no failover
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover active

To switch a standby ASA or failover group to the active state, use the **failover active** command in privileged EXEC mode. To switch an active ASA or failover group to standby, use the **no** form of this command.

failover active [**group** *group_id*]
no failover active [**group** *group_id*]

Syntax Description

group *group_id*	(Optional) Specifies the failover group to make active.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was modified to include failover groups.

Usage Guidelines

Use the **failover active** command to initiate a failover switch from the standby unit, or use the no **failover active** command from the active unit to initiate a failover switch. You can use this feature to return a failed unit to service, or to force an active unit offline for maintenance. If you are not using Stateful Failover, all active connections are dropped and must be reestablished by the clients after the failover occurs.

Switching for a failover group is available only for Active/Active failover. If you enter the **failover active** command on an Active/Active failover unit without specifying a failover group, all groups on the unit become active.

Examples

The following example switches the standby group 1 to active:

```
ciscoasa# failover active group 1
```

Related Commands

Command	Description
failover reset	Moves an ASA from a failed state to standby.

failover cloud authentication

To allow the ASA Virtual to authenticate with Microsoft Azure using a Service Principal, use the **failover cloud authentication** command in global configuration mode. To disable Microsoft Azure authentication, use the **no** form of this command.

failover cloud authentication { **application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key* }
no failover cloud authentication { **application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key* [**encrypt**] }

Syntax Description

application-id *appl-id*	Specifies the application ID required when you request an access key from the Azure infrastructure.
directory-id *dir-id*	Specifies the directory ID required when you request an access key from the Azure infrastructure.
key *secret-key*	Specifies the secret key required when you request an access key from the Azure infrastructure. If the **encrypt** keyword is present, the secret key is encrypted in the running configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

To be able to automatically make API calls to modify Azure route tables, the ASA Virtual HA units need to have Azure Active Directory credentials. Azure employs the concept of a Service Principal which, in simple terms, is a service account. A Service Proncipal allows you to provision an account with only enough permissions and scope to run a task within a predefined set of Azure resources.

When you have an application that needs to access or modify Azure resources, such as route tables, you must set up an Azure Active Directory (AD) application and assign the required permissions to it.

When you register an Azure AD application in the Azure portal, two objects are created in your Azure AD tenant: an application object, and a service principal object. The service principal object defines the policy and permissions for an application's use in a specific tenant, providing the basis for a security principal to represent the application at run-time.

After you set up the service principal, you obtain the **Directory ID**, **Application ID**, and **Secret key**. Theseare required to configure Azure authentication credentials.

Note Azure provides instructions on how to create an Azure AD application and service principal in the *Azure Resource Manager Documentation* .

Examples

The following example adds the Azure authentication credentials to the public cloud failover configuration:

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e420
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
failover cloud subscription-id	Adds the Azure Subscription ID to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud peer

To configure the public cloud failover peer, use the **failover cloud peer** command in global configuration mode. To disable the failover peer, use the **no** form of this command.

failover cloud peer { **ip** *ip-address* | **port** *port-number* }
no failover cloud peer

Syntax Description

ip *ip-address*	Specifies the IP address used to establish a TCP failover control connection to the public cloud HA peer.
port *port-number*	Specifies directory ID required when you request an access key from the Azure infrastructure.

Command Default

The default is the port number specified by the **failover cloud port control** command (or its default if not specified).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

The IP address is used to establish a TCP failover control connection to the public cloud HA peer. The port is used when attempting to open a failover connection to the HA peer, who may already by the Active unit. Configuring the port here may be needed if NAT is being performed between the HA peers. In most cases it won't need to be configured.

The **no** version of this command removes the peer IP address and sets the port number to its default value. If the port is not specified, the port number is set to its default value, even it is was set to a different value previously using this command.

Examples

The following example configures a public cloud failover peer:

```
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud polltime

To specify the public cloud failover unit poll and hold times, use the **failover cloud polltime** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover cloud polltime *poll_time* [**holdtime** *time*]
no failover cloud polltime

Syntax Description

holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the control port, after which the peer unit is declared failed. Valid values are from 3 to 60 seconds. You cannot enter a holdtime value that is less than 3 times the unit poll time.
polltime *poll_time*	Sets the amount of time between hello messages. Valid values are from 1 to 15 seconds.

Command Default

The default values on the ASA Virtual are as follows:

- The **polltime** *poll_time* is 5 second.
- The **holdtime** *time* is 15 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

Used to set the polling interval that the Backup uses for monitoring the presence of the Active unit. Optionally, you can also set the amount of time (hold time) that the Backup unit will wait, in the absence of a response from the Active unit, before taking over the Active role. The hold time will be forced to be at least three times the poll time. With a faster poll time, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

Examples

The following example configures failover polling for the public cloud failover configuration:

```
ciscoasa(config)# failover cloud polltime 10 holdtime 30
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud port

To specify the two TCP ports used by public cloud failover pairs, the port used for failover communication between the two peers, and the port used for Azure Load Balancer probes, use the **failover cloud port** command in global configuration mode. Use the **no** form of this command restore the default values for these ports.

failover cloud port { **control** *port-number* | **probe** *port-number* [**interface** *if-name*] }
no failover cloud port { **control** | **probe** }

Syntax Description

control *port-number*	(Optional) Specifies the TCP port used to communicate with public cloud HA peer.
probe *port-number*	(Optional) Specifies the TCP port used to respond to Azure Load Balancer health probes.
interface if-name	(Optional) Specifies an interface configured for the probe port which to accept Azure Load Balancer probes. If omitted, probes are accepted on the interface that the IP routing function in the ASA Virtual determines is the best for reaching the well-known source IP address used by the probes (168.63.129.16).

Command Default

The public cloud failover TCP control port number is 44442.

The Azure Load Balancer health probe port number is 44441.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

Use the **no** form of this command to restore the default port values.

On the physical ASA and the non-public cloud virtual ASA, the system handles failover conditions using gratuitous ARP requests where the backup ASA sends out a gratuitous ARP indicating it is now associated with the active IP and MAC addresses. Most public cloud environments do not allow broadcast traffic of this nature. For this reason, an HA configuration in the public cloud requires ongoing connections be restarted when failover happens.

The health of the active unit is monitored by the backup unit to determine if specific failover conditions are met. If those conditions are met, failover occurs. The failover time can vary from a few seconds to over a minute depending on the responsiveness of the public cloud infrastructure.

Examples

The following example configures TCP ports for failover communication and Azure Load Balancer probes to the public cloud failover configuration:

```
ciscoasa(config)# failover cloud port control 4444
ciscoasa(config)# failover cloud port probe 4443
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud route-table

To configure an Azure route table that directs internal routes to the Active unit, use the **failover cloud route-table** command in global configuration mode. To remove the route table configuration, use the **no** form of this command.

failover cloud route-table table-name [**subscription-id** *sub-id*]
no failover cloud route-table

Syntax Description

table-name	Specifies the name of the route table.
subscription-id *sub-id*	(Optional) Specifies the Azure Subscription ID, required when you want to modify Azure resources. If this parameter is present for a route table, this is the Azure subscription used when referencing the route table. If omitted, the subscription ID configured in global configuration mode is used.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.
9.9(2)	The **subscription-id** parameter was introduced.

Usage Guidelines

On failover, you want to direct internal routes to the active unit, which uses the configured route table information to automatically direct the routes to itself.

Configure these settings on both the primary and secondary units. There is no synching of configuration from the primary unit to the secondary unit.

To update user-defined routes in more than one Azure subscription, use the optional **subscription-id** parameter. The **subscription-id** at the **route-table** command level overrides the Azure Subscription ID specified at the global level. If you enter the **route-table** command without specifying the **subscription-id**, the global parameter is used.

Use the **no** form of this command remove the route table configuration.

Note When you enter this command the ASA Virtual switches to **cfg-fover-cloud-rt** mode.

Examples

The following examples show how to enable the cfg-fover-cloud-rt mode for public cloud failover route table configuration:

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)#
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
ciscoasa(cfg-fover-cloud-rt)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
rg	Adds an Azure resource group to the public cloud failover configuration.
route-table	Adds Azure route information to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.
failover cloud subscription-id	Adds the Azure Subscription ID to the public cloud failover configuration.

failover cloud route-table rg

To configure an Azure resource group, required for route table update requests, use the **rg** command in cfg-fover-cloud-rt configuration mode. To remove the resource group information from the configuration, use the **no** form of this command.

rg*resource-group*
no rg

Syntax Description

resource-group	Specifies the name of the Azure resource group.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
cfg-fover-cloud-rt configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

An Azure resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.

Configure these settings on both the primary and secondary units. There is no synching of configuration from the primary unit to the secondary unit.

Use the **no** form of this command remove the resource group information from the configuration.

Note Azure provides information about resource groups in the *Azure Resource Manager Documentation* .

Examples

The following example adds an Azure resource group to the public cloud failover configuration:

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
rg	Adds an Azure resource group to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud route-table route

To configure an route that requires updating during a failover, use the **route** command in cfg-fover-cloud-rt configuration mode. To remove the route information from the configuration, use the **no** form of this command.

route { **name** *route-name* **prefix** *address-prefix* **nexthop** *ip-address* }
no route name *route-name*

Syntax Description

route-name	Specifies the name of the route.
address-prefix	Specifies the address prefix, configured as an IP address prefix, a slash ('/') and a numerical netmask. For example '192.120.0.0/16'.
ip-address	Specifies the next hop IP address.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
cfg-fover-cloud-rt configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

On failover, you want to direct internal routes to the active unit, which uses the configured route table information to automatically direct the routes to itself.

Configure these settings on both the primary and secondary units. There is no synching of configuration from the primary unit to the secondary unit.

Use the **no** form of this command remove the route information from the configuration.

Note Azure provides information about routing requirements in the *Azure Resource Manager Documentation* .

Examples

The following example adds a route that requires updating to the public cloud failover configuration:

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
ciscoasa(cfg-fover-cloud-rt)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
rg	Adds an Azure resource group to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud subscription-id

To configure the Azure Subscription ID for the Azure Service Principal, use the **failover cloud subscription-id** command in global configuration mode. The **no** form of this command removes the subscription information from the configuration.

failover cloud subscription-id *sub-id*
no failover cloud subscription-id

Syntax Description

subscription-id *sub-id*	Specifies your Azure Subscription ID, required when you want to modify Azure resources.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

The Azure Subscription ID is needed to modify Azure route tables, for example, when you want to direct internal routes to the active unit.

Note You should be able to find your Subscription ID from the 'Subscriptions' tab of the Azure Portal, https://portal.azure.com .

Examples

The following example adds the Azure subscription ID to the public cloud failover configuration:

```
(config)# failover cloud (config)# failover cloud subscription-id ab2fe6b2-c2bd-44
(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.

Command	Description
failover cloud authentication	Adds the Azure authentication credentials to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud unit

To configure the ASA Virtual as either the primary or secondary unit in a public cloud failover configuration, use the **failover lan unit** command in global configuration mode. To remove the unit role setting, use the **no** form of this command.

failover cloud unit { **primary** | **secondary** }
no failover cloud unit

Syntax Description

primary	Specifies the ASA Virtual as a primary unit.
secondary	Specifies the ASA Virtual as a secondary unit.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

To ensure redundancy, you can deploy the ASA Virtual in a public cloud environment in an Active/Backup high availability (HA) configuration. HA in the public cloud implements a stateless Active/Backup solution that allows for a failure of the active ASA Virtual to trigger an automatic failover of the system to the backup ASA Virtual.

When setting up Active/Backup failover, you configure one unit to be primary and the other as secondary. At this point, the two units act as two separate devices for device and policy configuration, as well as for events, dashboards, reports and health monitoring.

The main differences between the two units in a failover pair are related to which unit is active and which unit is backup, namely which unit actively passes traffic. Although both units are capable of passing traffic, only the primary unit responds Load Balancer probes and programs any configured routes to use it as a route destination. The backup unit's primary function is to monitor the health of the primary unit. The primary unit always becomes the active unit if both units start up at the same time (and are of equal operational health).

Examples

The following example sets the ASA Virtual as the primary unit in a public cloud failover configuration:

```
ciscoasa(config)# failover cloud unit primary
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
failover cloud peer	Specifies public cloud failover peer information.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover exec

To execute a command on a specific unit in a failover pair, use the **failover exec** command in privileged EXEC or global configuration mode.

failover exec { **active** | **standby** | **mate** } *cmd_string*

Syntax Description

active	Specifies that the command is executed on the active unit or failover group in the failover pair. Configuration commands entered on the active unit or failover group are replicated to the standby unit or failover group.
cmd_string	The command to be executed. **Show**, configuration, and EXEC commands are supported.
mate	Specifies that the command is executed on the failover peer.
standby	Specifies that the command is executed on the standby unit or failover group in the failover pair. Configuration commands executed on the standby unit or failover group are not replicated to the active unit or failover group.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

You can use the **failover exec** command to send commands to a specific unit in a failover pair.

Because configuration commands are replicated from the active unit or context to the standby unit or context, you can use the **failover exec** command to enter configuration commands on the correct unit, no matter which unit you are logged in to. For example, if you are logged in to the standby unit, you can use the **failover exec active** command to send configuration changes to the active unit. Those changes are then replicated to the standby unit. Do not use the **failover exec** command to send configuration commands to the standby unit or context; those configuration changes are not replicated to the active unit and the two configurations will no longer be synchronized.

Output from configuration, exec, and **show** commands is displayed in the current terminal session, so you can use the **failover exec** command to issue **show** commands on a peer unit and view the results in the current terminal.

You must have sufficient privileges to execute a command on the local unit to execute the command on the peer unit.

Command Modes

The **failover exec** command maintains a command mode state that is separate from the command mode of your terminal session. By default, the **failover exec** command mode is global configuration mode for the specified device. You can change that command mode by sending the appropriate command (such as the **interface** command) using the **failover exec** command.

Changing **failover exec** command modes for the specified device does not change the command mode for the session that you are using to access the device. For example, if you are logged in to the active unit of a failover pair, and you issue the following command in global configuration mode, you will remain in global configuration mode, but any commands sent using the **failover exec** command will be executed in interface configuration mode:

```
ciscoasa(config)# failover exec interface GigabitEthernet0/1
ciscoasa(config)#
```

Changing commands modes for your current session to the device does not affect the command mode used by the **failover exec** command. For example, if you are in interface configuration mode on the active unit, and you have not changed the **failover exec** command mode, the following command would be executed in global configuration mode:

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

Use the **show failover exec** command to display the command mode on the specified device in which commands sent with the **failover exec** command are executed.

Security Considerations

The **failover exec** command uses the failover link to send commands to and receive the output of the command execution from the peer unit. You should use the **failover key** command to encrypt the failover link to prevent eavesdropping or man-in-the-middle attacks.

Limitations

- If you upgrade one unit using the zero-downtime upgrade procedure and not the other, both units must be running software that supports the **failover exec** command for the command to work.
- Command completion and context help are not available for the commands in the *cmd_string* argument.
- In multiple context mode, you can only send commands to the peer context on the peer unit. To send commands to a different context, you must first change to that context on the unit you are logged in to.
- You cannot use the following commands with the **failover exec** command:
  - **changeto**
  - **debug** (**undebug**)
- If the standby unit is in the failed state, it can still receive commands from the **failover exe**c command if the failure is due to a service card failure; otherwise, the remote command execution will fail.
- You cannot use the **failover exec** command to switch from privileged EXEC mode to global configuration mode on the failover peer. For example, if the current unit is in privileged EXEC mode, and you enter the **failover exec mate configure terminal** command, the **show failover exec mate** command output

will show that the failover exec session is in global configuration mode. However, entering configuration commands for the peer unit using the **failover exec** command will fail until you enter global configuration mode on the current unit.

- You cannot enter recursive **failover exec** commands, such as the **failover exec mate failover exec mate** *command.*
- Commands that require user input or confirmation must use the **/nonconfirm** option.

Examples

The following example shows how to use the **failover exec** command to display failover information on the active unit. The unit on which the command is executed is the active unit, so the command is executed locally.

```
ciscoasa(config)# failover exec active show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0
        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
ciscoasa(config)#
```

The following example uses the **failover exec** command to display the failover status of the peer unit. The command is executed on the the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
ciscoasa(config)# failover exec mate show failover
Failover On
Failover unit Secondary
```

```
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0
        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

The following example uses the **failover exec** command to display the failover configuration of the failover peer. The command is executed on the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
ciscoasa(config)# failover exec mate show running-config failover
failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

The following example uses the **failover exec** command to create a context on the active unit from the standby unit. The command is replicated from the active unit back to the standby unit. Note the two “Creating context...” messages. One is from the **failover exec** command output from the peer unit when the context is created, and the other is from the local unit when the replicated command creates the context locally.

```
ciscoasa(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
Total active Security Contexts: 1
! The following is executed in the system execution space on the standby unit.
ciscoasa(config)# failover exec active context text
```

```
Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)
ciscoasa(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)
Total active Security Contexts: 2
```

The following example shows the warning that is returned when you use the **failover exec** command to send configuration commands to a failover peer in the standby state:

```
ciscoasa# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241
  **** WARNING ****
       Configuration Replication is NOT performed from Standby unit to Active unit.
       Configurations are no longer synchronized.
ciscoasa(config)#
```

The following example uses the **failover exec** command to send the **show interface** command to the standby unit:

```
ciscoasa(config)# failover exec standby show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
```

```
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

The following example shows the error message returned when issuing an illegal command to the peer unit:

```
ciscoasa# failover exec mate bad command
bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

The following example shows the error message that is returned when you use the **failover exec** command when failover is disabled:

```
ciscoasa(config)# failover exec mate show failover
ERROR: Cannot execute command on mate because failover is disabled
```

Related Commands

Command	Description
debug fover	Displays failover-related debugging messages.
debug xml	Displays debugging messages for the XML parser used by the **failover exec** command.
show failover exec	Displays the **failover exec** command mode.

failover group

To configure an Active/Active failover group, use the **failover group** command in global configuration mode. To remove a failover group, use the **no** form of this command.

failover group *num*
no failover group *num*

Syntax Description

num	Failover group number. Valid values are 1 or 2.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can define a maximum of two failover groups. The **failover group** command can only be added to the system context of devices configured for multiple context mode. You can create and remove failover groups only when failover is disabled.

Entering this command puts you in the failover group command mode. The **primary**, **secondary**, **preempt**, **replication http**, **interface-policy**, **mac address**, and **polltime interface** commands are available in the failover group configuration mode. Use the **exit** command to return to global configuration mode.

Note The **failover polltime interface**, **failover interface-policy**, **failover replication http**, and **failover mac address** commands have no affect in Active/Active failover configurations. They are overridden by the following failover group configuration mode commands: **polltime interface**, **interface-policy**, **replication http**, and **mac address**.

When removing failover groups, you must remove failover group 1 last. Failover group 1 always contains the admin context. Any context not assigned to a failover group defaults to failover group 1. You cannot remove a failover group that has contexts explicitly assigned to it.

Note If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address using the **mac address** command.

Examples

The following partial example shows a possible configuration for two failover groups:

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
asr-group	Specifies an asymmetrical routing interface group ID.
interface-policy	Specifies the failover policy when monitoring detects interface failures.
join-failover-group	Assigns a context to a failover group.
mac address	Defines virtual mac addresses for the contexts within a failover group.
polltime interface	Specifies the amount of time between hello messages sent to monitored interfaces.
preempt	Specifies that a unit with a higher priority becomes the active unit after a reboot.
primary	Gives the primary unit higher priority for a failover group.
replication http	Specifies HTTP session replication for the selected failover group.
secondary	Gives the secondary unit higher priority for a failover group.

failover health-check bfd

To configure Bidirectional Forwarding Detection (BFD) for unit health monitoring, use the **failover health-check bfd** command in global configuration mode. To disable BFD, use the **no** form of this command.

failover health-check bfd *template_name*
no failover health-check bfd *template_name*

Syntax Description

template_name	The name of a BFD template.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

The regular unit monitoring can cause false alarms when CPU usage is high. The BFD method is distributed, so high CPU does not affect its operation.

You must first configure a BFD single-hop template to define the packet rate:

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier_value*

See the following limitations:

- Firepower 9300 and 4100 only.
- Active/Standby only.
- Routed mode only

Examples

The following example enables BFD unit health detection:

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
ciscoasa(config)# failover health-check bfd failover-temp
```

Related Commands

Command	Description
bfd template	Creates a template for use with BFD.
bfd interval	Defines the packet rate for the template.

failover interface ip

To specify the IPv4 address and mask or IPv6 address and prefixfor the failover interface and the Stateful Failover interface, use the **failover interface ip** command in global configuration mode. To remove the IP address, use the **no** form of this command.

failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address* | *prefix* **standby** *ipv6_address*]
no failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address* | *prefix* **standby** *ipv6_address*]

Syntax Description

if_name	Interface name for the failover or Stateful Failover interface.
ip_address mask	Specifies the IP address and mask for the failover or Stateful Failover interface on the primary device.
ipv6_address	Specifies the IPv6 address fore the failover or Stateful Failover interface on the primary device.
prefix	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).
standby *ip_address*	Specifies the IP address used by the secondary device to communicate with the primary device.
standby*ipv6_address*	Specifies the IPv6 address used by the secondary device to communicate with the primary device.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.2(2)	IPv6 address support was added.

Usage Guidelines

The standby address must be in the same subnet as the primary address.

You can only have one **failvover interface ip** command in the configuration. Therefore, your failover interface can have either an IPv6 or an IPv4 address; you cannot assign both an IPv6 and an IPv4 address to the interface.

Failover and Stateful Failover interfaces are functions of Layer 3, even when the ASA is operating in transparent firewall mode, and are global to the system.

In multiple context mode, you configure failover in the system context (except for the **monitor-interface** command).

This command must be part of the configuration when bootstrapping an ASA for LAN failover.

Examples

The following example shows how to specify an IPv4 address and mask for the failover interface:

```
ciscoasa(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

The following example shows how to specify an IPv6 address and prefix for the failover interface:

```
ciscoasa(config)# failover interface ip lanlink
2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover lan interface	Specifies the interface used for failover communication.
failover link	Specifies the interface used for Stateful Failover.
monitor-interface	Monitors the health of the specified interface.
show running-config failover	Displays the **failover** commands in the running configuration.

failover interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **failover interface-policy** command in global configuration mode. To restore the default, use the **no** form of this command.

failover interface-policy *num* [%]
no failover interface-policy *num* [%]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces when used as a number.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Command Default

The defaults are as follows:

- *num* is 1.
- Monitoring of physical interfaces is enabled by default; monitoring of logical interfaces is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

There is no space between the *num* argument and the optional **%** keyword.

If the number of failed interfaces meets the configured policy and the other ASA is functioning correctly, the ASA marks itself as failed and a failover might occur (if the active ASA is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the interface policy for each failover group with the **interface-policy** command in failover group configuration mode.

Examples

The following examples show two ways to specify the failover policy:

```
ciscoasa(config)# failover interface-policy 20%
ciscoasa(config)# failover interface-policy 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit and interface poll times.
failover reset	Restores a failed unit to an unfailed state.
monitor-interface	Specifies the interfaces being monitored for failover.
show failover	Displays information about the failover state of the unit.

failover ipsec pre-shared-key

To establish IPsec LAN-to-LAN tunnels on the failover and state links between the units to encrypt all failover communications, use the **failover ipsec pre-shared-key** command in global configuration mode To remove the key, use the **no** form of this command.

failover ipsec pre-shared-key *key*
no failover ipsec pre-shared-key

Syntax Description

0 Specifies an unencrypted password. This is the default.

8 Specifies an encrypted password. If you use a master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), then the key is encrypted in the configuration. If you are copying from the configuration (for example, from **more system:running-config** output), specify that the key is encrypted by using the **8** keyword.

Note
The **failover ipsec pre-shared-key** shows as ***** in **show running-config** output; this obscured key is not copyable.

key A *key* that you specify on both units that is used by IKEv2 to establish the tunnels, up to 128 characters in length.

Command Default

0 (unencrypted) is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

Unless you secure the failover communications, all information sent over the failover and Stateful Failover links is sent in clear text. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication if you are using the ASA to terminate VPN tunnels.

We recommend using the **failover ipsec pre-shared-key** method of encryption over the legacy **failover key** method.

You cannot use both IPsec encryption and the legacy **failover key** encryption. If you configure both methods, IPsec is used. However, if you use the master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), you must first remove the failover key using the **no failover key** command before you configure IPsec encryption.

Note If you configure HA failover encryption in evaluation mode, the systems use DES for the encryption. If you then register the devices using an export-compliant account, the devices will use AES after a reboot. Thus, if a system reboots for any reason, including after installing an upgrade, the peers will be unable to communicate and both units will become the active unit. We recommend that you do not configure encryption until after you register the devices. If you do configure this in evaluation mode, we recommend you remove the encryption before registering the devices.

When you use this command, the system creates an IKE policy. Because the system allows a maximum of 20 IKE policies, if there are already 20, this command will fail.

Note Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.

Examples

The following example configures an IPsec pre-shared key:

```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

Related Commands

Command	Description
show running-config failover	Displays the failover commands in the running configuration.
show vpn-sessiondb	Shows information about VPN tunnels, including the failover IPsec tunnels.

failover key

To specify the key for encrypted and authenticated communication between units in a failover pair (over the failover and state links), use the **failover key** command in global configuration mode. To remove the key, use the **no** form of this command.

failover key [**0** | **8**] { **hex** *key* | *shared_secret* }
no failover key

Syntax Description

0	Specifies an unencrypted password. This is the default.
8	Specifies an encrypted password. If you use a master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), then the shared secret is encrypted in the configuration. If you are copying from the configuration (for example, from **more system:running-config** output), specify that the shared secret is encrypted by using the **8** keyword. **Note** The **failover key** shared secret shows as ***** in **show running-config** output; this obscured key is not copyable.
hex *key*	Specifies a hexadecimal value for the encryption key. The key must be 32 hexadecimal characters (0-9, a-f).
shared_secret	Specifies an alphanumeric shared secret. The secret can be from 1 to 63 characters. Valid character are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.

Command Default

0 (unencrypted) is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was modified from **failover lan key** to **failover key**.
7.0(4)	This command was modified to include the **hex** *key* keyword and argument.
8.3(1)	This command was modified to support the master passphrase with the **0** and **8** keywords.

Usage Guidelines

Unless you secure the failover communications, all information sent over the failover and Stateful Failover links is sent in clear text. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication if you are using the ASA to terminate VPN tunnels.

We recommend using the **failover ipsec pre-shared-key** method of encryption over the legacy **failover key** method.

You cannot use both IPsec encryption (the **failover ipsec pre-shared-key** command) and the legacy **failover key** encryption. If you configure both methods, IPsec is used. However, if you use the master passphrase (see the **password encryption aes** and **key config-key password-encryption** commands), you must first remove the failover key using the **no failover key** command before you configure IPsec encryption.



Note If you configure HA failover encryption in evaluation mode, the systems use DES for the encryption. If you then register the devices using an export-compliant account, the devices will use AES after a reboot. Thus, if a system reboots for any reason, including after installing an upgrade, the peers will be unable to communicate and both units will become the active unit. We recommend that you do not configure encryption until after you register the devices. If you do configure this in evaluation mode, we recommend you remove the encryption before registering the devices.

Examples

The following example shows how to specify a shared secret for securing failover communication between units in a failover pair:

```
ciscoasa(config)# failover key abcdefg
```

The following example shows how to specify a hexadecimal key for securing failover communication between two units in a failover pair:

```
ciscoasa(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

The following example shows an encrypted password copied and pasted from **more system:running-config** output:

```
ciscoasa(config)# failover key 8 TPZCVNgdegLhWMa
```

Related Commands

Command	Description
show running-config failover	Displays the failover commands in the running configuration.

failover lan interface

To specify the interface used for failover communication, use the **failover lan interface** command in global configuration mode. To remove the failover interface, use the **no** form of this command.

failover lan interface *if_name* { *phy_if* [*.sub_if*] | *vlan_if*] }
no failover lan interface [*if_name* { *phy_if* [*.sub_if*] | *vlan_if*] }]

Syntax Description

if_name	Specifies the name of the ASA interface dedicated to failover.
phy_if	Specifies the physical interface.
sub_if	(Optional) Specifies a subinterface number.
vlan_if	Used on the ASASM to specify a VLAN interface as the failover link.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	The *phy_if* argument was added.
7.2(1)	The *vlan_if* argument was added.
9.5(1)	This command was modified to accept the management interface on the ASA 5506H-X.

Usage Guidelines

Do not use this command when both primary and secondary units have failover enabled. Changing the failover interface configuration leads to a split-brain scenario (Active-Active).

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit.

Failover Link Data

The following information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keep-alives)

- Network link status
- MAC address exchange
- Configuration replication and synchronization

Interface for the Failover Link

You can use any unused data interface (physical, redundant, or EtherChannel) as the failover link; however, you cannot specify an interface that is currently configured with a name. The failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface can only be used for the failover link (and also for the state link). The ASA does not support sharing interfaces between user data and the failover link even if different subinterfaces are configured for user data and failover. A separate physical, EtherChannel, or redundant interface must be used for the failover link.

See the following guidelines for the failover link:

- 5506-X through 5555-X—You cannot use the Management interface as the failover link; you must use a data interface. The only exception is for the 5506H-X, where you can use the management interface as the failover link.
- 5506H-X—You can use the Management 1/1 interface as the failover link. If you configure it for failover, you must reload the device for the change to take effect. In this case, you cannot also use the ASA Firepower module, because it requires the Management interface for management purposes.
- 5585-X—Do not use the Management 0/0 interface, even though it can be used as a data interface. It does not support the necessary performance for this use.
- Firepower 9300 ASA security module—You can use either a management type or data type interface as the failover link. To conserve interfaces and to share a failover link between modules in the same chassis, use a management type interface. For example, you have 2 chassis, each with 3 ASA security modules. You can create 3 failover pairs between the chassis. You can use a single 10 GigabitEthernet management interface between the chassis to act as the failover link. Just configure a unique VLAN subinterface within each module.
- All models—1 GB interface is large enough for a combined failover and state link.

For a redundant interface used as the failover link, see the following benefits for added redundancy:

- When a failover unit boots up, it alternates between the member interfaces to detect an active unit.
- If a failover unit stops receiving keepalive messages from its peer on one of the member interfaces, it switches to the other member interface.

For an EtherChannel used as the failover link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a failover link.

Connecting the Failover Link

Connect the failover link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the failover interfaces of the ASA.
- Using an Ethernet cable to connect the units directly, without the need for an external switch.

If you do not use a switch between the units, if the interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which unit has the failed interface and caused the link to come down.

The ASA supports Auto-MDI/MDIX on its copper Ethernet ports, so you can either use a crossover cable or a straight-through cable. If you use a straight-through cable, the interface automatically detects the cable and swaps one of the transmit/receive pairs to MDIX.

Additional Guidelines

- When using VLANs on connecting switches, use a dedicated VLAN for the failover link. Sharing the failover link VLAN with any other VLANs can cause intermittent traffic problems and ping and ARP failures. If you use a switch to connect the failover link, use dedicated interfaces on the switch and ASA for the failover link; do not share the interface with subinterfaces carrying regular network traffic.
- On systems running in multiple context mode, the failover link resides in the system context. This interface and the state link, if used, are the only interfaces that you can configure in the system context. All other interfaces are allocated to and configured from within security contexts.
- The IP address and MAC address for the failover link do not change at failover.



Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

Examples

The following example configures the failover parameters for the primary unit, including a shared failover and state link:

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

Related Commands

Command	Description
failover lan unit	Specifies the LAN-based failover primary or secondary unit.
failover link	Specifies the Stateful Failover interface.

failover lan unit

To configure the ASA as either the primary or secondary unit in a LAN failover configuration, use the **failover lan unit** command in global configuration mode. To restore the default setting, use the **no** form of this command.

failover lan unit { **primary** | **secondary** }
no failover lan unit { **primary** | **secondary** }

Syntax Description

primary	Specifies the ASA as a primary unit.
secondary	Specifies the ASA as a secondary unit.

Command Default

Secondary.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

For Active/Standby failover, the primary and secondary designation for the failover unit refers to which unit becomes active at boot time. The primary unit becomes the active unit at boot time when the following occurs:

- The primary and secondary unit both complete their boot sequence within the first failover poll check.
- The primary unit boots before the secondary unit.

If the secondary unit is already active when the primary unit boots, the primary unit does not take control; it becomes the standby unit. In this case, you need to enter the **no failover active** command on the secondary (active) unit to force the primary unit back to active status.

For Active/Active failover, each failover group is assigned a primary or secondary unit preference. This preference determines on which unit in the failover pair the contexts in the failover group become active at startup when both units start simultaneously (within the failover polling period).

This command must be part of the configuration when bootstrapping an ASA for LAN failover.

Examples

The following example sets the ASA as the primary unit in LAN-based failover:

```
ciscoasa(config)# failover lan unit primary
```

Related Commands

Command	Description
failover lan interface	Specifies the interface used for failover communication.

failover link

To specify the Stateful Failover interface and to enable Stateful Failover, use the **failover link** command in global configuration mode. To remove the Stateful Failover interface, use the **no** form of this command.

failover link *if_name* [*phy_if*]
no failover link

Syntax Description

if_name	Specifies the name of the ASA interface dedicated to Stateful Failover.
phy_if	(Optional) Specifies the physical or logical interface port. If the Stateful Failover interface is sharing the interface assigned for failover communication or sharing a standard firewall interface, then this argument is not required.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	The *phy_if* argument was added.
7.0(4)	This command was modified to accept standard firewall interfaces.
9.5(1)	This command was modified to accept the management interface on the ASA 5506H-X.

Usage Guidelines

To use Stateful Failover, you must configure a Stateful Failover link (also known as the state link) to pass connection state information.

Shared with the Failover Link

Sharing a failover link is the best way to conserve interfaces. If you experience performance problems on that interface, consider dedicating a separate interface for the state link.

Dedicated Interface

You can use a dedicated data interface (physical, redundant, or EtherChannel) for the state link. For an EtherChannel used as the state link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used.

Connect a dedicated state link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the failover interfaces of the ASA.
- Using an Ethernet cable to connect the appliances directly, without the need for an external switch.

If you do not use a switch between the units, if the interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which unit has the failed interface and caused the link to come down.

The ASA supports Auto-MDI/MDIX on its copper Ethernet ports, so you can either use a crossover cable or a straight-through cable. If you use a straight-through cable, the interface automatically detects the cable and swaps one of the transmit/receive pairs to MDIX.

For optimum performance when using long distance failover, the latency for the state link should be less than 10 milliseconds and no more than 250 milliseconds. If latency is more than10 milliseconds, some performance degradation occurs due to retransmission of failover messages.

Additional Guidelines

- In multiple context mode, the Stateful Failover link resides in the system context. This interface and the failover interface are the only interfaces in the system context. All other interfaces are allocated to and configured from within security contexts.
- The IP address and MAC address for the Stateful Failover link does not change at failover unless the Stateful Failover link is configured on a regular data interface.



Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

Examples

The following example configures the failover parameters for the primary unit, including a shared failover and state link:

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

Related Commands

Command	Description
failover interface ip	Configures the IP address of the **failover** command and Stateful Failover interface.
failover lan interface	Specifies the interface used for failover communication.

failover mac address

To specify the failover virtual MAC address for a physical interface, use the **failover mac address** command in global configuration mode. To remove the virtual MAC address, use the **no** form of this command.

failover mac address *phy_if active_mac standby_mac*
no failover mac address *phy_if active_mac standby_mac*

Syntax Description

active_mac	The MAC address assigned to the specified interface the active ASA. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.
phy_if	The physical name of the interface to set the MAC address.
standby_mac	The MAC address assigned to the specified interface of the standby ASA. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.

Command Default

Not configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **failover mac address** command lets you configure virtual MAC addresses for an Active/Standby failover pair. If virtual MAC addresses are not defined, then when each failover unit boots it uses the burned-in MAC addresses for its interfaces and exchanges those addresses with its failover peer. The MAC addresses for the interfaces on the primary unit are used for the interfaces on the active unit.

However, if both units are not brought online at the same time and the secondary unit boots first and becomes active, it uses the burned-in MAC addresses for its own interfaces. When the primary unit comes online, the secondary unit will obtain the MAC addresses from the primary unit. This change can disrupt network traffic. Configuring virtual MAC addresses for the interfaces ensures that the secondary unit uses the correct MAC address when it is the active unit, even if it comes online before the primary unit.

The **failover mac address** command is unnecessary (and therefore cannot be used) on an interface configured for LAN-based failover because the **failover lan interface** command does not change the IP and MAC addresses when failover occurs. This command has no affect when the ASA is configured for Active/Active failover.

When adding the **failover mac address** command to your configuration, it is best to configure the virtual MAC address, save the configuration to flash memory, and then reload the failover pair. If the virtual MAC address is added when there are active connections, then those connections stop. Also, you must write the complete configuration, including the **failover mac address** command, to the flash memory of the secondary ASA for the virtual MAC addressing to take effect.

When removing the MAC address using the **no** form of this command, it is recommended to reload both units to ensure the changes take effect.

If the **failover mac address** is specified in the configuration of the primary unit, it should also be specified in the bootstrap configuration of the secondary unit.



Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the virtual MAC address for each interface in a failover group with the **mac address** command in failover group configuration mode.

You can also set the MAC address using other commands or methods, but we recommend using only one method. If you set the MAC address using multiple methods, the MAC address used depends on many variables, and might not be predictable.

Examples

The following example configures the active and standby MAC addresses for the interface named intf2:

```
ciscoasa(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

Related Commands

Command	Description
show interface	Displays interface status, configuration, and statistics.

failover polltime

To specify the failover unit poll and hold times, use the **failover polltime** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec** *time*]
no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the failover link, after which the peer unit is declared failed. Valid values are from 3 to 45 seconds or from 800 to 999 milliseconds if the optional **msec** keyword is used.
msec	(Optional) Specifies that the given time is in milliseconds.
poll_time	Sets the amount of time between hello messages. Valid values are from 1 to 15 seconds or from 200 to 999 milliseconds if the optional **msec** keyword is used.
unit	(Optional) Indicates that the command is used for unit poll and hold times. Adding this keyword to the command does not have any affect on the command, but it can make it easier to differentiate this command from the **failover polltime interface** commands in the configuration.

Command Default

The default values on the ASA are as follows:

- The *poll_time* is 1 second.
- The **holdtime** *time* is 15 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from the **failover poll** command to the **failover polltime** command and now includes **unit** and **holdtime** keywords.

Release	Modification
7.2(1)	The **msec** keyword was added to the **holdtime** keyword. The **polltime** minimum value was reduced to 200 milliseconds from 500 milliseconds. The **holdtime** minimum value was reduced to 800 milliseconds from 3 seconds.

Usage Guidelines

You cannot enter a **holdtime** value that is less than three times the unit poll time. With a faster poll time, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switch overs when the network is temporarily congested.

If a unit does not receive a hello packet on the failover link for one polling period, additional testing occurs through the remaining interfaces. If there is still no response from the peer unit during the hold time, then the unit is considered failed and, if the failed unit is the active unit, the standby unit takes over as the active unit.

You can include both **failover polltime** [**unit**] and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through an ASA in a failover configuration, you should decrease the failover hold time on the ASA to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example changes the unit poll time frequency to 3 seconds:

```
ciscoasa(config)# failover polltime 3
```

The following example configures the ASA to send a hello packet every 200 milliseconds and to fail over in 800 milliseconds if no hello packets are received on the failover interface within that time. The optional **unit** keyword is included in the command.

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

Related Commands

Command	Description
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.
polltime interface	Specifies the interface poll and hold times for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover polltime interface

To specify the data interface polltime and holdtime in an Active/Standby failover configuration, use the **failover polltime interface** command in global configuration mode. To restore the default polltime and holdtime, use the **no** form of this command.

failover polltime interface [**msec**] *polltime* [**holdtime** *time*]
no failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time (as a calculation) between the last-received hello message from the peer unit and the commencement of interface tests to determine the health of the interface. It also sets the duration of each interface test as *holdtime* /16. Valid values are from 5 to 75 seconds. The default is 5 times the *polltime* . You cannot enter a holdtime value that is less than five times the *polltime* . To calculate the time before starting interface tests (y): **1.** x = (*holdtime* /*polltime)/2* , rounded to the nearest integer. (.4 and down rounds down; .5 and up rounds up.) **2.** y = x**polltime* For example, if you use the default holdtime of 25 and polltime of 5, then y = 15 seconds.
polltime	Specifies how long to wait between sending a hello packet to the peer. Valid values range from 1 to 15 seconds. The default is 5. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Command Default

The default values are as follows:

- The poll *time* is 5 seconds.
- The **holdtime** *time* is 5 times the poll *time*.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from the **failover poll** command to the **failover polltime** command and includes **unit**, **interface**, and **holdtime** keywords.
7.2(1)	The optional **holdtime** *time* and the ability to specify the poll time in milliseconds was added.

Usage Guidelines

This command is available for Active/Standby failover only. For Active/Active failover, use the **polltime interface** command in failover group configuration mode.

With a faster poll time, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through an ASA in a failover configuration, you should decrease the failover hold time on the ASA to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example sets the interface polltime frequency to 15 seconds:

```
ciscoasa(config)# failover polltime interface 15
```

The following example sets the interface polltime frequency to 500 milliseconds and the holdtime to 5 seconds:

```
ciscoasa(config)# failover polltime interface msec 500 holdtime 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit failover poll and hold times.
polltime interface	Specifies the interface polltime for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover poll-time link-state

To change the interface link state poll time, use the **failover polltime link-state** command in global configuration mode. To disable the link-state poll, use the **no** form of this command.

failover polltime link-state msec *poll_time*
no failover polltime link-state msec *poll_time*

Syntax Description

msec *poll_time*	Sets the polltime between 300 and 799 milliseconds.

Command Default

The default polltime is 500 msec.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

By default, each ASA in a failover pair checks the link state of its interfaces every 500 msec. You can customize the polltime; for example, if you set the polltime to 300 msec, the ASA can detect an interface failure and trigger failover faster.

In Active/Active mode, you set this rate for the system; you cannot set this rate per failover group.

Examples

The following example sets the link-state polltime to 300 msec:

```
ciscoasa(config)# failover polltime link-state msec 300
```

Related Commands

Command	Description
failover polltime unit	Sets the polltime for the unit health check.
failover polltime interface	Sets the polltime for the interface health check.

failover reload-standby

To force the standby unit to reboot, use the **failover reload-standby** command in privileged EXEC mode.

failover reload-standby

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use this command when your failover units do not synchronize. The standby unit restarts and resynchronizes to the active unit after it finishes booting.

Examples

The following example shows how to use the **failover reload-standby** command on the active unit to force the standby unit to reboot:

```
ciscoasa# failover reload-standby
```

Related Commands

Command	Description
write standby	Writes the running configuration to the memory on the standby unit.

failover replication http

To enable HTTP (port 80) connection replication, use the **failover replication http** command in global configuration mode. To disable HTTP connection replication, use the **no** form of this command.

failover replication http
no failover replication http

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from **failover replicate http** to **failover replication http**.

Usage Guidelines

By default, the ASA does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **failover replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment.

In Active/Active failover configurations, you control HTTP session replication per failover group using the **replication http** command in failover group configuration mode.

Examples

The following example shows how to enable HTTP connection replication:

```
ciscoasa(config)# failover replication http
```

Related Commands

Command	Description
replication http	Enables HTTP session replication for a specific failover group.
show running-config failover	Displays the **failover** commands in the running configuration.

failover replication rate

To configure the bulk-sync connection replication rate, use the **failover replication rate** command in global configuration mode. To restore the default setting, use the **no** form of this command.

failover replication rate *rate*
no failover replication rate

Syntax Description

rate	Sets the number of connections per second. Values and the default setting depend on your model's maximum connections per second.

Command Default

Varies depending on your model.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(4.1)/8.5(1.7)	This command was added.

Usage Guidelines

You can configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASASM is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synced.

Examples

The following example sets the failover replication rate to 20000 connections per second:

```
ciscoasa(config)# failover replication rate 20000
```

Related Commands

Command	Description
failover rate http	Enables HTTP connection replication.

failover reset

To restore a failed ASA to an unfailed state, use the **failover reset** command in privileged EXEC mode.

failover reset [**group** *group_id*]

Syntax Description

group	(Optional) Specifies a failover group. The **group** keyword applies to Active/Active failover only.
group_id	Failover group number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was modified to add the optional failover group ID.

Usage Guidelines

The **failover reset** command allows you to change the failed unit or group to an unfailed state. The **failover reset** command can be entered on either unit, but we recommend that you always enter the command on the active unit. Entering the failover reset command at the active unit will "unfail" the standby unit.

You can display the failover status of the unit with the **show failover** or **show failover state** commands.

There is no **no** form of this command.

In Active/Active failover, entering **failover reset** resets the whole unit. Specifying a failover group with the command resets only the specified group.

Examples

The following example shows how to change a failed unit to an unfailed state:

```
ciscoasa# failover reset
```

Related Commands

Command	Description
failover interface-policy	Specifies the policy for failover when monitoring detects interface failures.
show failover	Displays information about the failover status of the unit.

failover standby config-lock

To lock configuration changes on the standby unit or standby context in a failover pair, use the **failover standby config-lock** command in global configuration mode. To allow configuration on the standby unit, use the **no** form of this command.

failover standby config-lock
no failover standby config-lock

Syntax Description

This command has no arguments or keywords.

Command Default

By default, configurations on the standby unit/context are allowed with a warning message.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

You can lock configuration changes on the standby unit (Active/Standby failover) or the standby context (Active/Active failover) so you cannot make changes on the standby unit outside normal configuration syncing.

Examples

The following example disallows configuration on the standby unit:

```
ciscoasa(config)# failover standby config-lock
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover timeout

To specify the failover reconnect timeout value for asymmetrically routed sessions, use the **failover timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

failover timeout *hh* [**:mm :** [**:ss**]
failover timeout [*hh* [**:mm :** [**:ss**]]

Syntax Description

hh Specifies the number of hours in the timeout value. Valid values range from -1 to 1193. By default, this value is set to 0.

Setting this value to -1 disables the timeout, allowing connections to reconnect after any amount of time.

Setting this value to 0, without specifying any of the other timeout values, sets the command back to the default value, which prevents connections from reconnecting. Entering **no failover timeout** command also sets this value to the default (0).

Note
When set to the default value, this command does not appear in the running configuration.

mm (Optional) Specifies the number of minutes in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.

ss (Optional) Specifies the number of seconds in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.

Command Default

By default, *hh*, *mm*, and *ss* are 0, which prevents connections from reconnecting.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was modified to appear in the command listing.

Usage Guidelines

This command is used in conjunction with the **static** command with the **nailed** option. The **nailed** option allows connections to be reestablished in a specified amount of time after bootup or a system goes active. The **failover timeout** command specifies that amount of time. If not configured, the connections cannot be reestablished. The **failover timeout** command does not affect the **asr-group** command.

Note Adding the **nailed** option to the **static** command causes TCP state tracking and sequence checking to be skipped for the connection.

Entering the **no** form of this command restores the default value. Entering **failover timeout 0** also restores the default value. When set to the default value, this command does not appear in the running configuration.

Examples

The following example switches the standby group 1 to active:

```
ciscoasa(config)# failover timeout 12:30
ciscoasa(config)# show running-config failover
no failover
failover timeout 12:30:00
```

Related Commands

Command	Description
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

failover trace

To configure and view trace levels of a failover trace log, use the **failover trace** command in configuration mode.

failover trace [*options*]

Syntax Description

failover trace [*options*]	(Optional) Shows the failover event trace. Options include to show the failover event trace by levels (1-5): • **critical** — to filter failover critical event trace (level = 1) • **debugging**— to filter failover debugging trace (Debug level = 5) • **error**— to filter failover internal exception (level = 2) • **informational**— to filter failover informational trace (level = 4) • **warning**— to filter failover warnings (level = 3)

Command Default

Default value is configurable only in version 9.16.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.16	This command is available only in version 9.16.
9.18	This command is no longer configurable and set to informational by default.

Usage Guidelines

Use the **no** form of this command to disable failover.

failover wait-disable

When using bridge groups or IPv6 duplicate address detection (DAD), to disable waiting for the failover peer unit to go into the standby state, use the **failover wait-disable** command in global configuration mode. With these features, the new active unit waits to pass traffic until after the standby unit finishes network tasks and transitions to the standby state. To reenable waiting, use the **no** form of this command.

failover wait-disable
no failover wait-disable

Command Default

By default, the active unit will wait up to 3000 ms for the standby unit to finish transitiong to the standby state (**no failover wait-disable**).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.15(1)	This command was introduced.

Usage Guidelines

When you use bridge groups or IPv6 DAD, when a failover occurs the new active unit waits up to 3000 ms for the standby unit to finish networking tasks and transition to the standby state. Then the active unit can start passing traffic. To avoid this delay, you can disable the waiting time, and the active unit will start passing traffic before the standby unit transitions.

Examples

The following example disables waiting:

```
ciscoasa(config)# failover wait-disable
ciscoasa(config)#
```

fallback (Deprecated)

To configure the fallback timers that the Cisco Intercompany Media Engine uses to fallback from VoIP to PSTN when connection integrity degrades, use the **fallback** command in uc-ime configuration mode. To remove the fallback settings, use the **no** form of this command.

fallback { **sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec* }
no fallback { **sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec* }

Syntax Description

filename	Specifies the filename of the sensitivity file. Enter the name of a file on disk that includes the .fbs file extension. To specify the filename, you can include the path on the local disk, for example disk0:/file001.fbs .
hold-down timer	Sets the amount of time that ASA waits before notifying Cisco UCM whether to fall back to PSTN.
monitoring timer	Sets the time between which the ASA samples the RTP packets received from the Internet. The ASA uses the data sample to determine if fallback to the PSTN is needed for a call.
sensitivity-file	Specifies the file to use for mid-call PSTN fallback. The sensitivity file is parsed by the ASA and entered in the RMA library.
timer_millisec	Specifies the length of the monitoring timer in milliseconds. Enter an integer within the range 10-600. By default, the length of the monitoring timer is 100 milliseconds.
timer_sec	Secifies the length of the hold-down timer in seconds. Enter an integer within the range 10-360. By default, the length of the hold-down timer is 20 seconds.

Command Default

By default, the length of the monitoring timer is 100 milliseconds. The length of the hold-down timer is 20 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Uc-ime configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	The command was added.
9.4(1)	This command was deprecated along with all **uc-ime** mode commands.

Usage Guidelines

Specifies the fallback timer for the Cisco Intercompany Media Engine.

Internet connections can vary wildly in their quality and vary over time. Therefore, even if a call is sent over VoIP because the quality of the connection was good, the connection quality might worsen mid-call. To ensure an overall good experience for the end user, Cisco Intercompany Media Engine attempts to perform a mid-call fallback.

Performing a mid-call fallback requires the ASA to monitor the RTP packets coming from the Internet and send information into an RTP Monitoring Algorithm (RMA) API, which will indicates to the ASA whether fallback is required. If fallback is required, the ASA sends a REFER message to Cisco UCM to tell it that it needs to fallback the call to PSTN.



Note You cannot change the fallback timer when the Cisco Intercompany Media Engine proxy is enabled for SIP inspection. Remove the Cisco Intercompany Media Engine proxy from SIP inspection before changing the fallback timer.

Examples

The following example shows how to configure the Cisco Intercompany Media Engine while specifying the fallback timers:

```
ciscoasa
(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

The following example shows how to configure the Cisco Intercompany Media Engine while specifying a sensitivity file:

```
ciscoasa
(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback sensitivity-file local_uc-ime_fallback_policy
```

Related Commands

Command	Description
show running-config uc-ime	Shows the running configuration of the Cisco Intercompany Media Engine proxy.
show uc-ime	Displays statistical or detailed information about fallback notifications, mapping service sessions, and signaling sessions.
uc-ime	Creates the Cisco Intercompany Media Engine proxy instance on the ASA.

fast-flood

To fill IS-IS link-state packets (LSPs), use the **fast-flood** command in router isis configuration mode. To disable the fast flooding, use the **no** form of this command.

fast-flood [*lsp-number*]
no fast-flood [*lsp-number*]

Syntax Description

lsp-number	(Optional) The number of LSPs to be flooded before the SPF is started. The range is 1 to 15. The default is 5.

Command Default

Fast flooding is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	The command was added.

Usage Guidelines

The **fast-flood** command sends a specified number of LSPs from the ASA. If no LSP number value is specified, the default it 5. The LSPs invoke SPF before running SPF. When you speed up the LSP flooding process, you improve overall network convergence time.

The ASA should always flood, at least, the LSP that triggered SPF before the router runs the SPF computation.

We recommend that you enable the fast flooding of LSPs before the ASA runs the SPF computation, in order to achieve a faster convergence time

Examples

In the following example, the **fast-flood** command is entered to configure the ASA to fill the first seven LSPs that invoke SPF, before the SPF computation is started. When the **show running-configuration** command is entered, the output confirms that fast flooding has been enabled on the ASA:

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)# fast-flood 7
ciscoasa(config-router)# end
```

```
ciscoasa# show running-config | inc fast-flood
fast-flood 7
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.

Command	Description
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.

Command	Description
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

fault-monitor block-depletion

To enable block depletion monitoring, enter the **fault-monitor block depletion** command in router configuration mode. To disable the monitoring, enter the **no** form of this command.

fault-monitor block-depletion [**recovery-action** { *none* | *reload* } | **monitor-interval** *duration*]
no fault-monitor block-depletion

recovery-action { *none* | *reload* }	The default recovery action is **reload**, because when the device detects a block pool depletion, device reload is the only way to recovery. Avoiding device reload using the **none** option must be used with caution and with guidance from the Cisco TAC team. Typically, **none** is used if there are any false positive block detection or the TAC team needs to collect additional data before device goes for auto reload.
monitor-interval *duration*	You can modify the monitoring interval, which defines the duration to wait before any recovery action. The default value is 60 seconds. Enter a value between 30 and 300 seconds.

Command Default

Block depletion monitoring is enabled by default. The block depletion recovery action is set to *reload* and the default monitoring interval is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router fault-monitor configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.22(3)	The command was added.

Usage Guidelines

The fault manager monitors the device for various kinds of faults and recovers the device when a fault occurs. When you enable block-depletion, the fault manager collects troubleshooting logs during block depletion for diagnosis and restores the device's health through the reload action without any manual intervention.

When block depletion is detected, a compressed troubleshooting file is created in the **disk0:/FaultMonitor/** directory. The filename uses the format *bdep-ts_YYYYMMDD_HHMMSS_TIMEZONE.log*. Older files are purged automatically, retaining only the latest ten compressed files.

When block depletion is detected on a control node in a cluster device, the control node leaves the cluster, force crashes, and reloads. One of the data nodes then becomes the new control node. After reloading, the node rejoins the cluster as a data node. If block depletion is detected on a data node, the data node leaves the cluster, force crashes, reloads, and rejoins the cluster as a data node.

In a high-availability setup, when block depletion is detected on the device, the system moves the active device to a failed state to allow the standby device to take over. This switchover reduces downtime and packet loss. The failed peer sends logs for diagnostics. Use the show block to diagnose and debug the cause of block depletion.

Examples

To view the default block-depletion configuration, use **show running-config all fault-monitor**:

```
ciscoasa# show running-config all fault-monitor
fault-monitor
   block-depletion
   block-depletion recovery-action reload
   block-depletion monitor-interval 60
```

The following example illustrates modifying recovery action and monitoring interval for block-depletion:

```
ciscoasa# fault-monitor
ciscoasa(config-fault-monitor)# block-depletion recovery-action ?
fault-monitor mode commands/options:
  none    No Recovery Action
  reload  Reload the device on block depletion
ciscoasa(config-fault-monitor)# block-depletion monitor-interval ?
fault-monitor mode commands/options:
  <30-300>  Duration in seconds to wait before recovery action
ciscoasa(config-fault-monitor)# block-depletion monitor-interval 30
```

fault-monitor mbuf-depletion

To enable MBUF depletion monitoring, enter the **fault-monitor mbuf-depletion** command in router configuration mode. To disable the monitoring, enter the **no** form of this command.

fault-monitor mbuf-depletion [**recovery-action** { *none* | *reload* } | **monitor-interval** *duration*]
no fault-monitor mbuf-depletion

recovery-action { *none* | *reload* }	The default action, **reload**, collects troubleshooting data and reloads the device with core dump. Whereas, the **none** action logs the fault and collects troubleshooting data, but no automatic recovery is performed.
monitor-interval *duration*	You can modify the monitoring interval, which defines the duration to wait before any recovery action. The default value is 60 seconds. Enter a value between 30 and 300 seconds.

Command Default

The MBUF depletion recovery action is set to *reload* and the default monitoring interval is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router fault-monitor configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.24(10)	The command was added.

Usage Guidelines

The fault manager monitors the device for various kinds of faults and recovers the device when a fault occurs. When you enable mbuf-depletion, the fault manager collects troubleshooting logs during the depletion for diagnosis and restores the device's health through the reload action without any manual intervention.

The default recovery action is **reload**, because when the pool depletion is detected, device reload is the only way to recovery. When MBUF pool is depleted, and the monitoring interval is exhausted, fault monitor state detects the MBUF depletion. The device crashes and reloads. The fault monitor returns to monitoring state after the waiting state time period.

Avoiding device reload using the **none** option must be used with caution and with guidance from the Cisco TAC team. When MBUF pool is depleted, and the monitoring interval is exhausted, fault monitor state detects

the MBUF depletion and change to waiting state till 20% of the MBUF pool are recovered. When MBUF pool is released, the fault monitor state changes back to monitoring. Typically, **none** is used if there are any false positive block detection or the TAC team needs to collect additional data before device goes for auto reload.

When MBUF depletion is detected, a compressed troubleshooting file is created in the **disk0:/FaultMonitor/** directory. The filename uses the format *bdep-ts_YYYYMMDD_HHMMSS_TIMEZONE.log*. Older files are purged automatically, retaining only the latest ten compressed files.

When block depletion is detected on a control node in a cluster device, the control node leaves the cluster, force crashes, and reloads. One of the data nodes then becomes the new control node. After reloading, the node rejoins the cluster as a data node. If block depletion is detected on a data node, the data node leaves the cluster, force crashes, reloads, and rejoins the cluster as a data node.

In a high-availability setup, by default the MBUF is not monitored. However, if the configuration is modified on the active unit, the same is replicated on the standby unit. Thus, when MBUF depletion is detected on the device, the system moves the active device to a failed state to allow the standby device to take over. This switchover reduces downtime and packet loss. The failed peer sends logs for diagnostics. Use the show block to diagnose and debug the cause of block depletion.

Examples

To view the default mbuf-depletion configuration, use **show running-config all fault-monitor**:

```
ciscoasa# show running-config all fault-monitor
fault-monitor
   block-depletion
   block-depletion recovery-action reload
   block-depletion monitor-interval 60
   mbuf-depletion
   mbuf-depletion recovery-action reload
   mbuf-depletion monitor-interval 60
```

The following example illustrates disabling mbuf-depletion:

```
ciscoasa(config)# fault-monitor
ciscoasa(config-fault-monitor)#
ciscoasa(config-fault-monitor)# no mbuf-depletion
```

The following example illustrates modifying recovery action and monitoring interval for block-depletion:

```
ciscoasa# fault-monitor
ciscoasa(config-fault-monitor)# mbuf-depletion recovery-action ?
fault-monitor mode commands/options:
  none    No Recovery Action
  reload  Reload the device on mbuf depletion
ciscoasa(config-fault-monitor)# mbuf-depletion monitor-interval ?
fault-monitor mode commands/options:
  <30-300>  Duration in seconds to wait before recovery action
ciscoasa(config-fault-monitor)# mbuf-depletion monitor-interval 30
```

The following example illustrates the MBUF depletion status:

```
ciscoasa# show fault-monitor mbuf-depletion status
MBUF-Depletion: [ENABLED]
MBUF-Depletion Current State [2]: Monitoring State
Recovery action configured = [Reload]
MBUF-Depletion - monitor-interval [60] sec
```

The following example shows the output for **show fault-monitor mbuf-depletion status** during the 15-minute delayed start period:

```
MBUF-Depletion: [ENABLED]
MBUF-Depletion Current State [0]: SYS_NOT_READY
Monitoring will start after 12 mins
Recovery action configured = [Reload]
MBUF-Depletion - monitor-interval [60] sec
```

The following example shows the output for **show fault-monitor mbuf-depletion status** with the restart wait state after a depletion event and recovery:

```
MBUF-Depletion: [ENABLED]
MBUF-Depletion Current State [9]: WAIT_FOR_RESTART_MON
Monitoring will restart after pool recovers
MBUF class: 0, next check in 8 mins
Recovery action configured = [Reload]
MBUF-Depletion - monitor-interval [60] sec
FSM Restart Monitor Count: [1]
```



fe – fz

- feature, on page 1597
- fec, on page 1600
- file-bookmarks, on page 1602
- file-browsing, on page 1604
- file-encoding, on page 1606
- file-entry, on page 1608
- filter, on page 1610
- filter activex, on page 1612
- filter ftp, on page 1614
- filter https, on page 1616
- filter java, on page 1618
- filter url, on page 1620
- fips enable, on page 1624
- fips self-test poweron, on page 1626
- firewall transparent, on page 1627
- flow-export active refresh-interval, on page 1629
- flow-export delay flow-create, on page 1631
- flow-export destination, on page 1633
- flow-export event-type destination, on page 1635
- flow-export template timeout-rate, on page 1637
- flow-offload cluster-redirect, on page 1639
- flow-offload enable, on page 1640
- flow-offload-dtls, on page 1643
- flow-offload-dtls, on page 1645
- flow-offload-dtls egress-optimization, on page 1647
- flow-offload-ipsec, on page 1649
- flowcontrol, on page 1651
- flow-mobility lisp, on page 1654
- force re-authentication, on page 1656
- format, on page 1657
- forward interface, on page 1659
- forward-reference (Deprecated), on page 1661
- fqdn (crypto ca trustpoint), on page 1663

- fqdn (network object), on page 1665
- fragment, on page 1667
- frequency, on page 1670
- fsck, on page 1672
- ftp mode passive, on page 1674
- functions (Deprecated), on page 1675
- fxos mode appliance, on page 1677
- fxos permit, on page 1679
- fxos port, on page 1681

feature

To request smart licensing feature entitlements, use the **feature** command in license smart configuration mode. To remove the feature, use the **no** form of this command.



Note This command is supported on the ASA Virtual and chassis only.

feature { **tier standard** | **strong-encryption** | **context** *number* | **mobile-sp** | **carrier** }
no feature { **tier standard** | **strong-encryption** | **context** *number* | **mobile-sp** | **carrier** }

Syntax Description

carrier	Requests the Carrier (GTP/GPRS, Diameter, SCTP, M3UA) license. This license replaces the Mobile SP license.
context *number*	(Chassis only) Requests the Security Context license. Subtract the default number of contexts contained in the standard license. For example, if your model supports 250 contexts, and the default contexts is 2, then you should request 248 contexts maximum.
mobile-sp	(Firepower 9300/4100 only) Requests the Mobile SP (GTP/GPRS) license. This license was deprecated in favor of the Carrier license in Version 9.5(2).
strong-encryption	(Chassis only) Requests the Strong Encryption (3DES) license. With FXOS 1.1.3 and later, the Strong Encryption license is automatically enabled for qualified customers when you register the device. Only pre 2.3.0 Smart Software Manager satellite users need to use this command.
tier standard	The standard or essentials tier is the only option available. The Essentials license was formerly called the Standard license.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
License smart configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added.

Release	Modification
9.4(1.152)	Support for the Firepower 9300 ASA security modules, and the **strong-encryption**, **mobile-sp**, and **context** keywords was added.
9.5(2)	The **mobile-sp** keyword was replaced by the **carrier** keyword. The **strong-encryption** keyword was deprecated except for pre 2.3.0 Smart Software Manager satellite users.
9.6(1)	Support for the Firepower 4100 series was added.
9.8(2)	Support for the Firepower 2100 series was added.
9.18(1)	Support for the Secure Firewall 3100 was added, including for the carrier license.

Usage Guidelines

For the ASA Virtual, when you request the feature tier for the first time, you must exit license smart configuration mode for your changes to take effect. If you change the feature tier after you are authorized with the Cisco License Authority, you must reload the ASA Virtual for your changes to take effect.

Examples

The following example sets the ASA Virtual feature tier to standard, and the throughput level to 2G:

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

The following example requests 3 contexts on top of the default 2, for a total of 5:

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# feature context 3
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.

Command	Description
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

fec

To set Forward Error Correction (FEC) for 25 Gbps and higher interfaces, use the **fec** command in interface configuration mode. To restore the FEC setting to the default, use the **no** form of this command.



Note This command is only supported on the Secure Firewall 3100.

fec { **auto** | **cl108-rs** | **cl74-fc** | **disable** }
no fec { **auto** | **cl108-rs** | **cl74-fc** | **cl91-rs** | **disable** }

Syntax Description

auto	Auto-detects the FEC setting based on the SFP type.
cl108-rs	Sets the FEC mode to Clause 108 RS-FEC.
cl74-fc	Sets the FEC mode to Clause 74 FC-FEC.
cl91-rs	Sets the FEC mode to Clause 91 RS-FEC
disable	Disables FEC.

Command Default

The default setting is **auto**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.17(1)	This command was introduced for the Secure Firewall 3100.
9.18(3)/9.19(1)	Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers.
9.20(1)	Added support for cl91-rs for 100 GB interfaces.

Usage Guidelines

Set the FEC on the physical interface only. You need to set the FEC to EtherChannel member interfaces before you add them to the EtherChannel.

The setting chosen when you use **auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 9: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC	Network Module Default FEC
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate
25/50/100G	cl91-rs	cl91-rs

Examples

The following example sets the FEC to cl74-fc:

```
ciscoasa(config)# interface ethernet1/5
ciscoasa(config-if)# fec cl74-fc
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
duplex	Sets the duplex mode.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

file-bookmarks

To customize the File Bookmarks title or the File Bookmarks links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **file-bookmarks** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

file-bookmarks { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }
no file-bookmarks { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }

Syntax Description

link	Specifies a change to the links.
title	Specifies a change to the title.
style	Specifies a change to the HTML style.
text	Specifies a change to the text.
value	The actual text or CSS parameters to display (the maximum number is 256 characters).

Command Default

The default link style is color:#669999;border-bottom: 1px solid #669999;text-decoration:none.

The default title style is color:#669999;background-color:#99CCCC;font-weight:bold.

The default title text is “File Folder Bookmarks”.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid CSS parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the W3C website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma-separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.



Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the File Bookmarks title to "Corporate File Bookmarks":

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.

file-browsing

To enable or disable CIFS/FTP file browsing for file servers or shares, use the **file-browsing** command in dap webvpn configuration mode.

file-browsing enable | disable

Syntax Description

enable | disable	Enables or disables the ability to browse for file servers or shares.

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The following usage notes apply to file browsing:

- File browsing does not support internationalization.
- Browsing requires NBNS (Master Browser or WINS). If that fails or is not configured, use DNS.

The ASA can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the tunnel group
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or tunnel group.

When you enable or disable an attribute for a DAP record, the ASA applies that value and enforces it. For example, when you disable file browsing in dap webvpn configuration mode, the ASA looks no further for a

value. When you instead set no value for the **file-browsing** command, the attribute is not present in the DAP record, so the ASA moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable file browsing for the DAP record called Finance:

```
ciscoasa
 (config)# config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dap-webvpn)#
 file-browsing enable
ciscoasa
(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-entry	Enables or disables the ability to enter file server names to access.

file-encoding

To specify the character encoding for pages from Common Internet File System servers, use the **file-encoding** command in webvpn configuration mode. To remove the values of the file-encoding attribute use the **no** form of this command.

file-encoding { **server-name** | **server-ip-addr** } *charset*
no file-encoding { **server-name** | **server-ip-addr** }

Syntax Description

charset	String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets . You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850. The string is case-insensitive. The command interpreter converts upper case to lower case in the ASA configuration.
server-ip-addr	IP address, in dotted-decimal notation, of the CIFS server for which you want to specify character encoding.
server-name	Name of the CIFS server for which you want to specify character encoding. The ASA retains the case that you specify, although it ignores the case when matching the name to a server.

Command Default

Pages from all CIFS servers that do not have explicit file encoding entries in the WebVPN configuration inherit the character encoding value from the character encoding attribute.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Enter file encoding entries for all CIFS servers that require character encoding entries that differ from the value of the webvpn character encoding attribute.

The WebVPN portal pages downloaded from the CIFS server to the WebVPN user encode the value of the WebVPN file encoding attribute identifying the server, or if one does not, they inherit the value of the character encoding attribute. The remote user's browser maps this value to an entry in its character encoding set to determine the correct character set to use. The WebVPN portal pages do not specify a value if WebVPN

configuration does not specify a file encoding entry for the CIFS server and the character encoding attribute is not set. The remote browser uses its own default encoding if the WebVPN portal page does not specify the character encoding, or if it specifies a character encoding value that the browser does not support.

The mapping of CIFS servers to their appropriate character encoding, globally with the WebVPN character encoding attribute, and individually with file encoding overrides, provides for the accurate handling and display of CIFS pages when the correct rendering of file names or directory paths, as well as pages, are an issue.

Note The character encoding and file encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one of these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

Examples

The following example sets the file encoding attribute of the CIFS server named "CISCO-server-jp" to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding CISCO-server-jp shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

The following example sets the file encoding attribute of the CIFS server 10.86.5.174 to support IBM860 (alias "CP860") characters:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding 10.86.5.174 cp860
ciscoasa(config-webvpn)
```

Related Commands

Command	Description
character-encoding	Specifies the global character encoding used in all WebVPN portal pages except for pages from servers specified in file encoding entries in the WebVPN configuration.
show running-config webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.
debug webvpn cifs	Displays debugging messages about the Common Internet File System.

file-entry

To enable or disable the ability of a user to enter file server names to access, use the **file-entry** command in dap webvpn configuration mode.

file-entry enable | **disable**

Syntax Description

enable | **disable**	Enables or disables the ability to enter file server names to access.

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The ASA can apply attribute values from a variety of sources according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the Connection Profile (tunnel group)
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or Connection Profile.

When you enable or disable an attribute for a DAP record, the ASA applies that value and enforces it. For example, when you disable file entry in dap webvpn configuration mode, the ASA looks no further for a value. When you instead set no value for the **file-entry** command, the attribute is not present in the DAP record, so the ASA moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable file entry for the DAP record called Finance:

```
ciscoasa
 (config)#
config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dap-webvpn)#
 file-entry enable
ciscoasa
(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-browsing	Enables or disables the ability to browse for file servers or shares.

filter

To specify the name of the access list to use for WebVPN connections for this group policy or username, use the **filter** command in webvpn configuration mode. To remove the access list, use the **no** form of this command.

filter { **value** *ACLname* | **none** }
no filter

Syntax Description

none	Indicates that there is no WebVPN type access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *ACLname*	Provides the name of the previously configured access list.

Command Default

WebVPN access lists do not apply until you use the **filter** command to specify them.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **no** option allows inheritance of a value from another group policy. To prevent inheriting filter values, use the **filter value none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **filter** command to apply those ACLs for WebVPN traffic.

WebVPN does not use ACLs defined in the **vpn-filter** command.

Examples

The following example shows how to set a filter that invokes an access list named *acl_in* for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# filter acl_in
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn configuration mode to configure parameters that apply to group policies or usernames.

filter activex

To remove ActiveX objects in HTTP traffic passing through the ASA, use the filter activex command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter activex *port* [*-port*] | **except** *local_ip* **mask** *foreign_ip foreign_mask*
no filter activex *port* [*-port*] | **except** *local_ip* **mask** *foreign_ip foreign_mask*

Syntax Description

except	Creates an exception to a previous filter condition.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
foreign_mask	Network mask of the foreign_ip argument. Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_ip	The IP address of the highest security level interface from which access is requested. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
mask	Network mask of the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
port	The TCP port to which filtering is applied. Typically, this is port 21, but other values are accepted. The http or url literal can be used for port 21. The range of values permitted is 0 to 65535.
-port	(Optional) Specifies a port range.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

ActiveX objects may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can disable ActiveX objects with the filter **activex** command.

ActiveX controls, formerly known as OLE or OCX controls, are components that you can insert in a web page or other application. These controls include custom forms, calendars, or any of the extensive third-party forms for gathering or displaying information. As a technology, ActiveX creates many potential problems for network clients including causing workstations to fail, introducing network security problems, or being used to attack servers.

The filter **activex** command blocks the HTML **object** commands by commenting them out within the HTML web page. ActiveX filtering of HTML files is performed by selectively replacing the <applet> and </applet> and <object classid> and </object> tags with comments. Filtering of nested tags is supported by converting top-level tags to comments.



Caution The <object> tag is also used for Java applets, image files, and multimedia objects, which will also be blocked by this command.

If the <object> or </object> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the ASA cannot block the tag.

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command or for WebVPN traffic.

Examples

The following example specifies that ActiveX objects are blocked on all outbound connections:

```
ciscoasa(config)# filter activex 80 0 0 0 0
```

This command specifies that the ActiveX object blocking applies to web traffic on port 80 from any local host and for connections to any foreign host.

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
filter java	Removes Java applets from HTTP traffic passing through the ASA.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies anN2H2 or Websense server for use with the filter command.

filter ftp

To identify the FTP traffic to be filtered by a Websense or N2H2 server, use the filter **ftp** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter ftp *port* [*-port*] **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**interact-block**]
no filter ftp *port* [*-port*] **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**interact-block**]

Syntax Description

allow	(Optional) When the server is unavailable, let outbound connections pass through the ASA without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the ASA stops outbound port 80 (Web) traffic until the N2H2 or Websense server is back on line.
except	Creates an exception to a previous filter condition.
foreign_ip	The IP address of the lowest security level interface to which access is requested. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
foreign_mask	Network mask of the foreign_ip argument. Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
interact-block	(Optional) Prevents users from connecting to the FTP server through an interactive FTP program.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
mask	Network mask of the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
port	The TCP port to which filtering is applied. Typically, this is port 21, but other values are accepted. The ftp literal can be used for port 80.
-port	(Optional) Specifies a port range.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The filter ftp command lets you identify the FTP traffic to be filtered by a Websense or N2H2 server.

After enabling this feature, when a user issues an FTP GET request to a server, the ASA sends the request to the FTP server and to the Websense or N2H2 server at the same time. If the Websense or N2H2 server permits the connection, the ASA allows the successful FTP return code to reach the user unchanged. For example, a successful return code is “250: CWD command successful.”

If the Websense or N2H2 server denies the connection, the ASA alters the FTP return code to show that the connection was denied. For example, the ASA would change code 250 to “550 Requested file is prohibited by URL filtering policy.” Websense only filters FTP GET commands and not PUT commands.

Use the interactive-block option to prevent interactive FTP sessions that do not provide the entire directory path. An interactive FTP client allows the user to change directories without typing the entire path. For example, the user might enter cd ./files instead of cd /public/files. You must identify and enable the URL filtering server before using these commands.

Examples

The following example shows how to enable FTP filtering:

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter ftp 21 0 0 0 0
ciscoasa(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
filter https	Identifies the HTTPS traffic to be filtered by a Websense sor N2H2 erver.
filter java	Removes Java applets from HTTP traffic passing through the ASA.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

filter https

To identify the HTTPS traffic to be filtered by a N2H2 or Websense server, use the filter **https** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter https *port* [*-port*] | **except** *local_ip* **mask** *foreign_ip* [**allow**]
no filter https *port* [*-port*] | **except** *local_ip* **mask** *foreign_ip* [**allow**]

Syntax Description

allow	(Optional) When the server is unavailable, let outbound connections pass through the ASA without filtering. If you omit this option, and if the N2H2 or Websense server goes offline, the ASA stops outbound port 443 traffic until the N2H2 or Websense server is back online.
except	(Optional) Creates an exception to a previous filter condition.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
foreign_mask	Network mask of the foreign_ip argument. Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
mask	Network mask of the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
port	The TCP port to which filtering is applied. Typically, this is port 443, but other values are accepted. The https literal can be used for port 443.
-port	(Optional) Specifies a port range.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA supports filtering of HTTPS and FTP sites using an external Websense or N2H2 filtering server.

HTTPS filtering works by preventing the completion of SSL connection negotiation if the site is not allowed. The browser displays an error message such as “The Page or the content cannot be displayed.”

Because HTTPS content is encrypted, the ASA sends the URL lookup without directory and filename information.

Examples

The following example filters all outbound HTTPS connections except those from the 10.0.2.54 host:

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter https 443 0 0 0 0
ciscoasa(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the ASA.
filter java	Removes Java applets from HTTP traffic passing through the ASA.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

filter java

To remove Java applets from HTTP traffic passing through the ASA, use the filter **java** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter java { [*port* [- *port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]
no filter java { [*port* [- *port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

Syntax Description

except	(Optional) Creates an exception to a previous filter condition.
foreign_ip	The IP address of the lowest security level interface to which access is requested. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
foreign_mask	Network mask of the foreign_ip argument. Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_ip	The IP address of the highest security level interface from which access is requested. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_mask	Network mask of the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
port	The TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The http or url literal can be used for port 80.
port-port	(Optional) Specifies a port range.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Java applets may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can remove Java applets with the filter java command.

The **filter java** command filters out Java applets that return to the ASA from an outbound connection. The user still receives the HTML page, but the web page source for the applet is commented out so that the applet cannot execute. The **filter java** command does not filter WebVPN traffic.

If the <applet> or </applet> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the ASA cannot block the tag. If Java applets are known to be in <object> tags, use the **filter activex** command to remove them.

Examples

The following example specifies that Java applets are blocked on all outbound connections:

```
ciscoasa(config)# filter java 80 0 0 0 0
```

The following example specifies that the Java applet blocking applies to web traffic on port 80 from any local host and for connections to any foreign host.

The following example blocks the downloading of Java applets to a host on a protected network:

```
ciscoasa(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

Related Commands

filter activex	Removes ActiveX objects from HTTP traffic passing through the ASA.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

filter url

To direct traffic to a URL filtering server, use the filter **url** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter url *port* [- *port*] | **except** *local_ip local_mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]
no filter url *port* [- *port*] | **except** *local_ip local_mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

Syntax Description

allow	When the server is unavailable, let outbound connections pass through the ASA without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the ASA stops outbound port 80 (Web) traffic until the N2H2 or Websense server is back online.
cgi_truncate	When a URL has a parameter list starting with a question mark (?), such as a CGI script, truncate the URL sent to the filtering server by removing all characters after and including the question mark.
except	Creates an exception to a previous filter condition.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
foreign_mask	Network mask of the foreign_ip argument. Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
http	Specifies port 80. You can enter http or www instead of 80 to specify port 80.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_mask	Network mask of the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
longurl-deny	Denies the URL request if the URL is over the URL buffer size limit or the URL buffer is not available.
longurl-truncate	Sends only the originating hostname or IP address to the N2H2 or Websense server if the URL is over the URL buffer limit.
-port	(Optional) The TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The http or url literal can be used for port 80. Adding a second port after a hyphen optionally identifies a range of ports.
proxy-block	Prevents users from connecting to an HTTP proxy server.
url	Filter URLs from data moving through the ASA.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The filter url command lets you prevent outbound users from accessing World Wide Web URLs that you designate using the N2H2 or Websense filtering application.

Note The **url-server** command must be configured before issuing the **filter url** command.

The allow option of the filter **url** command determines how the ASA behaves if the N2H2 or Websense server goes off line. If you use the allow option with the filter **url** command and the N2H2 or Websense server goes offline, port 80 traffic passes through the ASA without filtering. If used without the allow option and with the server offline, the ASA stops outbound port 80 (Web) traffic until the server is back online, or if another URL server is available, passes control to the next URL server.

Note With the allow option set, the ASA passes control to an alternate server if the N2H2 or Websense server goes offline.

The N2H2 or Websense server works with the ASA to deny users from access to websites based on the company security policy.

Using the Filtering Server

Websense protocol Version 4 enables group and username authentication between a host and an ASA. The ASA performs a username lookup, and then Websense server handles URL filtering and username logging.

The N2H2 server must be a Windows workstation (2000, NT, or XP), running an IFP Server, with a recommended minimum of 512 MB of RAM. Also, the long URL support for the N2H2 service is capped at 3 KB, less than the cap for Websense.

Websense protocol Version 4 contains the following enhancements:

- URL filtering allows the ASA to check outgoing URL requests with the policy defined on the Websense server.
- Username logging tracks username, group, and domain name on the Websense server.

- Username lookup enables the ASA to use the user authentication table to map the host's IP address to the username.

Information on Websense is available at the following website:

http://www.websense.com/

Configuration Procedure

Follow these steps to filter URLs:

1. Designate an N2H2 or Websense server with the appropriate vendor-specific form of the url-server command.
2. Enable filtering with the filter command.
3. If needed, improve throughput with the url-cache command. However, this command does not update Websense logs, which may affect Websense accounting reports. Accumulate Websense run logs before using the url-cache command.
4. Use the show url-cache statistics and the show perfmon commands to view run information.

Working with Long URLs

Filtering URLs up to 4 KB is supported for the Websense filtering server, and up to 3 KB for the N2H2 filtering server.

Use the **longurl-truncate** and **cgi-truncate** options to allow handling of URL requests longer than the maximum permitted size.

If a URL is longer than the maximum, and you do not enable the longurl-truncate or longurl-deny options, the ASA drops the packet.

The longurl-truncate option causes the ASA to send only the hostname or IP address portion of the URL for evaluation to the filtering server when the URL is longer than the maximum length permitted. Use the longurl-deny option to deny outbound URL traffic if the URL is longer than the maximum permitted.

Use the cgi-truncate option to truncate CGI URLs to include only the CGI script location and the script name without any parameters. Many long HTTP requests are CGI requests. If the parameters list is very long, waiting and sending the complete CGI request including the parameter list can use up memory resources and affect ASA performance.

Buffering HTTP Responses

By default, when a user issues a request to connect to a specific website, the ASA sends the request to the web server and to the filtering server at the same time. If the filtering server does not respond before the web content server, the response from the web server is dropped. This delays the web server response from the point of view of the web client.

By enabling the HTTP response buffer, replies from web content servers are buffered and the responses will be forwarded to the requesting user if the filtering server allows the connection. This prevents the delay that may otherwise occur.

To enable the HTTP response buffer, enter the following command:

```
ciscoasa(config)# url-block block
 block-buffer-limit
```

Replace the *block-buffer-limit* argument with the maximum number of blocks that will be buffered. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks that can be buffered at one time.

Examples

The following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter url 80 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

The following example blocks all outbound HTTP connections destined to a proxy server that listens on port 8080:

```
ciscoasa(config)# filter url 8080 0 0 0 0 proxy-block
```

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the ASA.
filter java	Removes Java applets from HTTP traffic passing through the ASA.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

fips enable

To enable policy checking to enforce FIPS compliance on the system or module, use the fips enable command in global configuration mode. To disable policy checking, use the no form of this command.

fips enable
no fips enable

Syntax Description

enable	Enables or disables policy checking to enforce FIPS compliance.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• No	• Yes	• Yes	—

Command History

Release	Modification
7.0(4)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.8(2)	Enabling FIPS mode now requires you to save your configuration and reload. Also, both units in a failover pair require the same FIPS setting.

Usage Guidelines

To run in a FIPS-compliant mode of operation, you must apply both the fips enable command and the correct configuration specified in the security policy. The internal API allows the device to migrate toward enforcing correct configuration at run time.

When the FIPS-compliant mode is present in the startup configuration, FIPS POST will run and print the following console message:

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706
```

```
....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

Note FIPS mode is not supported in clustering mode.

Note If all interfaces are configured as members of port-channels, then the FIPS self-test will fail during boot. At least one interface must be enabled and not be configured as a member of a port-channel for the FIPS self-test to succeed during boot.

Examples

The following shows policy checking to enforce FIPS compliance on the system:

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot the
 device
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the ASA.
show fips	Displays the FIPS current operational state on the ASA.

fips self-test poweron

To execute power-on self-tests, use the fips self-test powereon command in privileged EXEC mode.

fips self-test poweron

Syntax Description

poweron	Executes power-on self-tests.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(4)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Entering this command causes the device to run all self-tests required for FIPS 140-2 compliance. Tests include the cryptographic algorithm test, software integrity test, and critical functions test.

Examples

The following example shows the system executing power-on of self-tests:

```
ciscoasa(config)# fips self-test poweron
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing, and configuration of crash write info to Flash.
fips enable	Enables or disables policy checking to enforce FIPS compliance on the system or module.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the ASA.

firewall transparent

To set the firewall mode to transparent mode, use the **firewall transparent** command in global configuration mode. To restore routed mode, use the **no** form of this command.

firewall transparent
no firewall transparent

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA is in routed mode.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes		—

Command History

Release	Modification
7.0(1)	This command was added.
8.5(1)/9.0(1)	You can set this per context in multiple context mode.

Usage Guidelines

A transparent firewall is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

You can set this command per context in multiple context mode.

When you change modes, the ASA clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

If you download a text configuration to the ASA that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the ASA changes the mode as soon as it reads the command and then continues reading the configuration you downloaded. If the command is later in the configuration, the ASA clears all the preceding lines in the configuration.

Examples

The following example changes the firewall mode to transparent:

```
ciscoasa(config)# firewall transparent
```

Related Commands

Command	Description
arp-inspection	Enables ARP inspection, which compares ARP packets to static ARP entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show firewall	Shows the firewall mode.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

flow-export active refresh-interval

To specify the time interval between flow-update events, use the **flow-export active refresh-interval** command in global configuration mode.

flow-export active refresh-interval *value*

Syntax Description

value Specifies the time interval between flow-update events in minutes. Valid values are from 1-60 minutes.

Command Default

The default value is 1 minute.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

If you have already configured the **flow-export delay flow-create** command, and you then configure the flow-export active refresh-interval command with an interval value that is not at least 5 seconds more than the delay value, the following warning message appears at the console:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
 appear before flow-creation events.
```

If you have already configured the flow-export active refresh-interval command, and you then configure the **flow-export delay flow-create** command with a delay value that is not at least 5 seconds less than the interval value, the following warning message appears at the console:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
 appear before flow-creation events.
```

Examples

The following example shows how to configure a time interval of 30 minutes:

```
ciscoasa(config)# flow-export active refresh-interval 30
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.

Commands	Description
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export delay flow-create

To delay export of the flow-create event, use the **flow-export delay flow-create** command in global configuration mode. To export the flow-create event without a delay, use the **no** form of this command.

flow-export delay flow-create *seconds*
no flow-export delay flow-create *seconds*

Syntax Description

seconds	Specifies the delay in seconds for exporting the flow-create event. Valid values are 1-180 seconds.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(2)	This command was added.

Usage Guidelines

If the flow-export delay flow-create command is not configured, the flow-create event is exported without a delay.

If the flow is torn down before the configured delay, the flow-create event is not sent; an extended flow teardown event is sent instead.

Examples

The following example shows how to delay the export of a flow-create event by ten seconds:

```
ciscoasa(config)# flow-export delay flow-create 10
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.

Commands	Description
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export destination

To configure a collector to which NetFlow packets are sent, use the **flow-export destination** command in global configuration mode. To remove a collector of NetFlow packets, use the **no** form of this command.

flow-export destination *interface-name ipv4-address | hostname udp-port*
no flow-export destination *interface-name ipv4-address | hostname udp-port*

Syntax Description

hostname	Specifies the hostname of the NetFlow collector.
interface-name	Specifies the name of the interface through which the destination can be reached.
ipv4-address	Specifies the IP address of the NetFlow collector. Only IPv4 is supported.
udp-port	Specifies the UDP port on which the NetFlow collector is listening. Valid values are 1-65535.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(1)	This command was added.
8.1(2)	The maximum number of flow export destinations was increased to five.

Usage Guidelines

You can use the flow-export destination command to configure the ASA to export NetFlow data to a NetFlow collector.

Note You can enter a maximum of five export destinations (collectors) per security context. When you enter a new destination, the template records are sent to the newly added collector. If you try to add more than five destinations, the following error message appears:“ERROR: A maximum of 5 flow-export destinations can be configured.”

If the ASA is configured to export NetFlow data, to improve performance, we recommend that you disable redundant syslog messages (those also captured by NetFlow) by entering the **logging flow-export-syslogs disable** command.

Examples

The following example shows how to configure a collector for NetFlow data:

```
ciscoasa(config)# flow-export destination inside 209.165.200.224 2055
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.
low-export delay flow-create	Delays the export of the flow-create event by a specified amount of time.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export event-type destination

To configure the address of NetFlow collectors and filters to determine which NetFlow records should be sent to each collector, use the **flow-export event-type destination** command in policy-map class configuration mode. To remove the address of NetFlow collectors and filters, use the **no** form of this command.

flow-export event-type { **all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown** } **destination**
no flow-export event-type { **all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown** } **destination**

Syntax Description

all	Specifies all four event types.
flow-create	Specifies flow-create events.
flow-denied	Specifies flow-denied events.
flow-teardown	Specifies flow-teardown events.
flow-update	Specifies flow-update events.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(2)	This command was added.

Usage Guidelines

NetFlow events are configured through Modular Policy Framework. If Modular Policy Framework is not configured for NetFlow, no events are logged. Traffic is matched based on the order in which classes are configured. After a match is detected, no other classes are checked. For NetFlow events, the configuration requirements are as follows:

- A flow-export destination (that is, a NetFlow collector) is uniquely identified by its IP address.
- Supported event types are flow-create, flow-teardown, flow-denied, flow-update, and all, which include the four previously listed event types.
- Flow-export actions are not supported in interface policies.
- Flow-export actions are only supported in the **class-default** command and in classes with the **match any** or **match access-list** command.

- If no NetFlow collector has been defined, no configuration actions occur.
- NetFlow Secure Event Logging filtering is order-independent.

Note To create a valid NetFlow configuration, you must have both the flow-export destination configuration and the flow-export event-type configuration. The flow-export destination configuration alone does nothing. You must also configure a class map for the flow-export event-type configuration. This can either be the default class map or one that you create.

Examples

The following example exports all NetFlow events between hosts 10.1.1.1 and 20.1.1.1 to the destination 15.1.1.1.

```
ciscoasa(config)# access-list
 flow_export_acl
 permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination
15.1.1.1
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.
flow-export delay flow-create	Delays the export of the flow-create event by a specified amount of time.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export template timeout-rate

To control the interval at which the template information is sent to NetFlow collectors, use the **flow-export template timeout-rate** command in global configuration mode. To reset the template timeout to the default value, use the **no** form of this command.

flow-export template timeout-rate *minutes*
no flow-export template timeout-rate *minutes*

Syntax Description

minutes	Specifies the interval in minutes. Valid values are 1-3600 minutes.
template	Enables the **timeout-rate** keyword for configuring export templates.
timeout-rate	Specifies the amount of time elapsed (interval) after the template is initially sent before it is resent.

Command Default

The default value for the interval is 30 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(1)	This command was added.

Usage Guidelines

You should configure the timeout rate based on the collector being used and at what rate the collectors expect the templates to be refreshed.

If the security appliance is configured to export NetFlow data, to improve performance, we recommend that you disable redundant syslog messages (those also captured by NetFlow) by entering the **logging flow-export-syslogs disable** command.

Examples

The following example shows how to configure NetFlow to send template records to all collectors every 60 minutes:

```
ciscoasa(config)# flow-export template timeout-rate 60
```

Related Commands

Commands	Description
clear flow-export counters	Resets all the runtime counters associated with NetFlow data.
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-offload cluster-redirect

To enable cluster redirect on the Secure Firewall 4200, use the **flow-offload cluster-redirect** command in global configuration mode. To disable cluster redirect, use the **no** form of this command.

flow-offload cluster-redirect
no flow-offload cluster-redirect

Syntax Description

This command has no arguments or keywords.

Command Default

Cluster redirect is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.23(1)	This command was introduced for the Secure Firewall 4200.

Usage Guidelines

For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance.

The **flow-offload enable** command must be enabled for this command to work. **flow-offload enable** is also enabled by default.

Examples

The following example disables cluster redirect.

```
ciscoasa(config)# no flow-offload cluster-redirect
```

Related Commands

Command	Description
flow-offload enable	Enables flow offload.
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.
show flow-offload	Displays information about flow off-loading.

flow-offload enable

To enable flow off-loading, use the **flow-offload enable** command in global configuration mode. To disable the off-loading, use the **no** form of this command.

flow-offloadenable
no flow-offload enable

Syntax Description

This command has no arguments or keywords.

Command Default

Flow off-loading is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2.1)	This command was introduced. It is available for the Firepower 9300 series running FXOS 1.1.3+ only.
9.6(1)	Support was added for the Firepower 4100 series running FXOS 1.1.4+.
9.6(2)	Support was added for multicast connections in transparent mode, but only for bridge groups that contain two and only two interfaces.
9.15(1)	A reload is only required at initial enabling for the Firepower 4100/9300.
9.17(1)	Support was added for the Secure Firewall 3100.
9.20(1)	Support was added for the Secure Firewall 4200.
9.23(1)	Flow offload is enabled by default for the Secure Firewall 3100/4200.

Usage Guidelines

If you deploy a appliance with an ASA security module in a data center, you can identify select traffic to be off-loaded to a super fast path, where the flows are switched in the NIC itself. Off-loading can help you improve performance for data-intensive applications such as large file transfers.

Before being off-loaded, the ASA first applies normal security processing, such as access rules and inspection, during connection establishment. The ASA also does session tear-down. But once a connection is established, if it is eligible to be off-loaded, further processing happens in the NIC rather than the ASA.

While offloaded, the flow does not receive security policy checking or other services, so that it can move through the system as fast as possible. For off-loaded flows, there is no inspection, TCP normalization (except for checksum verification, if you configure it), QoS, or sequence number checking.

To identify flows that can be off-loaded, you create a service policy rule that applies the flow off-loading service. A matching flow is then off-loaded if it meets the following conditions:

- IPv4 addresses only.
- TCP, UDP, GRE only.
- Standard or 802.1q tagged Ethernet frames only.
- (Transparent mode only.) Multicast flows for bridge groups that contain two and only two interfaces.
- It is not receiving services that cannot be applied to off-loaded flows, such as inspection, decryption, IPSec and VPN flows, or flows directed to a service module.

Reverse flows for off-loaded flows are also off-loaded.

In multiple-context mode, enabling or disabling flow offload enables or disables it for all contexts. You cannot have different settings per context.

Prior to 9.15(1) on the Firepower 4100/9300, you must reload the system whenever you enable or disable flow offload. Starting with version 9.15(1), a reload is only required the first time you enable flow offload. Reloading is not required for the Secure Firewall 3100/4200. When a reload is required, there are special considerations for changing the mode for clusters or failover pairs if you want a hitless change:

- Clustering—First enter the command on the control node, but do not reboot the control node immediately. Instead, reboot each node of the cluster first, then return to the control node and reboot it. You can then configure the offloading service policy on the control node.
- Failover—First enter the command on the active unit, but do not reboot it immediately. Instead, reboot the standby unit, then reboot the active unit. You can then configure the offloading service policy on the active unit.

Note For more specific information on device support, see http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/compatibility/fxos-compatibility.html .

Examples

The following example enables flow off-loading, saves the configuration, and reboots the system.

```
ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.
ciscoasa(config)# write memory

ciscoasa(config)# reload
```

Related Commands

Command	Description
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.

Command	Description
show flow-offload	Displays information about flow off-loading.

flow-offload-dtls

To enable DTLS crypto acceleration on the device, use the **flow-offload-dtls** command in global configuration mode. To disable this feature, use the **no** form of this command.

flow-offload-dtls

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.22(1)	The command was introduced.

Usage Guidelines

The Cisco Secure Firewall 4200 and 3100 series devices, with the help of the FPGA and the Nitrox V crypto accelerator, support DTLS cryptographic acceleration. This feature improves the throughput of the DTLS encrypted and decrypted traffic. Both IPv4 and IPv6 traffic is supported. This feature works only for DTLS 1.2.

Supported Devices

- Cisco Secure Firewall 4200 Series: 4215, 4225, 4245
- Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140

Supported Network Processing Unit FPGA Firmware Versions

- Cisco Secure Firewall 4200 Series: 1024.11.00
- Cisco Secure Firewall 3100 Series:
  - 3100 Low SKU: 1792.4.00
  - 3100 High SKU: 1792.3.00

If you upgrade your devices to Version 9.22(1) and later, the firmware is automatically upgraded.

To view the Network Processing Unit (NPU) FPGA firmware of the device, use the **show version detail | inc Fpga** command:

```
device# show version detail | inc Fpga
Fpga-Vers: 0.21.00
Fpga-Golden-Vers: 0.21.00
```

```
NpuFpga-Vers: 1792.4.00
TamFpga-Vers: 2.6.d
Epm-Fpga-Version: UNKNOWN
```

Example

The following example enables DTLS crypto acceleration on the device.

```
ciscoasa# flow-offload-dtls
```

Related Commands

Command	Description
flow-offload-dtls egress-optimization	Enables optimization of egress encrypted packets and improve latency.
show flow-offload-dtls info	Displays IPsec flow offload information.
show flow-offload-dtls statistics	Displays IPsec flow offload statistics.

flow-offload-dtls

To enable DTLS crypto acceleration on the device, use the **flow-offload-dtls** command in global configuration mode. To disable this feature, use the **no** form of this command.

flow-offload-dtls

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.22(1)	The command was introduced.

Usage Guidelines

The Cisco Secure Firewall 4200 and 3100 series devices, with the help of the FPGA and the Nitrox V crypto accelerator, support DTLS cryptographic acceleration. This feature improves the throughput of the DTLS encrypted and decrypted traffic. Both IPv4 and IPv6 traffic is supported. This feature works only for DTLS 1.2.

Supported Devices

- Cisco Secure Firewall 4200 Series: 4215, 4225, 4245
- Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140

Supported Network Processing Unit FPGA Firmware Versions

- Cisco Secure Firewall 4200 Series: 1024.11.00
- Cisco Secure Firewall 3100 Series:
  - 3100 Low SKU: 1792.4.00
  - 3100 High SKU: 1792.3.00

If you upgrade your devices to Version 9.22(1) and later, the firmware is automatically upgraded.

To view the Network Processing Unit (NPU) FPGA firmware of the device, use the **show version detail | inc Fpga** command:

```
device# show version detail | inc Fpga
Fpga-Vers: 0.21.00
Fpga-Golden-Vers: 0.21.00
```

```
NpuFpga-Vers: 1792.4.00
TamFpga-Vers: 2.6.d
Epm-Fpga-Version: UNKNOWN
```

Example

The following example enables DTLS crypto acceleration on the device.

```
ciscoasa# flow-offload-dtls
```

Related Commands

Command	Description
flow-offload-dtls egress-optimization	Enables optimization of egress encrypted packets and improve latency.
show flow-offload-dtls info	Displays IPsec flow offload information.
show flow-offload-dtls statistics	Displays IPsec flow offload statistics.

flow-offload-dtls egress-optimization

To enable optimization of egress encrypted packets and improve latency, use the **flow-offload-dtls egress-optimization** command in global configuration mode. To disable this feature, use the **no** form of this command.

flow-offload-dtls egress-optimization

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.22(1)	The command was introduced.

Usage Guidelines

This feature works only for DTLS 1.2. The hardware performs optimization of the egress encrypted packets to improve latency. The data path is optimized to enhance performance for single tunnel flows. Both IPv4 and IPv6 traffic is supported.

Supported Devices

- Cisco Secure Firewall 4200 Series: 4215, 4225, 4245
- Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140

Supported Network Processing Unit FPGA Firmware Versions

- Cisco Secure Firewall 4200 Series: 1024.11.00
- Cisco Secure Firewall 3100 Series:
  - 3100 Low SKU: 1792.4.00
  - 3100 High SKU: 1792.3.00

If you upgrade your devices to Version 9.22(1) and later, the firmware is automatically upgraded.

To view the Network Processing Unit (NPU) FPGA firmware of the device, use the **show version detail | inc Fpga** command:

```
device# show version detail | inc Fpga
Fpga-Vers: 0.21.00
Fpga-Golden-Vers: 0.21.00
```

```
NpuFpga-Vers: 1792.4.00
TamFpga-Vers: 2.6.d
Epm-Fpga-Version: UNKNOWN
```

Example

The following example enables optimization of egress encrypted packets and improves latency.

```
ciscoasa# flow-offload-dtls egress-optimization
```

Related Commands

Command	Description
flow-offload-dtls	Enables DTLS crypto acceleration on the device.
show flow-offload-dtls info	Displays IPsec flow offload information.
show flow-offload-dtls statistics	Displays IPsec flow offload statistics.

flow-offload-ipsec

To enable IPsec flow off-loading, use the **flow-offload-ipsec** command in global configuration mode. To disable the off-loading, use the **no** form of this command.

flow-offload-ipsec [**egress-optimization**]
no flow-offload-ipsec [**egress-optimization**]

Syntax Description

egress-optimization	(Optional.) Optimize the data path to enhance performance for single tunnel flows.

Command Default

IPsec flow offload is enabled on default platforms that support it, but egress optimization is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	The command was introduced for the Secure Firewall 3100.
9.20(1)	Support was added for the Secure Firewall 4200.
9.22(1)	Support was added for the Secure Firewall 1200.
9.23(1)	Support was added for IPsec flow offload for traffic on the cluster control link on the Secure Firewall 4200 in distributed site-to-site VPN mode.

Usage Guidelines

You can configure supporting device models to use IPsec flow offload. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. On the Secure Firewall 1200 series, IPsec connections are offloaded to the Marvell Cryptographic Accelerator (CPT) to improve device performance.On the Secure Firewall 6100 series, IPsec connections are offloaded to the Kintex 7 (KC400) FPGA. This FPGA contains a built-in crypto engine that is capable of handling AES-GCM-128 and AES-GCM-256 encryption and decryption.

Offloaded operations specifically relate to the pre-decryption and decryption processing on ingress, and the pre-encryption and encryption processing on egress. The system software handles the inner flow to apply your security policies.

IPsec flow offload is enabled by default, and applies to the following device types:

- Secure Firewall 1200

- Secure Firewall 3100
- Secure Firewall 4200
- Secure Firewall 6100

IPsec flow offload is also used when the device's VTI loopback interface is enabled.

For asymmetric flows in cluster distributed site-to-site VPN mode, IPsec flow offload now lets the flow owner decrypt IPsec traffic in hardware that was forwarded over the cluster control link. This feature is not configurable and is always available with IPsec flow offload.

The following IPsec flows are not offloaded:

- KEv1 tunnels. Only IKEv2 tunnels will be offloaded. IKEv2 supports stronger ciphers.
- Flows that have volume-based rekeying configured.
- Flows that have compression configured.
- Transport mode flows. Only tunnel mode flows will be offloaded.
- AH format. Only ESP/NAT-T format will be supported.
- Flows that have post-fragmentation configured.
- Flows that have anti-replay window size other than 64bit and anti-replay is not disabled.
- Flows that have firewall filter enabled.
- Multiple context mode.
- Secure Firewall 6100 supports AES-GCM-128 and AES-GCM-256 ciphers only. IPsec tunnels that are configured with other ciphers are not offloaded. Any IPsec packets that are not offloaded are processed by the software engine in the CPU.

Example

The following example enables both IPsec flow offload and egress optimization.

```
ciscoasa# flow-offload-ipsec
ciscoasa# flow-offload-ipsec egress-optimization
```

Related Commands

Command	Description
clear flow-offload-ipsec	Clears IPsec flow offload statistics.
show flow-offload-ipsec	Displays IPsec flow offload statistics and information.

flowcontrol

To enable pause (XOFF) frames for flow control, use the **flowcontrol** command in interface configuration mode. To disable pause frames, use the **no** form of this command.

Secure Firewall 3100:

flowcontrol send on
no flowcontrol send on

ASA Hardware:

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]
no flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

Syntax Description

high_water	Sets the high-water mark between 0 and 511 KB for 10 GigabitEthernet, and between 0 and 47 KB for 1 GigabitEthernet (or 0 and 11 KB for GigabitEthernet interfaces on the 4GE-SSM). When the buffer usage exceeds the high-water mark, the NIC sends a pause frame.
low_water	Sets the low-water mark between 0 and 511 KB for 10 GigabitEthernet, and between 0 and 47 KB for 1 GigabitEthernet (or 0 and 11 KB for GigabitEthernet interfaces on the 4GE-SSM). After the network interface controller (NIC) sends a pause frame, when the buffer usage is reduced below the low-water mark, the NIC sends an XON frame. The link partner can resume traffic after receiving an XON frame.
noconfirm	Applies the command without confirmation. Because this command resets the interface, without this option, you are asked to confirm the configuration change.
pause_time	Sets the pause refresh threshold value, between 0 and 65535 slots. Each slot is the amount of time to transmit 64 bytes, so the time per unit depends on your link speed. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by this timer value in the pause frame. If the buffer usage is consistently above the high watermark, pause frames are sent repeatedly, controlled by the pause refresh threshold value. The default is 26624.

Command Default

Pause frames are disabled by default.

For the Secure Firewall 3100, see the following values (not configurable):

- The global high watermark is 2 MB (8000 buffers).
- The global low watermark is 1.25 MB (5000 buffers).
- The port high watermark is .3125 MB (1250 buffers).
- The port low watermark is .25 MB (1000 buffers).

For ASA hardware 10 GigabitEthernet, see the following default settings:

- The default high watermark is 128 KB.
- The default low watermark is 64 KB.
- The default pause refresh threshold value is 26624 slots.

For For ASA hardware 1 GigabitEthernet, see the following default settings:

- The default high watermark is 24 KB.
- The default low watermark is 16 KB.
- The default pause refresh threshold value is 26624 slots.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(2)	This command was added for 10-GigabitEthernet interfaces on the ASA 5580.
8.2(3)	Added support for the ASA 5585-X.
8.2(5)/8.4(2)	Added support for 1-GigabitEthernet interfaces on all models.
9.18(1)	Added support for the Secure Firewall 3100.

Usage Guidelines

This command is supported on 1-GigabitEthernet and higher interfaces. This command does not support management interfaces.

Enter this command for a physical interface.

Note Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Secure Firewall 3100

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If the ASA port experiences congestion (exhaustion of queuing resources on the internal switch) and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Note The ASA supports transmitting pause frames so that the remote peer can rate-control the traffic.

However, receiving of pause frames is not supported.

The internal switch has a global pool of 8000 buffers of 250 bytes each, and the switch allocates buffers dynamically to each port. A pause frame is sent out every interface with flowcontrol enabled when the buffer usage exceeds the global high-water mark (2 MB (8000 buffers)); and a pause frame is sent out of a particular interface when its buffer exceeds the port high-water mark (.3125 MB (1250 buffers)). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark (1.25 MB globally (5000 buffers); .25 MB per port (1000 buffers)). The link partner can resume traffic after receiving an XON frame.

ASA Hardware

If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue.

When you enable this command, pause (XOFF) and XON frames are generated automatically by the NIC hardware based on the FIFO buffer usage:

1. The NIC sends a pause frame when the buffer usage exceeds the high watermark.
2. After a pause is sent, the NIC sends an XON frame when the buffer usage is reduced below the low watermark.
3. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by the timer value in the pause frame.
4. If the buffer usage is consistently above the high watermark, the NIC sends pause frames repeatedly, controlled by the pause refresh threshold value.

When you use this command on ASA models, the following warning message appears:

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

To change the parameters without being prompted, use the **noconfirm** keyword.

Examples

The following example enables pause frames using the default settings:

```
ciscoasa(config)# interface tengigabitethernet 1/0
ciscoasa(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
ciscoasa(config-if)# y
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

flow-mobility lisp

To enable flow mobility for the cluster, use the **flow-mobility lisp** command in cluster configuration mode. To disable flow mobility, use the **no** form of this command.

flow-mobility lisp
no flow-mobility lisp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.
3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.

4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following example enables flow mobility for cluster1:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# flow-mobility lisp
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the preshared key to validate LISP messages.

force re-authentication

To allow an identity provider to authenticate directly rather than rely on a previous security context when a SAML authentication request occurs, use the force re-authentication command in saml idp webvpn configuration mode. To disable this setting, use the no form of this command.

force re-authentication

Command Default

By default, this setting is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn	• Yes	• Yes	• Yes	• Yes	—

Usage Guidelines

ASA must have the SAML configuration. This command is necessary when you require direct re-authentication with the IdP.

Example

The following example shows this command:

```
ciscoasa(config-webvpn-saml-idp)# force re-authentication
```

Related Commands

Command	Description
saml idp	Adds a new SAML IdP.

format

To erase all files and format the file system, use the **format** command in privileged EXEC mode.

format { **disk0:** | **disk1:** | **flash:** }

Syntax Description

disk0:	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **format** command erases all data on the specified file system and then rewrites the FAT information to the device.

Caution Use the **format** command with extreme caution, only when necessary, to clean up corrupted flash memory.

To delete all visible files (excluding hidden system files), enter the **delete /recursive** command, instead of the **format** command.

Note On the ASA 5500 series, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information. To repair a corrupt file system, try entering the **fsck** command before entering the **format** command.

Examples

This example shows how to format the flash memory:

```
ciscoasa# format flash:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the flash memory.
fsck	Repairs a corrupt file system.

forward interface

For models with a built-in switch, such as the ASA 5505, use the **forward interface** command in interface configuration mode to restore connectivity for one VLAN from initiating contact to one other VLAN. To restrict one VLAN from initiating contact to one other VLAN, use the **no** form of this command.

forward interface vlan *number*
no forward interface vlan *number*

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

vlan *number*	Specifies the VLAN ID to which this VLAN interface cannot initiate traffic.

Command Default

By default, all interfaces can initiate traffic to all other interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

You might need to restrict one VLAN depending on how many VLANs your license supports.

In routed mode, you can configure up to three active VLANs with the ASA 5505 Base license, and up to five active VLANs with the Security Plus license. An active VLAN is a VLAN with a **nameif** command configured. You can configure up to five inactive VLANs on the ASA 5505 for either license, but if you make them active, be sure to follow the guidelines for your license.

With the Base license, the third VLAN must be configured with the **no forward interface** command to restrict this VLAN from initiating contact to one other VLAN.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside work network, and a third VLAN assigned to your home network. The home network does not need to access

the work network, so you can use the **no forward interface** command on the home VLAN; the work network can access the home network, but the home network cannot access the work network.

If you already have two VLAN interfaces configured with a **nameif** command, be sure to enter the **no forward interface** command before the **nameif** command on the third interface; the ASA does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505.

Examples

The following example configures three VLAN interfaces. The third home interface cannot forward traffic to the work interface.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
...
```

Related Commands

Command	Description
backup interface	Assigns an interface to be a backup link to an ISP, for example.
clear interface	Clears counters for the **show interface** command.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
switchport	Sets an interface to switch port mode.
switchport access vlan	Assigns a switch port to a VLAN.

forward-reference (Deprecated)

To make it possible to refer to ACLs and objects that do not yet exist, use the **forward-reference** command in global configuration mode.

forward-reference enable
no forward-reference enable

Syntax Description

enable	Enables forward referencing of ACLs (in access groups) and objects (in objects and ACLs).

Command Default

(Pre-9.18) The default is that forward-referencing is disabled. An ACL or object must exist to be able to refer to it in an access list rule, another object, or an access group.

Starting with 9.18, this command is enabled by default, and you can no longer configure it. Forward referencing is always enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.
9.18(1)	This command was removed. The default was changed to enabled at all times. You cannot change this behavior.

Usage Guidelines

This command is most useful when used in conjunction with the **configure session** command, which creates isolated sessions for editing ACLs and their objects. For example, within a session, you could delete an ACL that is currently referenced by an **access-group** command, and create a new ACL with the same name. After committing the session, the new version of the ACL is compiled, and after compilation, becomes the active version of the access group.

Similarly, you can delete and recreate objects that are used by active access rules.

Forward referencing is designed for access rule ACL usage. You cannot delete an object currently used by other features, such as NAT or VPN.

Enable forward referencing with caution. The default behavior ensures that you do not make simple typos when configuring objects, access lists, and access groups. With forward referencing, the ASA cannot tell the difference between a typo and an intentional reference to something you intend to create in the future.

Any rule, access group, or object that points to a non-existent object or ACL is ignored during operation. It does not become operational until you create the missing item.

Examples

The following example enables forward referencing:

```
ciscoasa(config)# forward-reference enable
```

Related Commands

Command	Description
access-group	Assigns an ACL to an interface or globally.
access-list	Creates ACL rules.
configure session	Creates or opens a session.
object	Creates an object.
object-group	Creates an object group.

fqdn (crypto ca trustpoint)

To include the indicated FQDN in the Subject Alternative Name extension of the certificate during enrollment, use the **fqdn** command in crypto ca trustpoint configuration mode. To restore the default setting of the FQDN, use the **no** form of the command.

fqdn [*fqdn* | **none**]
no fqdn

Syntax Description

fqdn	Specifies the FQDN. The maximum length is 64 characters.
none	Specifies no fully qualified domain name.

Command Default

The default setting does not include the FQDN.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you are configuring the ASA to support authentication of a Nokia VPN Client using certificates, use the **none** keyword. See the **crypto isakmp identity** or **isakmp identity** command for more information about supporting certificate authentication of the Nokia VPN Client.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and includes the FQDN engineering in the enrollment request for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# fqdn engineering
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

Command	Description
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut-and-paste enrollment with this trustpoint.

fqdn (network object)

To configure a FQDN for a network object, use the **fqdn** command in object configuration mode. To remove the object from the configuration, use the **no** form of this command.

fqdn [**v4** | **v6**] *fqdn*
no fqdn [**v4** | **v6**] *fqdn*

Syntax Description

fqdn	Specifies the FQDN, including the host and domain. The FQDN must begin and end with a digit or letter. Only letters, digits, and hyphens are allowed as internal characters. Labels are separated by a dot (for example, www.cisco.com).
v4	(Optional) Specifies an IPv4 domain name.
v6	(Optional) Specifies an IPv6 domain name.

Command Default

By default, the domain name is an IPv4 domain.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

If you configure an existing network object with a different value, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a network object:

```
ciscoasa (config)# object network FQDN_1
ciscoasa (config-network-object)# fqdn example.cisco.com
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.

Command	Description
fqdn	Specifies a fully qualified domain name network object.
host	Specifies a host network object.
nat	Enables NAT for the network object.
object network	Creates a network object.
object-group network	Creates a network object group.
range	Specifies a range of addresses for the network object.
show running-config object network	Shows the network object configuration.
subnet	Specifies a subnet network object.

fragment

To provide additional management of packet fragmentation and improve compatibility with NFS, use the fragment command in global configuration mode. To return to the default values, use the **no** form of this command.

fragment reassembly { **full** | **virtual** } { **size** | **chain** | **timeout** *limit* } [*interface*]
no fragment reassembly { **full** | **virtual** } { **size** | **chain** | **timeout** *limit* } [*interface*]

Syntax Description

chain limit	Specifies the maximum number of fragments into which a full IP packet can be fragmented.
interface	(Optional) Specifies the ASA interface. If an interface is not specified, the command applies to all interfaces.
reassembly full | **virtual**	Specifies the full or virtual reassembly for IP fragments that are routed through the ASA. IP fragments that terminate at the ASA are always fully reassembled.
size limit	Sets the maximum number of fragments that can be in the IP reassembly database waiting for reassembly. **Note** The ASA does not accept any fragments that are not part of an existing fabric chain after the queue size reaches 2/3 full. The remaining 1/3 of the queue is used to accept fragments where the source/destination IP addresses and IP identification number are the same as an incomplete fragment chain that is already partially queued. This limit is a DoS protection mechanism to help legitimate fragment chains be reassembled when there is a fragment flooding attack.
timeout limit	Specifies the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.

Command Default

The defaults are as follows:

- **chain** is 24 packets.
- *interface* is all interfaces.
- **size** is 200.
- **timeout** is 5 seconds.
- Virtual reassembly is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified so that you now must choose one of the following keywords: **chain**, **size**, or **timeout**. You can no longer enter the **fragment** command without entering one of these keywords, as was supported in prior releases of the software.
8.0(4)	The **reassembly full** | **virtual** option was added.

Usage Guidelines

By default, the ASA accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, you should consider configuring the ASA to prevent fragmented packets from traversing the ASA by entering the **fragment chain 1***interface* command on each interface. Setting the limit to 1 means that all packets must be whole; that is, unfragmented.

If a large percentage of the network traffic through the ASA is NFS, additional tuning might be necessary to avoid database overflow.

In an environment where the MTU size is small between the NFS server and client, such as a WAN interface, the chain keyword might require additional tuning. In this case, we recommend using NFS over TCP to improve efficiency.

Setting the size limit to a large value can make the ASA more vulnerable to a DoS attack by fragment flooding. Do not set the **size** limit equal to or greater than the total number of blocks in the 1550 or 16384 pool.

The default values will limit DoS attacks caused by fragment flooding.

The following processes are performed regardless of the **reassembly** option setting:

- IP fragments are collected until a fragment set is formed or until a timeout interval has elapsed (see the **timeout** option).
- If a fragment set is formed, integrity checks are performed on the set. These checks include no overlapping, no tail overflow, and no chain overflow (see the **chain** option).

If the **fragment reassembly virtual** command is configured, the fragment set is forwarded to the transport layer for further processing.

If the **fragment reassembly full** command is configured, the fragment set is first coalesced into a single IP packet. The single IP packet is then forwarded to the transport layer for further processing.

Examples

The following example shows how to prevent fragmented packets on the outside and inside interfaces:

```
ciscoasa(config)# fragment chain 1 outside
ciscoasa(config)# fragment chain 1 inside
```

Continue entering the fragment chain 1 interface command for each additional interface on which you want to prevent fragmented packets.

The following example shows how to configure the fragment database on the outside interface to a maximum size of 2000, a maximum chain length of 45, and a wait time of 10 seconds:

```
ciscoasa(config)# fragment size 2000 outside
ciscoasa(config)# fragment chain 45 outside
ciscoasa(config)# fragment timeout 10 outside
```

The following example displays output from the **show fragment** command that includes the **reassembly virtual** option:

```
ciscoasa(config)# show fragment
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

Related Commands

Command	Description
clear configure fragment	Resets all the IP fragment reassembly configurations to defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

frequency

To set the rate at which the selected SLA operation repeats, use the **frequency** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

frequency*seconds*
no frequency

Syntax Description

seconds	The number of seconds between SLA probes. Valid values are from 1 to 604800 seconds. This value cannot be less than the **timeout** value.

Command Default

The default frequency is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
SLA monitor protocol configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

An SLA operation repeats at a given frequency for the lifetime of the operation. For example:

- An **ipIcmpEcho** operation with a frequency of 60 seconds repeats by sending the echo request packets once every 60 seconds for the lifetime of the operation.
- The default number of packets in an echo operation is 1. This packet is sent when the operation is started and is then sent again 60 seconds later.

If an individual SLA operation takes longer to execute than the specified frequency value, a statistics counter called “busy” is increased rather than immediately repeating the operation.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 3 seconds, and the timeout value is set to 1000 milliseconds.

```
ciscoasa(config)# sla monitor 123
```

```
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.
timeout	Defines the amount of time that the SLA operation waits for a response.

fsck

To perform a file system check and to repair corruptions, use the **fsck** command in privileged EXEC mode.

fsck [**/noconfirm**] { **disk0:** | **disk1:** \ | **flash:** }

Syntax Description

/noconfirm	(Optional) Does not prompt for confirmation to repair.
disk0:	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. The **flash** keyword is aliased to **disk0:**.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **fsck** command checks and tries to repair corrupt file systems. Use this command before trying more permanent procedures.

If the FSCK utility fixes an instance of disk corruption (due to a power failure or abnormal shutdown, for example), it creates recovery files named FSCK*xxx* .REC. These files can contain a fraction of a file or a whole file that was recovered while FSCK was running. In rare circumstances, you might need to inspect these files to recover data; generally, these files are not needed, and can be safely deleted.

Note The FSCK utility runs automatically at startup, so you may see these recovery files even if you did not manually enter the **fsck** command.

Examples

The following example shows how to check the file system of the flash memory:

```
ciscoasa# fsck disk0:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the flash memory.
format	Erases all files on a file system, including hidden system files, and reinstalls the file system.

ftp mode passive

To set the FTP mode to passive, use the ftp mode passive command in global configuration mode. To set the FTP client to active mode, use the **no** form of this command.

ftp mode passive
no ftp mode passive

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **ftp mode passive** command sets the FTP mode to passive, which is the default. The ASA can use FTP to upload or download image files or configuration files to or from an FTP server. The **ftp mode passive** command controls how the FTP client on the ASA interacts with the FTP server.

In passive FTP, the client initiates both the control connection and the data connection. Passive mode refers to the server state, in that the server is passively accepting both the control connection and the data connection, which are initiated by the client.

In passive mode, both destination and source ports are ephemeral ports (greater than 1023). The mode is set by the client, as the client issues the **passive** command to initiate the setup of the passive data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

Examples

The following example disables passive mode:

```
ciscoasa(config)# no ftp mode passive
```

Related Commands

copy	Uploads or downloads image files or configuration files to or from an FTP server.
debug ftp client	Displays detailed information about FTP client activity.
show running-config ftp mode	Displays FTP client configuration.

functions (Deprecated)

Note The last supported release for this command was Version 8.0(1).

You cannot use the **functions** command for Release 8.0(2). It is deprecated and remains in this command reference only for reasons of backward compatibility. Use the **import** and **export** commands to create URL lists for websites, file access, and plug-ins, customization, and language translations.

To configure automatic downloading of the port forwarding Java applet, Citrix support, file access, file browsing, file server entry, application of a webtype ACL, HTTP proxy, port forwarding, or URL entry over WebVPN for this user or group policy, use the **functions** command in webvpn configuration mode. To remove a configured function, use the **no** form of this command.

functions { **auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none** }
no functions { **auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none** }

Syntax Description

auto-download	Enables or disables automatic download of the port forwarding Java applet after WebVPN login. You must first enable port forwarding, Outlook/Exchange proxy, or HTTP proxy.
citrix	Enables or disables support for terminal services from a MetaFrame Application Server to the remote user. This keyword lets the ASA act as a secure gateway within a secure Citrix configuration. These services provide users with access to MetaFrame applications through a standard Web browser.
file-access	Enables or disables file access. When enabled, the WebVPN home page lists file servers in the server list. You must enable file access to enable file browsing and/or file entry.
file-browsing	Enables or disables browsing for file servers and shares. You must enable file browsing to allow user entry of a file server.
file-entry	Enables or disables user ability to enter names of file servers.
filter	Applies a webtype ACL. When enabled, the ASA applies the webtype ACL defined with the WebVPN **filter** command.
http-proxy	Enables or disables the forwarding of an HTTP applet proxy to the remote user. The proxy is useful for technologies that interfere with proper mangling, such as Java, ActiveX, and flash. It bypasses mangling while ensuring the continued use of the ASA. The forwarded proxy modifies the browser's old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer.
none	Sets a null value for all WebVPN functions. Prevents inheriting functions from a default or specified group policy.

port-forward	Enables port forwarding. When enabled, the ASA uses the port forwarding list defined with the WebVPN **port-forward** command.
url-entry	Enables or disables user entry of URLs. When enabled, the ASA still restricts URLs with any configured URL or network ACLs. When URL entry is disabled, the ASA restricts WebVPN users to the URLs on the home page.

Command Default

Functions are disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The **auto-download** and **citrix** keywords were added.
8.0(2)	This command was deprecated.

Usage Guidelines

To remove all configured functions, including a null value created by issuing the **functions none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting function values, use the **functions none** command.

Examples

The following example shows how to configure file access and file browsing for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# functions file-access file-browsing
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.

fxos mode appliance

To set the Firepower 2100 to Appliance mode, use the **fxos mode appliance** command in global configuration mode. To set the mode to Platform mode, use the **no** form of this command.

fxos mode appliance
no fxos mode appliance

Note This command is supported on the Firepower 2100 only.

Syntax Description

This command has no arguments or keywords.

Command Default

The mode is set to Appliance mode by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

The Firepower 2100 runs an underlying operating system called the FXOS. You can run the Firepower 2100 in the following modes:

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.
- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Firewall Chassis Manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI.

When you change the mode, the configuration is cleared and you need to save the current configuration and reload the system. The default configuration is applied upon reload. Prior to reloading, you can set the mode back to the original value without any disruption. Note that the **clear configure all** and **configure factory-default** commands do not clear the current mode.

Use the **show fxos mode** to view the current mode.

Examples

The following example sets the mode to Platform mode:

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684
23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Related Commands

Command	Description
connect fxos	Connects to the FXOS CLI.
show fxos mode	Shows the current mode, Appliance or Platform.

fxos permit

To use FXOS SSH, HTTPS, or SNMP on the Firepower 2100 from an ASA data interface, use the **fxos permit** command in global configuration mode. To disable access, use the **no** form of this command.

fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* } *interface_name*
no fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* } *interface_name*

Syntax Description

https	Allows HTTPS access for the Firewall Chassis Manager. The default port is 3443.
interface_name	Specifies the ASA data interface where access is allowed. You cannot specify a management-only interface.
ipv4_address netmask	Specifies the IPv4 address and subnet mask.
ipv6_address/prefix_length	Specifies the IPv6 prefix and prefix length.
snmp	Allows SNMP access to FXOS. The default port is 3061. For SNMP traffic originating on the device, you must also set the **ip-client** command.
ssh	Allows SSH access to FXOS. The default port is 3022.

Command Default

See the following defaults:

- HTTPS default port—3443
- SNMP default port—3061
- SSH default port—3022

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.8(2)	We added this command.

Usage Guidelines

If you want to manage FXOS on the Firepower 2100 from a data interface, you can configure SSH, HTTPS, and SNMP access. This feature is useful if you want to manage the device remotely, and you want to keep

Management 1/1 on an isolated network. You can continue to use Management 1/1 for local access; you cannot allow remote access from Management 1/1 for FXOS at the same time as forwarding traffic to the ASA data interfaces because you can only specify one gateway. By default, the FXOS management gateway is the internal path to the ASA.

The ASA uses non-standard ports for FXOS access; the standard port is reserved for use by the ASA on the same interface. Use the **fxos port** command to change the port value. When the ASA forwards traffic to FXOS, it translates the non-standard destination port to the FXOS port for each protocol (do not change the HTTPS port in FXOS). The packet destination IP address (which is the ASA interface IP address) is also translated to an internal address for use by FXOS. The source address remains unchanged. For returning traffic, the ASA uses its data routing table to determine the correct egress interface. When you access the ASA data IP address for the management application, you must log in using an FXOS username; ASA usernames only apply for ASA management access.

You can also enable FXOS management traffic initiation on ASA data interfaces using the **ip-client** command, which is required for SNMP traps, or NTP and DNS server access, for example.

In the FXOS configuration, you must configure an access list (**ip-block** command) to allow your management addresses. You need to allow any addresses that you specified in the **fxos permit** commands. Also, make sure the default gateway is set to 0.0.0.0, which sets the ASA as the gateway. See the FXOS **set out-of-band** command.



Note You cannot use a VPN tunnel to an ASA data interface and access FXOS directly. As a workaround for SSH, you can VPN to the ASA, access the ASA CLI, and then use the **connect fxos** command to access the FXOS CLI. Note that SSH, HTTPS, and SNMPv3 are/can be encrypted, so direct connection to the data interface is safe.

Examples

The following example enables SSH and HTTPS access on the inside interface for the 192.168.1.0/24 and 2001:DB8::34/64 networks:

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

Related Commands

Command	Description
connect fxos	From the ASA CLI, connects to the FXOS CLI.
fxos port	Sets the FXOS management access port.
ip-client	Allows FXOS management traffic to egress the ASA data interface.

fxos port

To set the SSH, HTTPS, or SNMP port when accessing FXOS on a Firepower 2100 ASA data interface, use the **fxos port** command in global configuration mode. To use the default port, use the **no** form of this command.

fxos { **https** | **ssh** | **snmp** } **port** *port*
no fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* }

Syntax Description

https	Sets the port for HTTPS access for FXOS. The default port is 3443.
port	Specifies the port number.
snmp	Sets the port for SNMP access for FXOS. The default port is 3061.
ssh	Sets the port for SSH access for FXOS. The default port is 3022.

Command Default

See the following defaults:

- HTTPS default port—3443
- SNMP default port—3061
- SSH default port—3022

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.8(2)	We added this command.

Usage Guidelines

When you use the **fxos permit** command to allow FXOS access on a Firepower 2100 data interface, you can set the port to use for each application. The ASA uses non-standard ports for FXOS access; the standard port is reserved for use by the ASA on the same interface. When the ASA forwards traffic to FXOS, it translates the non-standard destination port to the FXOS port for each protocol (do not change the HTTPS port in FXOS).

Examples

The following example sets the ports for SSH and HTTPS access:

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

Related Commands

Command	Description
connect fxos	From the ASA CLI, connects to the FXOS CLI.
fxos permit	Allows FXOS management access on ASA data interfaces.
ip-client	Allows FXOS management traffic to egress the ASA data interface.



g – h

- gateway, on page 1685
- gateway-fqdn, on page 1687
- graceful-restart, on page 1689
- graceful-restart helper, on page 1691
- group, on page 1693
- group-alias, on page 1695
- group-delimiter, on page 1697
- group-lock, on page 1698
- group-object, on page 1699
- group-policy, on page 1701
- group-policy attributes, on page 1704
- group-prompt, on page 1707
- group-search-timeout, on page 1709
- group-url, on page 1710
- gsn-limit, on page 1712
- gtp-u-header-check, on page 1713
- h245-tunnel-block, on page 1715
- hardware-bypass, on page 1716
- hardware-bypass boot-delay, on page 1718
- hardware-bypass manual, on page 1720
- health-check, on page 1722
- health-check application, on page 1724
- health-check auto-rejoin, on page 1727
- health-check chassis-heartbeat-delay-rejoin, on page 1730
- health-check monitor-interface, on page 1732
- hello-interval, on page 1735
- hello padding multi-point, on page 1736
- help, on page 1740
- hidden-parameter, on page 1742
- hidden-shares, on page 1744
- hold-time, on page 1746
- homepage, on page 1748
- homepage use-smart-tunnel, on page 1750

- host (network object), on page 1752
- host (parameters), on page 1753
- hostname, on page 1755
- hostname dynamic, on page 1756
- hostscan enable, on page 1760
- hostscan image, on page 1762
- hpm topn enable, on page 1764
- hsi, on page 1765
- hsi-group, on page 1766
- hsts enable, on page 1767
- hsts max-age, on page 1769
- html-content-filter, on page 1771
- http (global), on page 1773
- http[s] (parameters), on page 1775
- http authentication-certificate, on page 1777
- http-comp, on page 1779
- http connection idle-timeout, on page 1780
- http-only-cookie, on page 1782
- http-only-cookie, on page 1784
- http-proxy (call-home), on page 1786
- http-proxy (dap), on page 1788
- http-proxy (webvpn), on page 1790
- http redirect, on page 1793
- http server basic-auth-client, on page 1795
- http server enable, on page 1797
- http server idle-timeout, on page 1798
- http server session-timeout, on page 1800
- https-proxy, on page 1802
- http username-from-certificate, on page 1804
- hw-module module allow-ip, on page 1807
- hw-module module ip, on page 1808
- hw-module module password-reset, on page 1810
- hw-module module recover, on page 1812
- hw-module module recover (ASA 5506W-X), on page 1815
- hw-module module reload, on page 1816
- hw-module module reset, on page 1818
- hw-module module shutdown, on page 1820

gateway

To specify which group of call agents are managing a particular gateway, use the **gateway** command in mgcp map configuration mode. To remove the configuration, use the **no** form of this command.

gateway *ip_address* [*group_id*]

Syntax Description

gateway	The group of call agents that are managing a particular gateway.
group_id	The ID of the call agent group, from 0 to 2147483647.
ip_address	The IP address of the gateway.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Mgcp map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **gateway** command to specify which group of call agents are managing a particular gateway. The IP address of the gateway is specified with the >*ip_address* option. The >*group_id* option is a number from 0 to 4294967295 that must correspond with the >*group_id* of the call agents that are managing the gateway. A gateway may only belong to one group.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debugging information for MGCP.
mgcp-map	Defines an MGCP map and enables mgcp map configuration mode.
show mgcp	Displays MGCP configuration and session information.

gateway-fqdn

To configure the FQDN of the ASA. use the **gateway-fqdn** command. To remove the configuration, use the **no** form of this command.

gateway-fqdn value { **FQDN_Name** | **none** }
no gateway-fqdn

Syntax Description

fqdn-name	Defines the ASA FQDN to push down to the Secure Client.
none	Defines the FQDN as null value where the FQDN is not specified. The global FQDN configured using hostname and domain-name commands will be used if available.

Command Default

The default FQDN name is not set in the default group policy. New group policies are set to inherit this value.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If you have configured Load Balancing between your ASAs, specify the FQDN of the ASA in order to resolve the ASA IP address used for re-establishing the VPN session. This setting is critical to support client roaming between networks of different IP protocols (such as IPv4 to IPv6).

You cannot use the ASA FQDN present in the Secure Client profile to derive the ASA IP address after roaming. The addresses may not match the correct device (the one the tunnel was established to) in the load balancing scenario.

If the ASA's FQDN is not pushed to the client, the client will try to reconnect to whatever IP address the tunnel had previously established. In order to support roaming between networks of different IP protocols (from IPv4 to IPv6), Secure Client must perform name resolution of the device FQDN after roaming, so that it can determine which ASA address to use for re-establishing the tunnel. The client uses the ASA FQDN present in its profile during the initial connection. During subsequent session reconnects, it always uses the device FQDN pushed by ASA (and configured by the administrator in the group policy), when available. If the FQDN is not configured, the ASA derives the device FQDN (and sends it to the client) from whatever is set under Device Setup > Device Name/Password and Domain Name in ASDM.

If the device FQDN is not pushed by the ASA, the client cannot reestablish the VPN session after roaming between networks of different IP protocols.

Usage Guidelines

Examples

The following example defines the FQDN of the ASA as ASAName.example.cisco.com

```
ciscoasa(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
ciscoasa(config-group-policy)#
```

The following example removes the FQDN of the ASA from the group policy. The group policy then inherits this value from the Default Group Policy.

```
ciscoasa(config-group-policy)# no gateway-fqdn
ciscoasa(config-group-policy)#
```

The following example defines the FQDN as having no value. The global FQDN configurd using ciscoasa and domain-name commands will be used if available.

```
ciscoasa(config-group-policy)# gateway-fqdn none
ciscoasa(config-group-policy)#
```

graceful-restart

To configure graceful restart for OSPFv3 on a NSF capable ASA, use the graceful-restart command under router configuration mode. Optionally, configure the graceful restart interval with the restart-interval option. Use the no form of the command to disable graceful-restart.

graceful-restart [**restart-interval** *seconds*]
no graceful-restart

Syntax Description

restart-interval seconds	(Optional) Specifies the length of the graceful restart interval, in seconds. The range is from 1 to 1800. The default is 120. **Note** For a restart interval below 30 seconds, graceful restart will be terminated.

Command Default

OSPFv3 graceful restart is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration mode	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.3(1)	This command was introduced.

Usage Guidelines

Use the graceful-restart command to allow OSPFv3 to remain in the data forwarding path through a process restart.

Note Set the restart interval to be long enough to allow a typical reboot cycle for ASA. Do not set the restart-interval too long to avoid the network relying on old route information.

Examples

The following example enables OSPFv3 graceful-restart:

```
ciscoasa
(config)# ipv6 router ospf 1
ciscoasa
(config-router)# graceful-restart restart-interval 180
```

Related Commands

Command	Description
graceful-restart helper	Enables OSPFv3 graceful restart on NSF-aware ASA.

graceful-restart helper

To configure graceful restart for OSPFv3 on a NSF aware ASA, use the graceful-restartUse the no form of the command to disable graceful-restart helper mode.

graceful-restart helper [**strict-lsa-checking**]
no graceful-restart helper

Syntax Description

strict-lsa-checking	(Optional) Enables strict link-state advertisement (LSA) checking for helper mode.

Command Default

OSPFv3 graceful restart helper mode is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was introduced.

Usage Guidelines

When an ASA has NSF enabled, it is said to be NSF-capable and will operate in graceful restart mode--the OSPF process performs nonstop forwarding recovery due to a Route Processor (RP) switchover. By default, the neighboring ASAs of the NSF-capable ASA will be NSF-aware and will operate in NSF helper mode. When the NSF-capable ASA is performing graceful restart, the helper ASAs assist in the nonstop forwarding recovery process. If you do not want the ASA to help the restarting neighbor with nonstop forwarding recovery, enter the no nsf ietf helper command.

To enable strict LSA checking on both NSF-aware and NSF-capable ASAs, enter the graceful-restart helper strict-lsa-checking command. However, strict LSA checking will not become effective until the ASA becomes a helper ASA during a graceful restart process. With strict LSA checking enabled, the helper ASA will terminate the helping process of the restarting ASA if it detects that there is a change to an LSA that would be flooded to the restarting ASA or if there is a changed LSA on the retransmission list of the restarting ASA when the graceful restart process is initiated.

Examples

The following example enables graceful-restart helper with strict LSA checking:

```
ciscoasa
(config)# ipv6 router ospf 1
ciscoasa
(config-router)# graceful-restart helper strict-lsa-checking
```

Related Commands

Command	Description
graceful-restart	Enables OSPFv3 graceful restart on NSF-capable ASA.

group

To specify the Diffie-Hellman group in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the group command in ikev2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

group { **1** | **2** | **5** | **14** | **19** | **20** | **21** | **24** }
no group { **1** | **2** | **5** | **14** | **19** | **20** | **21** | **24** }

Syntax Description

1	Specifies the 768-bit Diffie-Hellman group 1 (not supported in FIPS mode).
2	Specifies the 1024-bit Diffie-Hellman group 2.
5	Specifies the 1536-bit Diffie-Hellman group 5.
14	Chooses ECDH group as the IKEv2 DH key exchange group.
19	Chooses ECDH groups as the IKEv2 DH key exchange group.
20	Chooses ECDH groups as the IKEv2 DH key exchange group.
21	Chooses ECDH groups as the IKEv2 DH key exchange group.
24	Chooses ECDH groups as the IKEv2 DH key exchange group.

Command Default

The default Diffie-Hellman group is group 14.

Usage Guidelines

An IKEv2 SA is a key used in Phase 1 to enable IKEv2 peers to communicate securely in Phase 2. After entering the crypto ikev2 policy command, you can use the group command to set the SA Diffie-Hellman group. The ASA and the Secure Client use the group identifier to derive a shared secret without transmitting it to each other. The lower the Diffie-Hellman group number, the less CPU time it requires to execute. The higher the Diffie-Hellman group number, the greater the security.

When the Secure Client is operating in non-FIPS mode, the ASA supports Diffie-Hellman groups 1, 2 and 5. In FIPS mode, it supports groups 2 and 5. Therefore, if you configure the ASA to use only group 1, the Secure Client in FIPS mode will fail to connect.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ikev2 policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	The ability to choose an ECDH group as the IKEv2 DH key exchange group was added.
9.13.(1)	The default DH group is **group 14.** The command options **group 2**, **group 5** and **group 24** was deprecated and will be removed in the later release.

Examples

The following example enters ikev2 policy configuration mode and sets the Diffie-Hellman group to group 5:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 5
ciscoasa(config-ikev2-policy) group 2(Deprecated)
ciscoasa(config-ikev2-policy) group 5(Deprecated)
ciscoasa(config-ikev2-policy) group 24(Deprecated)
ciscoasa(config-ikev2-policy) group 14
```

Related Commands

Command	Description
encryption	Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections.
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
lifetime	Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections.
prf	Specifies the pseudo-random function in an IKEv2 SA for AnyConnect IPsec connections.

group-alias

To create one or more alternate names by which the user can refer to a tunnel group, use the **group-alias** command in tunnel-group webvpn configuration mode. To remove an alias from the list, use the **no** form of this command.

group-alias name [**enable** | **disable**]
no group-alias *name*

Syntax Description

disable	Disables the group alias.
enable	Enables a previously disabled group alias.
name	Specifies the name of a tunnel group alias. This can be any string you choose, except that the string cannot contain spaces.

Command Default

There is no default group alias, but if you do specify a group alias, that alias is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The group alias that you specify appears in the drop-down list on the login page. Each group can have multiple aliases or no alias. This command is useful when the same group is known by several common names, such as “Devtest” and “QA”.

Examples

The following example shows the commands for configuring the tunnel group named “devtest” and establishing the aliases “QA” and “Fra-QA” for the group:

```
ciscoasa(config)# tunnel-group devtest type webvpn
ciscoasa(config)# tunnel-group devtest webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias QA
ciscoasa(config-tunnel-webvpn)# group-alias Fra-QA
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel group database or the named tunnel group configuration.
show webvpn group-alias	Displays the aliases for the specified tunnel group or for all tunnel groups.
tunnel-group webvpn-attributes	Enters the tunnel-group webvpn configuration mode for configuring WebVPN tunnel group attributes.

group-delimiter

To enable group name parsing and specify the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated, use the **group-delimiter** command in global configuration mode. To disable this group name parsing, use the **no** form of this command.

group-delimiter*delimiter*
no group-delimiter

Syntax Description

delimiter	Specifies the character to use as the group name delimiter. Valid values are: **@**, **#**, and **!**.

Command Default

By default, no delimiter is specified, disabling group-name parsing.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The delimiter is used to parse tunnel group names from user names when tunnels are negotiated. By default, no delimiter is specified, disabling group name parsing.

Examples

This example shows the **group-delimiter** command to change the group delimiter to the hash mark (#):

```
ciscoasa(config)# group-delimiter #
```

Related Commands

Command	Description
clear configure group-delimiter	Clears the configured group delimiter.
show running-config group-delimiter	Displays the current group delimiter value.
strip-group	Enables or disables strip group processing.

group-lock

To restrict remote users to access through the tunnel group only, issue the **group-lock** command in group-policy configuration mode or username configuration mode. To remove the **group-lock** attribute from the running configuration, use the **no** form of this command.

group-lock { **value** *tunnel-grp-name* | **none** }
no group-lock

Syntax Description

none	Sets group-lock to a null value, thereby allowing no group lock restriction. Prevents inheriting a group lock value from a default or specified group policy.
value *tunnel-grp-name*	Specifies the name of an existing tunnel group that the ASA requires for the user to connect.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Usage Guidelines

To disable group lock, use the **group-lock none** command. The **no group-lock** command allows inheritance of a value from another group policy.

Group lock restricts users by checking if the group configured in the VPN client is the same as the tunnel group to which the user is assigned. If it is not, the ASA prevents the user from connecting. If you do not configure group lock, the ASA authenticates users without regard to the assigned group.

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to set group lock for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# group-lock value tunnel group name
```

group-object

To add group objects to object groups, use the**group-object** command while configuring the object. To remove group objects, use the **no** form of this command.

group-object*obj_grp_name*
no group-object *obj_grp_name*

Syntax Description

obj_grp_name	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Protocol, network, service, icmp-type, security group, and user object-group configuration modes	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	Support for adding object groups in the object-group user configuration mode for use with the Identity Firewall feature was added.

Usage Guidelines

The **group-object** command is used with the **object-group** command to add an object that itself is an object group. This sub-command allows logical grouping of the same type of objects and construction of hierarchical object groups for structured configuration.

Duplicate objects are allowed in an object group if they are group objects. For example, if object 1 is in both group A and group B, it is allowed to define a group C which includes both A and B. It is not allowed, however, to include a group object which causes the group hierarchy to become circular. For example, it is not allowed to have group A include group B and then also have group B include group A.

The maximum allowed levels of a hierarchical object group is 10.

Note The ASA does not support IPv6 nested network object groups, so you cannot group an object with IPv6 entries under another IPv6 object group.

Examples

The following example shows how to use the **group-object** command to eliminate the need to duplicate hosts:

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network)# network-object host 192.168.1.1
ciscoasa(config-network)# network-object host 192.168.1.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network)# network-object host 172.23.56.1
ciscoasa(config-network)# network-object host 172.23.56.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network)# group-object host_grp_1
ciscoasa(config-network)# group-object host_grp_2
ciscoasa(config-network)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)# access-list all permit tcp object-group all-hosts any eq w
```

The following example shows how to use the **group-object** command to add a local user group to a user group object:

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

group-policy *name* { **internal** [**from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password* }
no group-policy *name*

Syntax Description

external server-group *server_group*	Specifies the group policy as external and identifies the AAA server group for the ASA to query for attributes.
from *group-policy_name*	Initializes the attributes of this internal group policy to the values of a preexisting group policy.
internal	Identifies the group policy as internal.
name	Specifies the name of the group policy. The name can be up to 64 characters long and can contain spaces. Group names with spaces must be enclosed in double quotes, for example, “Sales Group”.
password *server_password*	Provides the password to use when retrieving attributes from the external AAA server group. The password can be up to 128 characters long and cannot contain spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0.1	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A default group policy, named “DefaultGroupPolicy,” always exists on the ASA. However, this default group policy does not take effect unless you configure the ASA to use it. For configuration instructions, see the CLI configuration guide.

Use the **group-policy attributes** command to enter group-policy configuration mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
backup-servers	keep-client-config
banner	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none

Attribute	Default Value
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

In addition, you can configure webvpn configuration mode attributes for the group policy, either by entering the **webvpn** command in group policy configuration mode or by entering the **group-policy attributes** command and then entering the **webvpn** command in group-webvpn configuration mode. See the description of the **group-policy attributes** command for details.

Examples

The following example shows how to create an internal group policy with the name "FirstGroup":

```
ciscoasa
(config)#
 group-policy FirstGroup internal
```

The following example shows how to create an external group policy with the name "ExternalGroup," the AAA server group "BostonAAA," and the password "12345678":

```
ciscoasa
(config)#
 group-policy ExternalGroup external server-group BostonAAA password 12345678
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy attributes	Enters group-policy configuration mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn configuration mode to configure WebVPN attributes for the group.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn	Enters webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

group-policy attributes

To enter the group-policy configuration mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, user the **no** form of this command.

group-policy*name***attributes**
no group-policy *name* **attributes**

Syntax Description

name	Specifies the name of the group policy.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

In group-policy configuration mode, you can configure Attribute-Value Pairs for a specified group policy or enter group-policy webvpn configuration mode to configure WebVPN attributes for the group.

The syntax of the commands in attributes mode have the following characteristics in common:

- The **no** form removes the attribute from the running configuration, and enables inheritance of a value from another group policy.
- The **none** keyword sets the attribute in the running configuration to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

A default group policy, named DefaultGroupPolicy, always exists on the ASA. However, this default group policy does not take effect unless you configure the ASA to use it. For configuration instructions, see the CLI configuration guide.

The **group-policy attributes** command enters group-policy configuration mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
backup-servers	keep-client-config

Attribute	Default Value
banner	none
client-access-rule	none
client-bypass-protocol	disable
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN

Attribute	Default Value
wins-server	none

In addition, you can configure webvpn-mode attributes for the group policy, by entering the **group-policy attributes** command and then entering the **webvpn** command in group-policy configuration mode. See the description of the **webvpn** command (group-policy attributes and username attributes modes) for details.

Examples

The following example shows how to enter group-policy attributes mode for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy	Creates, edits, or removes a group policy.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn	Enters group-webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

group-prompt

To customize the group prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the ASA, use the **group-prompt** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

group-prompt { **text** | **style** } *value*
group-prompt { **text** | **style** } *value*

Syntax Description

text	Specifies a change to the text.
style	Specifies a change the style.
value	The actual text to display or Cascading Style Sheet (CSS) parameters (the maximum number is 256 characters).

Command Default

The default text of the group prompt is "GROUP:".

The default style of the group prompt is color:black;font-weight:bold;text-align:right.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid CSS parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma-separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.



Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the text is changed to "Corporate Group:", and the default style is changed with the font weight increased to bolder:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# group-prompt text Corporate Group:
ciscoasa(config-webvpn-custom)# group-prompt style font-weight:bolder
```

Related Commands

Command	Description
password-prompt	Customizes the password prompt of the WebVPN page.
username-prompt	Customizes the username prompt of the WebVPN page.

group-search-timeout

To specify the maximum time to wait for a response from an Active Directory server queried using the show ad-groups command, use the **group-search-timeout** command in aaa-server host configuration mode. To remove the command from the configuration, use the **no** form of the command:

group-search-timeout*seconds*
no group-search-timeout *seconds*

Syntax Description

seconds	The time to wait for a response from the Active Directory server, from 1 to 300 seconds.

Command Default

The default is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command is added.

Usage Guidelines

The **show ad-groups** command applies only to Active Directory servers using LDAP, and displays groups that are listed on an Active Directory server. Use the **group-search-timeout** command to adjust the time to wait for a response from the server.

Examples

The following example sets the timeout to 20 seconds:

```
ciscoasa(config-aaa-server-host)#group-search-timeout 20
```

Related Commands

Command	Description
ldap-group-base-dn	Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.
show ad-groups	Displays groups that are listed on an Active Directory server.

group-url

To specify incoming URLs or IP addresses for the group, use the **group-url** command in tunnel-group webvpn configuration mode. To remove a URL from the list, use the **no** form of this command.

group-url *url* [**enable** | **disable**]
no group-url *url*

Syntax Description

disable	Disables the URL, but does not remove it from the list.
enable	Enables the URL.
url	Specifies a URL or IP address for this tunnel group.

Command Default

There is no default URL or IP address, but if you do specify a URL or IP address, it is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Specifying a group URL or IP address eliminates the need for the user to select a group at login. When a user logs in, the ASA looks for the user's incoming URL/address in the tunnel group policy table. If it finds the URL/address and if this command is enabled in the tunnel group, then the ASA automatically selects the associated tunnel group and presents the user with only the username and password fields in the login window. This simplifies the user interface and has the added advantage of never exposing the list of groups to the user. The login window that the user sees uses the customizations configured for that tunnel group.

If the URL/address is disabled and the **group-alias** command is configured, then the drop-down list of groups is also displayed, and the user must make a selection.

You can configure multiple URLs/addresses (or none) for a group. Each URL/address can be enabled or disabled individually. You must use a separate **group-url** command for each URL/address specified. You must specify the entire URL/address, including either the HTTP or HTTPS protocol.

You cannot associate the same URL/address with multiple groups. The ASA verifies the uniqueness of the URL/address before accepting it for a tunnel group.

Examples

The following example shows the commands for configuring the WebVPN tunnel group named "test" and establishing two group URLs, "http://www.cisco.com" and "https://supplier.example.com" for the group:

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com
ciscoasa(config-tunnel-webvpn)# group-url https://supplier.example.com
ciscoasa(config-tunnel-webvpn)#
```

The following example enables the group URLs http://www.cisco.com and http://192.168.10.10 for the tunnel group named RadiusServer:

```
ciscoasa(config)# tunnel-group RadiusServer type webvpn
ciscoasa(config)# tunnel-group RadiusServer general-attributes
ciscoasa(config-tunnel-general)# authentication server-group RADIUS
ciscoasa(config-tunnel-general)# accounting-server-group RADIUS
ciscoasa(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com
enable
ciscoasa(config-tunnel-webvpn)# group-url http://192.168.10.10
enable
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel group database or the named tunnel group configuration.
show webvpn group-url	Displays the URLs for the specified tunnel group or for all tunnel groups.
tunnel-group webvpn-attributes	Enters the webvpn configuration mode for configuring WebVPN tunnel group attributes.

gsn-limit

To specify the maximum number of GPRS support node (GSN) endpoints tracked by the GPRS Tunneling Protocol (GTP) inspection engine, use the **gsn-limit** command. Use the **no** form of the command to remove the limit on the number of GSN endpoints tracked by the GTP inspection engine.

gsn-limit [*limit*]
no gsn-limit [*limit*]

Command Default

By default, the **gsn-limit** command specifies the maximum number of GSN endpoints tracked by the GTP inspection engine to 10,000.

Command History

Release	Modification
9.20	This command was introduced.

Usage Guidelines

If you do not want to use the default value, you can specify a value between 1 and 4294967295 for the *limit* parameter.

Examples

The following example shows how to set the maximum number of GPRS support node (GSN) endpoints tracked by the GTP inspection engine to 50,000:

```
>policy-map type inspect gtp <policy-map-name>
  >parameters
    >gsn-limit 50000
```

Related Commands

Command	Description
policy-map type inspect	When using the Modular Policy Framework, define special actions for inspection of application traffic by using this command.

gtp-u-header-check

To check whether the inner payload of a GTP data packet is a valid IP packet and drop it if it is not, use the **gtp-u-header-check** command in GTP inspection policy map parameters configuration mode. Use the **no** form of this command disable the check.

gtp-u-header-check [**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**] | **gtp-in-gtp-encapsulation**]
no gtp-u-header-check [**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**] | **gtp-in-gtp-encapsulation**]

Syntax Description

anti-spoofing	Checks whether the mobile user IP address in the IP header of the inner payload matches the IP address assigned in GTP control messages such as Create Session Response, and drops the GTP-U message if the IP addresses do not match. This check supports IPv4, IPv6, and IPv4v6 PDN Types. If the mobile station gets its address using DHCP, the end-user IP address in GTPv2 is 0.0.0.0 (IPv4) or *prefix*::0 (IPv6), so in this case, the system updates the end-user IP address with the first IP address found in the inner packets. You can change the default behavior for DHCP-obtained addresses using the **gtpv2-dhcp** keywords.
gtpv2-dhcp-bypass	(Anti-spoofing) Do not update the 0.0.0.0 or *prefix*::0 address. Instead, allow packets where the end-user IP address is 0.0.0.0 or *prefix*::0. This option bypasses the anti-spoofing check when DHCP is used to obtain the IP address.
gtpv2-dhcp-drop	(Anti-spoofing) Do not update the 0.0.0.0 or *prefix*::0 address. Instead, drop all packets where the end-user IP address is 0.0.0.0 or *prefix*::0. This option prevents access for users that use DHCP to obtain the IP address.
gtp-in-gtp-encapsulation	Drop GTP-in-GTP encapsulated packets. This option can help prevent GTP tunneling attacks. The system examines the data payload for GTP ports (UDP/2123 or UDP/2152) as the source or destination port, and drops matching packets. Without this option, GTP-in-GTP encapsulated packets are allowed.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was introduced.
9.24(1)	The **gtp-in-gtp-encapsulation** was added.

Usage Guidelines

You can use this command to implement anti-spoofing. It is possible for hackers to pretend (spoof) that they are another customer by using another IP address than the one assigned through GTP-C. Anti-spoofing checks whether the GTP-U address used is actually the one which was assigned using GTP-C.

Examples

The following example enables anti-spoofing with the default behavior.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# gtp-u-header-check anti-spoofing
```

The following example drops GTP-in-GTP encapsulated packets.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# gtp-u-header-check gtp-in-gtp-encapsulation
```

Related Commands

Commands	Description
anti-replay	Enables GTP anti-replay in GTP inspection.
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.
show service-policy inspect gtp	Displays the GTP configuration and statistics.

h245-tunnel-block

To block H.245 tunneling in H.323, use the **h245-tunnel-block** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

h245-tunnel-block action [**drop-connection** | **log**]
no h245-tunnel-block action [**drop-connection** | **log**]

Syntax Description

drop-connection	Drops the call setup connection when an H.245 tunnel is detected.
log	Issues a log when an H.245 tunnel is detected.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to block H.245 tunneling on an H.323 call:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# h245-tunnel-block action drop-connection
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

hardware-bypass

To enable the hardware bypass on the Cisco ISA 3000 so that traffic continues to flow between an interface pair during a power outage, use the **hardware-bypass** command in global configuration mode. To disable the hardware bypass, use the **no** form of this command.

hardware-bypass GigabitEthernet { **1/1-1/2** | **1/3-1/4** } [**sticky**]
no hardware-bypass GigabitEthernet { **1/1-1/2** | **1/3-1/4** } [**sticky**]



Note This feature is only available on the Cisco ISA 3000 appliance.

Syntax Description

GigabitEthernet {**1/1-1/2** | **1/3-1/4**}	Supported interface pairs are copper GigabitEthernet 1/1 & 1/2; and GigabitEthernet 1/3 & 1/4. If you have a fiber Ethernet model, only the copper Ethernet pair (GigabitEthernet 1/1 & 1/2) supports hardware bypass. Enter this command separately for each pair.
sticky	(Optional) Keeps the appliance in hardware bypass mode after the power comes back and the appliance boots up. In this case, you need to manually turn off the hardware bypass when you are ready using the **no hardware-bypass manual** command; this option lets you control when the brief interruption occurs.

Command Default

Hardware bypass is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	—	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1.225)	This command was added.

Usage Guidelines

When the hardware bypass is active, no firewall functions are in place, so make sure you understand the risks of allowing traffic through. When the hardware bypass is deactivated, there is a brief connection interruption as the ASA takes over the flows.

Note When the ISA 3000 loses power and goes into hardware bypass mode, only the above interface pairs can communicate; when using the default configuration, inside1 <---> inside2, and outside1 <---> outside2 can no longer communicate. Any existing connections between these interfaces will be lost.

Examples

The following example disables hardware bypass for GigabitEthernet 1/1 and 1/2, and enables it for 1/3 and 1/4:

```
ciscoasa(config)# no hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

Related Commands

Command	Description
hardware-bypass boot-delay	Configures the hardware bypass to remain active until after the ASA FirePOWER module boots up.
hardware-bypass manual	Manually activates or deactivates the hardware bypass.

hardware-bypass boot-delay

To configure the hardware bypass on the Cisco ISA 3000 to remain active until after the ASA Firepower module boots up, use the **hardware-bypass boot-delay** command in global configuration mode. To disable the boot delay, use the **no** form of this command.

hardware-bypass boot-delay module-up sfr
no hardware-bypass boot-delay module-up sfr



Note This feature is only available on the Cisco ISA 3000 appliance.

Syntax Description

module-up sfr	Delays disabling the hardware bypass until after the ASA FirePOWER module boots up.

Command Default

The boot delay is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	—	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1.225)	This command was added.

Usage Guidelines

You must enable hardware bypass using the **hardware-bypass** command without the **sticky** option for the **hardware-bypass boot-delay** command to operate. Without the **hardware-bypass boot-delay** command, the hardware bypass is likely to become inactive before the ASA FirePOWER module finishes booting up. This scenario can cause traffic to be dropped if you configured the module to fail-close, for example.

Examples

The following example enables hardware bypass (*without* the **sticky** option), and enables the boot delay:

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
ciscoasa(config)# hardware-bypass boot-delay module-up sfr
```

Related Commands

Command	Description
hardware-bypass	Configures the hardware bypass for supported interface pairs.
hardware-bypass manual	Manually activates or deactivates the hardware bypass.

hardware-bypass manual

To manually activate or deactivate the hardware bypass on the Cisco ISA 3000, use the **hardware-bypass manual** command in privileged EXEC mode.

hardware-bypass manual GigabitEthernet { **1/1-1/2** | **1/3-1/4** }
no hardware-bypass manual GigabitEthernet { **1/1-1/2** | **1/3-1/4** }

Note This feature is only available on the Cisco ISA 3000 appliance.

Syntax Description

GigabitEthernet {**1/1-1/2** | **1/3-1/4**}	Supported interface pairs are copper GigabitEthernet 1/1 & 1/2; and GigabitEthernet 1/3 & 1/4. If you have a fiber Ethernet model, only the copper Ethernet pair (GigabitEthernet 1/1 & 1/2) supports hardware bypass. Enter this command separately for each pair.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	—	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1.225)	This command was added.

Usage Guidelines

When you configure the **hardware-bypass** command **sticky** option that keeps bypass enabled, you must use the **hardware-bypass manual** command to deactivate hardware bypass after power is restored.

This command changes the current hardware bypass state. In the event of a power failure, the **hardware-bypass** configuration command actions take priority. For example, if **hardware-bypass** is disabled in the configuration, but you enable hardware bypass manually, then at a power failure, hardware bypass becomes disabled according to the configuration.

Examples

The following example manually deactivates hardware bypass for GigabitEthernet 1/2 and 1/2:

```
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

Related Commands

Command	Description
hardware-bypass	Configures the hardware bypass for supported interface pairs.
hardware-bypass boot-delay	Configures the hardware bypass to remain active until after the ASA FirePOWER module boots up.

health-check

To enable the cluster health check feature, use the **health-check** command in cluster group configuration mode. To disable the health check, use the **no** form of this command.

health-check [**holdtime** *timeout*] [**vss-enabled**]
no health-check [**holdtime** *timeout*] [**vss-enabled**]

Syntax Description

holdtime *timeout*	Determines the amount of time between keepalive or interface status messages, between .3 (9.8(1) and later or .8 (9.7 and earlier) and 45 seconds. The default is 3 seconds. Note that configuring a lower holdtime will increase CCL messaging and CPU activity. If you downgrade your ASA software after setting the hold time to .3 - .7, this setting will revert to the default of 3 seconds because the new setting is unsupported.
vss-enabled	If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, then you might need to enable the **vss-enabled** option. For some switches, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable **vss-enabled**, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them.

Command Default

Health check is enabled by default, with a holdtime of 3 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.1(4)	The **vss-enabled** keyword was added.
9.8(1)	The **holdtime** minimum value was lowered to .3 seconds.

Usage Guidelines

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the ASA or the switch, or adding an additional switch to form a VSS or vPC) you should disable the health check feature and also disable interface monitoring for the disabled interfaces (**no health-check**

monitor-interface). When the topology change is complete, and the configuration change is synced to all units, you can re-enable the health check feature.

Keepalive messages between members determine member health. If a unit does not receive any keepalive messages from a peer unit within the holdtime period, the peer unit is considered unresponsive or dead.

Note In 9.8(1), the unit health check messaging scheme was changed to *heartbeats* in the data plane from *keepalives* in the control plane. Using the data plane improves CPU usage and reliability.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units.

Examples

The following example disables the health check:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no health-check
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check auto-rejoin	Customizes the auto-rejoin cluster settings after a health check failure.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

health-check application

To enable Cloud Web Security application health checking, use the **health-check application** command in scansafe general-options configuration mode. To remove health checking or return to the default timeout, use the **no** form of this command.

health-check application { [**url** *url_string*] | **timeout** *seconds* }
no health-check application { [**url** *url_string*] | **timeout** *seconds* }

Syntax Description

url *url_string*	(Optional.) Specifies the URL to use when polling the application. If you do not specify a URL, the default URL is used. The default URL is http://gs.scansafe.net/goldStandard?type=text&size=10. Specify a URL only if instructed to do so by Cisco Cloud Web Security.
timeout *seconds*	Specifies how long the ASA waits after sending a GET request for the health check URL to get a response. The ASA retries the request after the timeout up to the retry limit for polling the server before marking the server as down and initiating failover. The default is 15 seconds, the range is 5-120 seconds.

Command Default

Health checking is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Scansafe general-options configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server. These servers are routinely polled to check for their availability. If your ASA is unable to reach the Cloud Web Security proxy server (for example, if no SYN/ACK packets arrive from the proxy server), then the proxy server is polled through a TCP three-way handshake to check its availability. If the proxy server is unavailable after a configured number of retries (the default is five), the server is declared as unreachable, and the backup proxy server becomes active.

You can further refine failover by checking the health of the Cloud Web Security application. In some cases, the server can complete the TCP three-way handshake, yet the Cloud Web Security application on the server is not functioning correctly. If you enable application health checking, the system can fail over to the backup

server even if the three-way handshake completes, if the application itself does not respond. This provides a more reliable failover setup. Use the **health-check application** command to enable this extra check.

Health checking involves sending a GET request with a test URL to the Cloud Web Security application. Failure to respond within the configured timeout and retry limits marks the server as down, and the system initiates failover. The backup server is also tested to ensure that it is functioning correctly before it is marked as the active server. After failover, the application on the primary server is retested every 30 seconds until it comes back online and can be marked the active server again.

The ASA automatically falls back to the primary Cloud Web Security proxy server from the backup server after continued polling shows that the primary server is active for two consecutive retry count periods. You can change this polling interval using the **retry-count** command.

Examples

The following example configures a primary and backup server and enables health checking using the default URL and timeout. You must enter the **health-check application** command separately to enable health checking and to set a non-default timeout.

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.

Command	Description
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current HTTP(S) connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

health-check auto-rejoin

To customize the auto-rejoin cluster settings after a health check failure, use the **health-check auto-rejoin** command in cluster group configuration mode. To restore the default values, use the **no** form of this command.

health-check { **data-interface** | **cluster-interface** | **system** } **auto-rejoin** { **unlimited** | *auto_rejoin_max* } [*auto_rejoin_interval* [*auto_rejoin_interval_variation*]]
no health-check { **data-interface** | **cluster-interface** | **system** } **auto-rejoin** [{ **unlimited** | *auto_rejoin_max* } [*auto_rejoin_interval* [*auto_rejoin_interval_variation*]]]

Syntax Description

auto_rejoin_interval	(Optional) Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is **5** minutes. The maximum total time that the unit attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.
auto_rejoin_interval_variation	(Optional) Defines if the interval duration increases, between 1 and 3: • **1**—No change • **2**—2 x the previous duration • **3**—3 x the previous duration. For example, if you set the interval duration to 5 minutes, and set the variation to **2**, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is **1** for the cluster-interface and **2** for the data-interface and system.
auto_rejoin_max	Defines the number of attempts at rejoining the cluster, between 0 and 65535. **0** disables auto-rejoining. The default value is **unlimited** for the cluster-interface and **3** for the data-interface and system.
cluster-interface	Sets the auto-rejoin settings for the cluster control link.
data-interface	Sets the auto-rejoin settings for data interfaces.
system	Sets the auto-rejoin settings for internal errors for the system. Internal failures include: application sync timeout; inconsistent application statuses; and so on.
unlimited	Sets the number of attempts at rejoining the cluster to unlimited, the default for the cluster-interface.

Command Default

- The cluster auto-rejoin feature for a failed cluster control link is unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is 3 attempts every 5 minutes, with the increasing interval set to 2.
- The cluster auto-rejoin feature for an internal system error is 3 attempts every 5 minutes, with the increasing interval set to 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.9(2)	Added the **system** keyword.
9.5(1)	This command was added.

Usage Guidelines

This command lets you customize the auto-rejoin options to suit your network conditions.

Examples

The following example configures 10 rejoin attempts for both interface types. For data interfaces, the rejoin interval is 10 minutes, with an interval duration increase of 3 x the interval. for the cluster control link, the rejoin interval is 7 minutes, with an interval duration increase of 2 x the interval.

```
ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 10 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 10 7 2
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# enable noconfirm
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.

Command	Description
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mac-address site-id	Configures a site-specific MAC address for each site.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.
site-id	Sets a site ID to avoid MAC address flapping in inter-site clustering.

health-check chassis-heartbeat-delay-rejoin

To set the chassis rejoin to match the **health-check system auto-rejoin** command for chassis heartbeat failures, use the **health-check chassis-heartbeat-delay-rejoin** command in cluster group configuration mode. To have the chassis rejoin immediately, use the **no** form of this command.

health-check chassis-heartbeat-delay-rejoin
no health-check chassis-heartbeat-delay-rejoin

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.20(2)	This command was added.

Usage Guidelines

By default, if the chassis heartbeat fails and then recovers, the node rejoins the cluster immediately. However, if you configure the **health-check chassis-heartbeat-delay-rejoin** command, it will rejoin according to the settings of the **health-check system auto-rejoin** command.

Examples

The following example configures the **health-check system auto-rejoin** and then enables use of those settings for the chassis heartbeat rejoin.

```
ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# health-check system auto-rejoin 10 10 3
ciscoasa(cfg-cluster)# health-check chassis-heartbeat-delay-rejoin
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# enable noconfirm
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mac-address site-id	Configures a site-specific MAC address for each site.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.
site-id	Sets a site ID to avoid MAC address flapping in inter-site clustering.

health-check monitor-interface

To monitor interfaces, use the **health-check monitor-interface** command in cluster group configuration mode. To disable monitoring, use the **no** form of this command.

health-check monitor-interface { *interface_id* | **service-module** | **service-application** | **debounce-time** }
no health-check monitor-interface { *interface_id* | **service-module** | **service-application** | **debounce-time** }

Syntax Description

interface_id	Enables monitoring on interfaces. You can specify any port-channel ID, redundant ID, or single physical interface ID. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored.
service-application	Enables monitoring of the decorator application on the Firepower 4100/9300.
service-module	Enables monitoring of a software or hardware module on ASA hardware models, such as the ASA FirePOWER module.
debounce-time	Configures the debounce time before the ASA removes a failed interface. Set the debounce time between 300 and 9000 ms. The default is 500 ms. Lower values allow for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the ASA waits the number of milliseconds specified before removing the interface. In the case of an EtherChannel that transitions from a down state to an up state (for example, the switch reloaded, or the switch enabled an EtherChannel), a longer debounce time can prevent the interface from appearing to be failed on a cluster unit just because another cluster unit was faster at bundling the ports.

Command Default

Interface health monitoring is enabled on all interfaces by default.

The debounce time is 500 ms.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Release	Modification
9.5(1)	The **service-module** keyword was added.
9.6(1)	The **service-application** keyword was added.
9.8(1)	The **debounce-time** keyword was added for the Firepower 4100/9300.
9.9(2)	The **debounce-time** keyword was added for ASA appliances.
9.10(1)	The **debounce-time** keyword now applies to interfaces changing from a down state to an up state.

Usage Guidelines

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the ASA or the switch, or adding an additional switch to form a VSS or vPC) you should disable the health check feature (**no health-check**) and also disable interface monitoring for the disabled interfaces (**no health-check monitor-interface**). When the topology change is complete, and the configuration change is synced to all units, you can re-enable the health check feature.

Interface status messages detect link failure. If an interface fails on a particular unit, but the same interface is active on other units, then the unit is removed from the cluster.

If a unit does not receive interface status messages within the holdtime, then the amount of time before the ASA removes a member from the cluster depends on the type of interface and whether the unit is an established member or is joining the cluster. For EtherChannels (spanned or not), if the interface is down on an established member, then the ASA removes the member after 9 seconds. If the unit is joining the cluster as a new member, the ASA waits 45 seconds before rejecting the new unit. For non-EtherChannels, the unit is removed after 500 ms, regardless of the member state.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units.

Examples

The following example disables the health check:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/1
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.

Command	Description
health-check auto-rejoin	Customizes the auto-rejoin cluster settings after a health check failure.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

hello-interval

To specify the interval between EIGRP hello packets sent on an interface, use the **hello-interval** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

hello-interval eigrp *as-number seconds*
no hello-interval eigrp *as-number seconds*

Syntax Description

as-number	Specifies the autonomous system number of the EIGRP routing process.
seconds	Specifies the interval between hello packets that are sent on the interface. Valid values are from 1 to 65535 seconds.

Command Default

The default is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will occur. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

Related Commands

Command	Description
hold-time	Configures the EIGRP hold time advertised in hello packets.

hello padding multi-point

To enable IS-IS hello padding at the router level, enter the **hello padding multi-point** command in router isis configuration mode. To disable IS-IS hello padding, use the **no** form of this command.

hello padding multi-point
no hello padding multi-point

Syntax Description

This command has no arguments or keywords.

Command Default

Hello padding is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command enables IS-IS hellos to be padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding to avoid wasting network bandwidth in case the MTU of both interfaces is the same, or in case of translational bridging. While hello padding is disabled, the ASAs still send the first five IS-IS hellos padded to the full MTU size to maintain the benefits of discovering MTU mismatches.

To disable hello padding for all interfaces on an ASA for the IS-IS routing process, enter the **no hello padding multi-point** command in router configuration mode. To selectively disable hello padding for a specific interface, enter the **no isis hello padding** command in interface configuration mode.

Examples

In the following example the **no hello padding multi-point** command is used to turn off hello padding at the router level:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# hello padding multi-point
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.

Command	Description
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.

Command	Description
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

help

To display help information for the command specified, use the **help** command in user EXEC mode.

help { *command* | **?** }

Syntax Description

?	Displays all commands that are available in the current privilege level and mode.
command	Specifies the command for which to display the CLI help.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **help** command displays help information about all commands. You can see help for an individual command by entering the **help** command followed by the command name. If you do not specify a command name and enter **?** instead, all commands that are available in the current privilege level and mode display.

If you enable the **pager** command and after 24 lines display, the listing pauses, and the following prompt appears:

```
<--- More --->
```

The More prompt uses syntax similar to the UNIX **more** command as follows:

- To see another screen of text, press the **Space** bar.
- To see the next line, press the **Enter** key.
- To return to the command line, press the q key.

Examples

The following example shows how to display help for the **rename** command:

```
ciscoasa
#
help rename
USAGE:
```

```
        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>
DESCRIPTION:
rename          Rename a file
SYNTAX:
/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path
ciscoasa
#
```

The following examples shows how to display help by entering the command name and a question mark:

```
ciscoasa(config)# enable ?
usage: enable password <pwd> [encrypted]
```

Help is available for the core commands (not the show, no, or clear commands) by entering ? at the command prompt:

```
ciscoasa(config)# ?
aaa
   Enable, disable, or view TACACS+ or RADIUS

                     user authentication, authorization and accounting
...
```

Related Commands

Command	Description
show version	Displays information about the operating system software.

hidden-parameter

To specify hidden parameters in the HTTP POST request that the ASA submits to the authenticating web server for SSO authentication, use the **hidden-parameter** command in aaa-server-host configuration mode. To remove all hidden parameters from the running configuration, use the **no** form of this command.

hidden-parameter*string*
nohidden-parameter



Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string A hidden parameter embedded in the form and sent to the SSO server. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for all lines together—the complete hidden parameter—is 2048.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server-host configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

This is an SSO with HTTP Forms command.

The WebVPN server of the ASA uses an HTTP POST request to submit an SSO authentication request to an authenticating web server. That request may require specific hidden parameters from the SSO HTML form—other then username and password—that are not visible to the user. You can discover hidden parameters that the web server expects in the POST request by using a HTTP header analyzer on a form received from the web server.

The **hidden-parameter** command lets you specify a hidden parameter that the web server requires in the authentication POST request. If you use a header analyzer, you can copy and paste the entire hidden parameter string, including any encoded URL parameters.

For ease of entry, you can enter a hidden parameter on multiple, sequential lines. The ASA then concatenates the lines into a single hidden parameter. While the maximum characters per hidden-parameter line is 255 characters, you can enter fewer characters on each line.

Note Any question mark in the string must be preceded by a **Ctrl+v** escape sequence.

Examples

The following example shows a hidden parameter comprised of four form entries and their values, separated by &. Excerpted from the POST request, the four entries and their values are:

- SMENC with a value of ISO-8859-1
- SMLOCALE with a value of US-EN
- target with a value of https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do

%3FEMCOPageCode%3DENG

- smauthreason with a value of 0

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
ciscoasa(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
ciscoasa(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
ciscoasa(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
ciscoasa(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for SSO authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a prelogin cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

hidden-shares

To control the visibility of hidden shares for CIFS files, use the **hidden-shares** command in group-webvpn configuration mode. To remove the hidden shares option from the configuration, use the **no** form of this command.

hidden-shares { **none** | **visible** }
[**no**] **hidden-shares** { **none** | **visible** }

Syntax Description

none	Specifies that no configured hidden shares are visible or accessible to users.
visible	Reveals hidden shares, making them accessible to users.

Command Default

The default behavior for this command is none.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-webvpn configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

A hidden share is identified by a dollar sign ($) at the end of the share name. For example, drive C is shared as C$. With hidden shares, a shared folder is not displayed, and users are restricted from browsing or accessing these hidden resources.

The **no** form of the **hidden-shares** command removes the option from the configuration and disables hidden shares as a group policy attribute.

Examples

The following example makes visible WebVPN CIFS hidden-shares related to GroupPolicy2:

```
ciscoasa(config)# webvpn
ciscoasa(config-group-policy)# group-policy GroupPolicy2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# hidden-shares visible
ciscoasa(config-group-webvpn)#
```

Related Commands

Command	Description
debug webvpn cifs	Displays debugging messages about the CIFS.
group-policy attributes	Enters group-policy configuration mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn configuration mode to configure WebVPN attributes for the group.
url-list	Configures a set of URLs for WebVPN users to access.
url-list	Applies a list of WebVPN servers and URLs to a particular user or group policy.

hold-time

To specify the hold time advertised by the ASA in EIGRP hello packets, use the **hold-time** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

hold-time eigrp *as-number seconds*
no hold-time eigrp *as-number seconds*

Syntax Description

as-number	The autonomous system number of the EIGRP routing process.
seconds	Specifies the hold time, in seconds. Valid values are from 1 to 65535 seconds.

Command Default

The default is 15 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This value is advertised in the EIGRP hello packets sent by the ASA. The EIGRP neighbors on that interface use this value to determine the availability of the ASA. If they do not receive a hello packet from the ASA during the advertised hold time, the EIGRP neighbors will consider the ASA to be unavailable.

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If the ASA does not receive a hello packet within the specified hold time, routes through this neighbor are considered unavailable.

Increasing the hold time delays route convergence across the network.

Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

Related Commands

Command	Description
hello-interval	Specifies the interval between EIGRP hello packets sent on an interface.

homepage

To specify a URL for the web page that displays upon login for this WebVPN user or group policy, use the **homepage** command in webvpn configuration mode. To remove a configured home page, including a null value created by issuing the **homepage none** command, use the **no** form of this command.

homepage { **value** *url-string* | **none** }
no homepage

Syntax Description

none	Indicates that there is no WebVPN home page. Sets a null value, thereby disallowing a home page. Prevents inheriting a home page.
value *url-string*	Provides a URL for the home page. The string must begin with either http:// or https://.

Command Default

There is no default home page.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To specify a home page URL for users associated with the group policy, enter a value for the URL string in this command. To inherit a home page from the default group policy, use the **no** form of the comand. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a home page, use the **homepage none** command.

Clientless users are immediately brought to this page after successful authentication. Secure Client launches the default web browser to this URL upon successful establishment of the VPN connection. On Linux platforms, Secure Client does not currently support this command and ignores it.

Examples

The following example shows how to specify www.example.com as the home page for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
```

```
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
```

Related Commands

Command	Description
webvpn	Lets you enter webvpn configuration mode to configure parameters that apply to group policies or usernames.

homepage use-smart-tunnel

To allow the group policy home page to use the smart tunnel feature when clientless SSL VPN is used, use the **homepage use-smart-tunnel** command in the group-policy webvpn configuration mode.

homepage { **value** *url-string* | **none** }
homepage use-smart-tunnel

Syntax Description

none	Indicates that there is no WebVPN home page. Sets a null value, thereby disallowing a home page. Prevents inheriting a home page.
value *url-string*	Provides a URL for the home page. The string must begin with either http:// or https://.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

You can use the HTTP capture tool to monitor the browser session and verify that the smart tunnel was initiated during the WebVPN connection. What you see in the browser capture determines whether the request is forwarded to the web page without degradation and whether the smart tunnel is used. If you see something like https://172.16.16.23/+CSCOE+portal.html, the *+CSCO** indicates that the content is degraded by the ASA. When the smart tunnel is initiated, you see an **http get** command to a specific URL without the +CSCO* (such as GET 200 html http://mypage.example.com).

Examples

If you consider a case where Vendor V wants to provide Partner P with clientless access to their internal inventory server pages, Vendor V's administrator must decide the following:

- Will users have access to the inventory pages after they log into a clientless SSL VPN, whether or not they go through the clientless portal?
- Will the smart tunnel be a good choice for access because the page includes a Microsoft Silverlight component?

- Is a tunnel-all policy suitable because once the browser has been tunneled, all tunnel policy forces all browser traffic to go through Vendor V's ASA, leaving Partner P's users with no access to internal resources?

With the assumption that inventory pages are hosted at inv.example.com (10.0.0.0), the following example creates a tunnel policy that contains only one host:

```
ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.0.0.0
ciscoasa(config-webvpn)# smart-tunnel network inventory host inv.example.com
```

The following example applies a tunnel-specified tunnel policy to the partner's group policy:

```
ciscoasa(config-group-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory
```

The following example specifies the group policy home page and enables a smart tunnel on it:

```
ciscoasa(config-group-webvpn)# homepage value http://inv.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
```

host (network object)

To configure a host for a network object, use the **host** command in object network configuration mode. To remove the host from the object, use the **no** form of this command.

host*ip_address*
no host *ip_address*

Syntax Description

ip_address	Identifies the host IP address for the object, either IPv4 or IPv6.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

If you configure an existing network object with a different IP address, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a host network object:

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
nat	Enables NAT for the network object.
object network	Creates a network object.
object-group network	Creates a network object group.
show running-config object network	Shows the network object configuration.

host (parameters)

To specify a host to interact with using RADIUS accounting, use the **host** command in radius-accounting parameter configuration mode, which is accessed by using the **parameters** command in the policy-map type inspect radius-accounting submode. To disable the specified host, use the **no** form of this command.

host *address* [**key** *secret*]
no host *address* [**key** *secret*]

Syntax Description

host	Specifies a single endpoint sending the RADIUS accounting messages.
address	The IP address of the client or server sending the RADIUS accounting messages.
key	Optional keyword to specify the secret of the endpoint sending the gratuitous copy of the accounting messages.
secret	The shared secret key of the endpoint sending the accounting messages used to validate the messages. This can be up to 128 alphanumeric characters.

Command Default

The **no** option is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Radius-accounting parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Multiple instances of this command are allowed.

Examples

The following example shows how to specify a host with RADIUS accounting:

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# host 209.165.202.128 key cisco123
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

hostname

To set the ASA hostname, use the **hostname** command in global configuration mode. To restore the default hostname, use the **no** form of this command.

hostname*name*
no hostname [*name*]

Syntax Description

name Specifies a hostname up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.

Command Default

The default hostname depends on your platform.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	You can no longer use non-alphanumeric characters (other than a hyphen).

Usage Guidelines

The hostname appears as the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts.

The hostname that you optionally set within a context does not appear in the command line, but can be used for the **banner** command **$(hostname)** token.

Examples

The following example sets the hostname to firewall1:

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

Related Commands

Command	Description
banner	Sets a login, message of the day, or enable banner.
domain-name	Sets the default domain name.

hostname dynamic

To enable IS-IS dynamic hostname capability on the ASA, use the **hostname dynamic** command in router isis configuration mode. To disable the dynamic hostname feature, use the **no** form of this command.

hostname dynamic
no hostname dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

The dynamic hostname is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

In the IS-IS routing domain, the system ID is used to represent each ASA. The system ID is part of the network entity title (NET) that is configured for each IS-IS ASA. For example, an ASA with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a. Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname** command displays the entries in the system-ID-to-router-name mapping table.

The dynamic hostname mechanism uses link-state protocol (LSP) flooding to distribute the router-name-to-system-ID mapping information across the entire network. Every ASA on the network will try to install the system ID-to-router name mapping information in its routing table.

If an ASA that has been advertising the dynamic name type, length, value (TLV) on the network suddenly stops the advertisement, the mapping information last received remains in the dynamic host mapping table for up to one hour, which allows the network administrator to display the entries in the mapping table during a time when the network experiences problems. Entering the **show isis hostname** command displays the entries in the mapping table.

Examples

The following example sets the hostname to firewall1:

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

hostscan enable

To enable hostscan for clientless SSL VPN remote access or remote access using the Secure Client, use the hostscan enable command in webvpn configuration mode. To disable hostscan, use the **no** form of this command.

hostscan enable
no hostscan enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Hostscan is enabled or disabled globally for all remote access connection attempts made to the ASA with one exception.

The **hostscan enable** command does the following:

1. Provides a validity check that supplements the check performed by the previous hostscan image *path* command.
2. Creates an sdesktop folder on disk0: if one is not already present.
3. Inserts a data.xml (Hostscan configuration) file in the sdesktop folder if one is not already present.
4. Loads the data.xml from the flash device to the running configuration.
5. Enables Hostscan.

Note You can enter the **show webvpn hostscan** command to determine whether or not hostscan is enabled.

- The hostscan image *path* command must be in the running configuration before you enter the **hostscan enable** command.
- The **no hostscan enable** command disables Hostscan in the running configuration. If Hostscan is disabled, you cannot access Hostscan Manager and remote users cannot use Hostscan.
- If you transfer or replace the data.xml file, disable and then enable Hostscan to load the file into the running configuration.
- Hostscan is enabled or disabled globally for all remote access connection attempts made to the ASA. You cannot enable or disable Hostscan for an individual connection profile or group policy.

Exception: Connection profiles for clientless SSL VPN connections can be configured so that Hostscan will not run on the client computer if the computer is attempting to connect to the ASA using a group URL and Hostscan is enabled globally. For example:

ciscoasa(config)# **tunnel-group***group-name***webvpn-attributes**

ciscoasa(config-tunnel-webvpn)# **group-url https://www.url-string.com**

ciscoasa(config-tunnel-webvpn)# without-Hostscan

Examples

The following commands shows how to view the status of the hostscan image and enable it:

```
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# hostscan enable
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan version 4.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
hostscan image	Copies the hostscan image named in the command from the flash drive specified in the path to the running configuration.
show webvpn hostscan	Identifies the version of Hostscan if it is enabled. Otherwise, the CLI indicates "Secure Desktop is not enabled."
without-Hostscan	Configures connection profiles for clientless SSL VPN sessions so that hostscan will not run on the client computer if the computer is attempting to connect to the ASA using a group URL and Hostscan is enabled globally.

hostscan image

To install or upgrade the Cisco Host Scan distribution package and add it to the running configuration, use the hostscan image command in webvpn configuration mode. To remove the Host Scan distribution package from the running configuration, use the **no** form of this command:

hostscan image *path*
no hostscan image *path*

Syntax Description

path Specifies the path and filename of the Cisco Host Scan package, up to 255 characters.

The Host Scan package can be a standalone Host Scan package that can be downloaded from Cisco.com and has the file name convention, hostscan-version.pkg, or it can be the full Secure Client package that can also be downloaded from Cisco.com and has the file name convention, anyconnect-win-version-k9.pkg. When customers specify the Secure Client, the ASA extracts the Host Scan package from the Secure Client package and installs it.

The Host Scan package contains the Host Scan software as well as the Host Scan library and support charts.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Enter the **show webvpn hostscan** command to determine the version of the Host Scan image that is currently installed and enabled.

After installing Host Scan with the **hostscan image** command, enable the image using the enable command.

Enter the **write memory** command to save the running configuration to ensure that the Host Scan image is available the next time that the ASA reboots.

Examples

The following commands show how to install a Cisco Host Scan package, enable it, view it, and save the configuration on the flash drive:

```
ciscoasa> en
```

```
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# hostscan image disk0:/hostscan_3.0.0333-k9.pkg

ciscoasa(config-webvpn)# hostscan enable
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e
22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
show webvpn hostscan	Identifies the version of Cisco Host Scan if it is enabled. Otherwise, the CLI indicates "Hostscan is not enabled."
hostscan enable	Enables Hostscan for management and remote user access.

hpm topn enable

To enable real-time reports in ASDM of the top hosts connecting through the ASA, use the **hpm topn enable** command in global configuration mode. To disable the hosts reporting, use the **no** form of this command.

hpm topn enable
no hpm topn enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

You might want to disable this command to maximize system performance. This command populates the ASDM Home > Firewall Dashboard > Top 200 Hosts pane.

Examples

The following example enables the top hosts reporting:

```
ciscoasa(config)# hpm topn enable
```

Related Commands

Command	Description
clear configure hpm	Clears the HPM configuration.
show running-config hpm	Shows the HPM configuration.

hsi

To add an HSI to an HSI group for H.323 protocol inspection, use the **hsi** command in hsi group configuration mode. To disable this feature, use the **no** form of this command.

hsi*ip_address*
no hsi *ip_address*

Syntax Description

ip_address	IP address of the host to add. A maximum of five HSIs per HSI group is allowed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Hsi group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to add an HSI to an HSI group in an H.323 inspection policy map:

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
endpoint	Adds an endpoint to the HSI group.
hsi-group	Creates an HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

hsi-group

To define an HSI group for H.323 protocol inspection and to enter hsi group configuration mode, use the **hsi-group** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

hsi-group*group_id*
no hsi-group *group_id*

Syntax Description

group_id	HSI group ID number, from 0 to 2147483647.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure an HSI group in an H.323 inspection policy map:

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
endpoint	Adds an endpoint to the HSI group.
hsi	Adds an HSI to the HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

hsts enable

To configure sending the HTTP Strict Transport Security Header to browsers and other user agents, use the **hsts enable** command in webvpn configuration mode. To remove this setting from the configuration use the no form of this command. Once enabled, compliant browsers and user agents will switch to HTTPS if access is attempted in an unsecured manner.

hsts enable
no hsts enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the Strict Transport Security Header is not used.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

HTTP Strict Transport Security (HSTS) is a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

When enabled, the default timeout value if of 10,886,400 seconds (18weeks) is used. This can be changed using the **hsts max-age** command.

Examples

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# hsts enable
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
hsts max-age	Maximum amount of time the ASA will be treated as an HSTS host and accessed securely.

Command	Description
show running-config webvpn hsts	Displays the running configuration for SSL VPN, including any HTTP settings.

hsts max-age

When configured to send the HTTP Strict Transport Security Header to browsers or other user agents, (using the **hsts enable** command), **hsts max-age** sets the maximum amount of time the ASA will be treated as an HSTS host and accessed securely

hsts max-age *max-value-in-seconds*

Syntax Description

max-value-in-seconds	The amount of time in seconds that HSTS will be in effect. Range is from <0-31536000> seconds.

Command Default

By default, the maximum is 10,886,400 (18 weeks).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

HTTP Strict Transport Security (HSTS) is a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

When enabled, the default timeout value of 10,886,400 seconds (18weeks) is used. This command alters the timeout.

Examples

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# hsts max-age 31536000
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
hsts enable	Enables sending of the HSTS Header.

Command	Description
show running-config webvpn hsts	Displays the running configuration for SSL VPN, including any HTTP settings.

html-content-filter

To filter Java, ActiveX, images, scripts, and cookies for WebVPN sessions for this user or group policy, use the **html-content-filter** command in webvpn configuration mode. To remove a content filter, use the **no** form of this command.

html-content-filter { **java** | **images** | **scripts** | **cookies** | **none** }
no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

Syntax Description

cookies	Removes cookies from images, providing limited ad filtering and privacy.
images	Removes references to images (removes <IMG> tags).
java	Removes references to Java and ActiveX (removes the <EMBED>, <APPLET>, and <OBJECT> tags.
none	Indicates that there is no filtering. Sets a null value, thereby disallowing filtering. Prevents inheriting filtering values.
scripts	Removes references to scripting (removes <SCRIPT> tags).

Command Default

No filtering occurs.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To remove all content filters, including a null value created by issuing the **html-content-filter none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting an HTML content filter, use the **html-content-filter none** command.

Using the command a second time overrides the previous setting.

Examples

The following example shows how to set filtering of Java and ActiveX, cookies, and images for the group policy named FirstGroup:

```
ciscoasa
```

```
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# html-content-filter java cookies images
```

Related Commands

Command	Description
webvpn	Lets you enter webvpn configuration mode to configure parameters that apply to group policies or usernames. Lets you enter global configuration mode to configure global settings for WebVPN.

http (global)

To specify hosts that can access the HTTP server internal to the ASA, use the **http** command in global configuration mode. To remove one or more hosts, use the **no** form of this command. To remove the attribute from the configuration, use the **no** form of this command without arguments.

http*ip_addresssubnet_maskinterface_name*
no http

Syntax Description

interface_name	Provides the name of the ASA interface through which the host can access the HTTP server. A physical or virtual interface can be specified. if a BVI interface is specified, **managenent-access** must be configured on that interface.
ip_address	Provides the IP address of a host that can access the HTTP server.
subnet_mask	Provides the subnet mask of a host that can access the HTTP server.

Command Default

No hosts can access the HTTP server.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	If you have a directly-connected HTTP management station, you can use a /31 subnet on the ASA and the host to create a point-to-point connection.
9.9.(2)	Virtual interfaces can now be specified.

Examples

The following example shows how to allow the host with the IP address of 10.10.99.1 and the subnet mask of 255.255.255.255 access to the HTTP server via the outside interface:

```
ciscoasa(config)# http 10.10.99.1 255.255.255.255 outside
```

The next example shows how to allow any host access to the HTTP server via the outside interface:

```
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http[s] (parameters)

To specify the service type for the scansafe inspection policy map, use the **http**[**s**] command in parameters configuration mode. To remove the service type, use the **no** form of this command. You can access the parameters configuration mode by first entering the **policy-map type inspect scansafe** command.

{ **http** | **https** }
no { **http** | **https** }

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You can only specify one service type for a Scansafe inspection policy map, either **http** or **https**. There is no default; you must specify a type.

Examples

The following example creates an inspection policy map, and sets the service type to HTTP:

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.

Command	Description
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

http authentication-certificate

To require a certificate for authentication with ASDM HTTPS connections, use the **http authentication-certificate** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command.

http authentication-certificate *interface name* [**match** *certificate_map_name*]
no http authentication-certificate [*interface* [**match** *certificate_map_name*]]

Syntax Description

interface	Specifies the interface on the ASA that requires certificate authentication.
match *certificate_map_name*	Requires the certificate to match a certificate map. Configure the map using the **crypto ca certificate map** command.

Command Default

HTTP certificate authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0.3	This command was deprecated in favor of the **ssl certificate-authentication** command.
8.2.1	This command was re-added; the global **ssl certificate-authentication** command was kept for backwards compatibility.
8.4.7, 9.1.3	Certificate-only authentication was enabled. Previously, this command only added certificate authentication to user authentication when you enabled the **aaa authentication http console** command.
9.6(2)	We added the **match** *certificate_map_name* option.

Usage Guidelines

You can require certificate authentication, with or without AAA authentication. You configure certificate authentication for each interface, so that connections on a trusted/inside interface do not have to provide a certificate. You can use the command multiple times to enable certificate authentication on multiple interfaces.

The ASA validates certificates against the PKI trust points. If a certificate does not pass validation, the ASA closes the SSL connection.

Examples

The following example shows how to require certificate authentication for clients connecting to the interfaces named outside and external:

```
ciscoasa(config)# http authentication-certificate inside
ciscoasa(config)# http authentication-certificate external
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the ASA interface through which the host accesses the HTTP server.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.
ssl authentication-certificate	To require a certificate for SSL connections.

http-comp

To enable compression of HTTP data over a WebVPN connection for a specific group or user, use the http-comp command in the group-policy webvpn and username webvpn configuration modes. To remove the command from the configuration and have the value be inherited, use the **no** form of this command.

http-comp { **gzip** | **none** }
no http-comp { **gzip** | **none** }

Syntax Description

gzip	Specifies compression is enabled for the group or user.
none	Specifies compression is disabled for the group or user.

Command Default

By default, compression is set to enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

For WebVPN connections, the **compression** command configured in global configuration mode overrides the **http-comp** command configured in group policy and username webvpn configuration modes.

Examples

The following example disables compression for the group-policy sales:

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# http-comp none
```

Related Commands

Command	Description
compression	Enables compression for all SVC, WebVPN, and IPsec VPN connections.

http connection idle-timeout

To set an idle timeout for HTTPS connections to the ASA, including ASDM, clientless VPN, Secure Client, and other clients, use the **http connection idle-timeout** command in global configuration mode. To disable the timeout, use the **no** form of this command.

http connection idle-timeout *seconds*
no http connection idle-timeout

Syntax Description

seconds	The idle timeout, from10-86400 seconds.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.14(1)	This command was added.

Usage Guidelines

The ASA disconnects a connection that is idle for the set period of time. If you set both the **http server idle-timeout** and the **http connection idle-timeout** commands, the **http connection idle-timeout** command takes precedence.

Examples

The following example sets the idle timeout for HTTPS sessions to 600 seconds:

```
ciscoasa(config)# http connection idle-timeout 600
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration, disables the HTTP server, and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask and the interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.

Command	Description
http server enable	Enables the HTTP server for ASDM sessions.
http server idle-timeout	Sets the ASDM idle timeout.
http server session-timeout	Limits the session time of ASDM sessions to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http-only-cookie

To enable the httponly flag for a Clientless SSL VPN session cookie, use the **http-only-cookie** command in webvpn configuration mode. To remove the flag from the configuration, use the **no** form of this command.

http-only-cookie
no http-only-cookie

Syntax Description

This command has no arguments or keywords.

Command Default

The httponly flag is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.2(3)	This command was introduced.

Usage Guidelines

Embedded objects such as Flash applications and Java applets, as well as external applications, usually rely on an existing session cookie to work with the server. They get it from a browser using some Javascript on initialization. Adding the httponly flag to the Clientless SSL VPN session cookie makes the session cookie only visible to the browser, not the client-side scripts, and it makes session sharing impossible.

Change the VPN session cookie setting only when there are no active Clientless SSL VPN sessions Use the **show vpn-sessiondb webvpn** command to check the status of Clientless SSL VPN sessions. Use the **vpn-sessiondb logoff webvpn** command to log out of all Clientless SSL VPN sessions.

The following Clientless SSL VPN features will not work when the **http-only-cookie** command is enabled:

- Java plug-ins
- Java rewriter
- Port forwarding
- File browser
- Sharepoint features that require desktop applications (for example, MS Office applications)
- AnyConnect Web launch
- Citrix Receiver, XenDesktop, and Xenon

- Other non-browser-based and browser plugin-based applications

Note Use this command only if Cisco TAC advises you to do so. Enabling this command presents a security risk.

Examples

The following example shows how to enable the httponly flag for a Clientless SSL VPN session cookie:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# http-only-cookie
ciscoasa(config-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the running configuration for Clientless SSL VPN.

http-only-cookie

To enable the httponly flag for a Clientless SSL VPN session cookie, use the **http-only-cookie** command in webvpn configuration mode. To remove the flag from the configuration, use the **no** form of this command.

http-only-cookie
no http-only-cookie

Syntax Description

This command has no arguments or keywords.

Command Default

The httponly flag is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.2(3)	This command was introduced.

Usage Guidelines

Embedded objects such as Flash applications and Java applets, as well as external applications, usually rely on an existing session cookie to work with the server. They get it from a browser using some Javascript on initialization. Adding the httponly flag to the Clientless SSL VPN session cookie makes the session cookie only visible to the browser, not the client-side scripts, and it makes session sharing impossible.

Change the VPN session cookie setting only when there are no active Clientless SSL VPN sessions Use the **show vpn-sessiondb webvpn** command to check the status of Clientless SSL VPN sessions. Use the **vpn-sessiondb logoff webvpn** command to log out of all Clientless SSL VPN sessions.

The following Clientless SSL VPN features will not work when the **http-only-cookie** command is enabled:

- Java plug-ins
- Java rewriter
- Port forwarding
- File browser
- Sharepoint features that require desktop applications (for example, MS Office applications)
- AnyConnect Web launch
- Citrix Receiver, XenDesktop, and Xenon

- Other non-browser-based and browser plugin-based applications

Note Use this command only if Cisco TAC advises you to do so. Enabling this command presents a security risk.

Examples

The following example shows how to enable the httponly flag for a Clientless SSL VPN session cookie:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# http-only-cookie
ciscoasa(config-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the running configuration for Clientless SSL VPN.

http-proxy (call-home)

To set the HTTP(S) proxy for smart licensing and Smart Call Home, use the **http-proxy** command in call-home configuration mode. To remove the proxy, use the **no** form of this command.

http-proxy*ip_address***port***port*
no http-proxy *ip_address* **port** *port*

Syntax Description

ip_address	Sets the IP address for the HTTP proxy server.
port *port*	Sets the port number for the HTTP proxy. For example, use 443 for an HTTPS server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Call-home configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

This command sets an HTTP or HTTPS proxy globally for Smart Call Home and smart licensing.

Examples

The following example sets the HTTP proxy:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.

Command	Description
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

http-proxy (dap)

To enable or disable HTTP proxy port forwarding, use the **http-proxy** command in dap-webvpn configuration mode.To remove the attribute from the configuration, use the **no** form of this command.

http-proxy { **enable** | **disable** | **auto-start** }
no http-proxy

Syntax Description

auto-start	Enables and automatically starts HTTP proxy port forwarding for the DAP record.
enable/disable	Enables or disables HTTP proxy port forwarding for the DAP record.

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap-webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The ASA can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the tunnel group
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or tunnel group.

When you enable or disable an attribute for a DAP record, the ASA applies that value and enforces it. For example, when you disable HTTP proxy in dap-webvpn configuration mode, the ASA looks no further for a value. When you instead use the **no** value for the **http-proxy** command, the attribute is not present in the DAP record, so the ASA moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable HTTP proxy port forwarding for the DAP record named Finance.

```
ciscoasa
 (config)#
dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dap-webvpn)#
 http-proxy enable
ciscoasa
(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record	Displays the running configuration for all DAP records, or for the named DAP record.

http-proxy (webvpn)

To configure the ASA to use an external proxy server to handle HTTP requests, use the **http-proxy** command in webvpn configuration mode. To remove the HTTP proxy server from the configuration, use the **no** form of this command.

http-proxy { **host** [*port*] [**exclude** *url*] | **pac** *pacfile* } [**username** *username* { **password** *password* }]
no http-proxy

Syntax Description

host	Hostname or IP address for the external HTTP proxy server.
pac pacfile	Identifies the PAC file that contains a JavaScript function that specifies one or more proxies.
password	(Optional, and available only if you specify a username) Enter this keyword to accompany each HTTP proxy request with a password to provide basic, proxy authentication.
password	Password to send to the proxy server with each HTTP request.
port	(Optional) Port number used by the HTTP proxy server. The default port is 80, which is the port that the ASA uses if you do not supply a value. The range is 1-65535.
url	Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards: • ***** to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string. • **?** to match any single character, including slashes and periods. • [*x*-*y*] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set. • [**!***x*-*y*] to match any single character that is not in the range.
username	(Optional) Enter this keyword to accompany each HTTP proxy request with a username to provide basic, proxy authentication.
username	Username to send to the proxy server with each HTTP request.

Command Default

By default, no HTTP proxy server is configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **exclude**, **username**, and **password** keywords were added.

Usage Guidelines

Requiring Internet access via a server that the organization controls provides another opportunity for filtering to assure secure Internet access and administrative control.

The ASA supports only one instance of the **http-proxy** command. If one instance of this command is already present in the running configuration and you enter another instance, the CLI overwrites the previous instance. The CLI lists any **http-proxy** commands in the running configuration if you enter the **show running-config webvpn** command. If the response does not list an **http -proxy** command, then none is present.

Note Proxy NTLM authentication is not supported in **http-proxy**. Only proxy without authentication and basic authentication are supported.

Examples

The following example shows how to configure use of an HTTP proxy server with an IP address of 209.165. 201.2 using the default port, 443:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# http-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

The following example shows how to configure use of the same proxy server, and send a username and password with each HTTP request:

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

The following example shows the same command, except when the ASA receives the specific URL www.example.com in an HTTP request, it resolves the request instead of passing it on to the proxy server:

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
ciscoasa(config-webvpn)
```

The following example shows how to use the **exclude** option:

```
ciscoasa(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
 12345678
ciscoasa(config-webvpn)
```

The following example shows how to use the **pac** option:

```
ciscoasa(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

Related Commands

Command	Description
https-proxy	Configures the use of an external proxy server to handle HTTPS requests.
show running-config webvpn	Displays the running configuration for SSL VPN, including any HTTP and HTTPS proxy servers.

http redirect

To specify that the ASA redirect HTTP connections to HTTPS, use the **http redirect** command in global configuration mode. To remove a specified **http redirect** command from the configuration, use the **no** form of this command. To remove all **http redirect** commands from the configuration, use the **no** form of this command without arguments.

http redirect *interface* [*port*]
no http redirect [*interface*]

Syntax Description

interface	Identifies the interface for which the ASA should redirect HTTP requests to HTTPS.
port	Identifies the port that the ASA listens on for HTTP requests, which it then redirects to HTTPS. By default, it listens on port 80,

Command Default

HTTP redirect is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The interface requires an access list that permits HTTP. Otherwise the ASA does not listen to port 80, or to any other port that you configure for HTTP.

If the **http redirect** command fails, the following message appears:

```
"TCP port <port_number> on interface <interface_name> is in use by another feature. Please
 choose a different port for the HTTP redirect service"
```

Use a different port for the HTTP redirect service.

Examples

The following example shows how to configure HTTP redirect for the inside interface, keeping the default port 80:

```
ciscoasa(config)# http redirect inside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the ASA interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server basic-auth-client

To allow non-browser-based HTTPS clients to access HTTPS services on the ASA, use the **http server basic-auth-client** command in global configuration mode. To remove support for a client, use the **no** form of this command.

http server basic-auth-client *user_agent*
no http server basic-auth-client *user_agent*

Syntax Description

user_agent Specifies the client's User-Agent string in the HTTP header of the HTTP request. You can specify the complete string or a partial string; partial strings must match the start of the User-Agent string. We recommend complete strings for better security. Note that the string is case-sensitive.

For example, **curl** will match the following User-Agent string:

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

curl will not match the following User-Agent string:

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

CURL will not match the following User-Agent string:

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

Command Default

By default, ASDM, CSM, and REST API are allowed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.12(1)	Command added.

Usage Guidelines

Enter each client string using a separate command. Many specialty clients (for example, python libraries, curl, and wget) do not support Cross-site request forgery (CSRF) token-based authentication, so you need to

specifically allow these clients to use the ASA basic authentication method. For security purposes, you should only allow required clients.

Examples

The following example allows the curl client:

```
ciscoasa(config)# http server basic-auth-client curl
```

Related Commands

Command	Description
http server enable	Enables the HTTPS server on the ASA.

http server enable

To enable the ASA HTTP server, use the **http server enable** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

http server enable [*port*]

Syntax Description

port	The port to use for HTTP connections. The range is 1-65535. The default port is 443.

Command Default

The HTTP server is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to enable the HTTP server.

```
ciscoasa(config)# http server enable
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the ASA interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server idle-timeout

To set an idle timeout for ASDM connections to the ASA, use the **http server idle-timeout** command in global configuration mode. To disable the timeout, use the **no** form of this command.

http server idle-timeout [*minutes*]
no http server idle-timeout [*minutes*]

Syntax Description

minutes	The idle timeout, from 1-1440 minutes.

Command Default

The default setting is 20 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Although you can enter this command in multiple context mode, the command has no effect. You cannot configure HTTP server timeouts in multiple context mode.

Examples

The following example sets the idle timeout for ASDM sessions to 500 minutes:

```
ciscoasa(config)# http server idle-timeout 500
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration, disables the HTTP server, and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask and the interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http server enable	Enables the HTTP server for ASDM sessions.

Command	Description
http server session-timeout	Limits the session time of ASDM sessions to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server session-timeout

To set a session timeout for ASDM connections to the ASA, use the **http server session-timeout** command in global configuration mode. To disable the timeout, use the **no** form of this command.

http server session-timeout [*minutes*]
no http server session-timeout [*minutes*]

Syntax Description

minutes The session timeout, from 1-1440 minutes.

Command Default

The session timeout is disabled. ASDM connections have no session time limit.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Although you can enter this command in multiple context mode, the command has no effect. You cannot configure HTTP server timeouts in multiple context mode.

Examples

The following example sets a session timeout for ASDM connections to 1000 minutes:

```
ciscoasa(config)# http server session-timeout 1000
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask and the interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http server enable	Enables the HTTP server for ASDM sessions.

Command	Description
http server session-timeout	Limits the idle time of ASDM sessions to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

https-proxy

To configure the ASA to use an external proxy server to handle HTTPS requests, use the **https-proxy** command in webvpn configuration mode. To remove the HTTPS proxy server from the configuration, use the **no** form of this command.

https-proxy { *host* [*port*] [**exclude** *url*] | [**username** *username* { **password** *password* }]
no https-proxy

Syntax Description

host	Hostname or IP address for the external HTTPS proxy server.
password	(Optional, and available only if you specify a username) Enter this keyword to accompany each HTTPS proxy request with a password to provide basic, proxy authentication.
password	Password to send to the proxy server with each HTTPS request.
port	(Optional) Port number used by the HTTPS proxy server. The default port is 443, which is the port the ASA uses if you do not supply a value. The range is 1-65535.
url	Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards: • ***** to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string. • **?** to match any single character, including slashes and periods. • [*x*-*y*] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set. • [**!***x*-*y*] to match any single character that is not in the range.
username	(Optional) Enter this keyword to accompany each HTTPS proxy request with a username to provide basic, proxy authentication.
username	Username to send to the proxy server with each HTTPS request.

Command Default

By default, no HTTPS proxy server is configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **exclude**, **username**, and **password** keywords were added.

Usage Guidelines

Requiring Internet access via a server that the organization controls provides another opportunity for filtering to assure secure Internet access and administrative control.

The ASA supports only one instance of the **https-proxy** command. If one instance of this command is already present in the running configuration and you enter another instance, the CLI overwrites the previous instance. The CLI lists any **https-proxy** commands in the running configuration if you enter the **show running-config webvpn** command. If the response does not list an **https-proxy** command, then none is present.

Examples

The following example shows how to configure use of an HTTPS proxy server with an IP address of 209.165. 201.2 using the default port, 443:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# https-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

The following example shows how to configure use of the same proxy server, and send a username and password with each HTTPS request:

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

The following example shows the same command, except that when the ASA receives the specific URL www.example.com in an HTTPS request, it resolves the request instead of passing it on to the proxy server:

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
 password mysecretdonttell
ciscoasa(config-webvpn)
```

The following example shows how to use the **exclude** option:

```
ciscoasa(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
 12345678
ciscoasa(config-webvpn)
```

The following example shows how to use the **pac** option:

```
ciscoasa(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

Related Commands

Command	Description
http-proxy	Configures the use of an external proxy server to handle HTTP requests.
show running-config webvpn	Displays the running configuration for SSL VPN, including any HTTP and HTTPS proxy servers.

http username-from-certificate

To specify the field in a certificate/rule from which you want to derive the username for ASDM authorization or authentication use, use the **http username-from-certificate** command.

http username-from-certificate { < **primary-attr** > [< **secondary-attr** >] | **use-entire-name** | **use-script** } | **pre-fill-username**

Syntax Description

pre-fill-username	Enables the use of the existing username-from-certificate command from the tunnel-group general-attributes mode that serves the same purpose for VPN connections. When enabled, this username, along with the password typed in by the user, is used for authentication.
primary-attr	Specify the attribute used to derive the username.
secondary-attr	Specify an additional attribute used with the primary attribute to derive the username.
use-entire-name	Use entire DN name. Not available as a secondary attribute.
use-script	Use LUA script generated by ASDM.

Command Default

The default for this command is http username-from-certificate CN OU.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Possible values for primary and secondary attributes and the meanings of the related keywords are as follows:

Attribute/Keyword	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISE 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available as a secondary attribute.
DNQ	Domain Name Qualifier.

Attribute/Keyword	Definition
EA	Email address.
GENQ	Generation qualifier.
GN	Given name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (0).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located.
T	Title.
UID	User Identifier.
UPN	User Principal Name.

This command is not available on platforms that do not support webvpn(ASA 1000v) and platforms with No Payload Encryption (NPE) enabled.

Examples

```
100/act(config)# http ?
configure mode commands/options:
  Hostname or A.B.C.D         The IP address of the host and/or network
                              authorized to access the HTTP server
  X:X:X:X::X/<0-128>          IPv6 address/prefix authorized to access the HTTP
                              server
  authentication-certificate  Request a certificate from the HTTPS client when
                              a management connection is being established
  redirect                    Redirect HTTP connections to the security gateway
                              to use HTTPS
  server                      Enable the http server required to run Device
                              Manager
  username-from-certificate   Specify fields from certificate DN to be used for
                              authorization/authentication
100/act(config)# help http
USAGE:
        [no] http {<local_ip>|<hostname>} <mask> <if_name>
        [no] http authentication-certificate <if_name>
        [no] http redirect <if_name> [<port>]
        [no] http server enable [<port>]
        [no] http username-from-certificate {<primary-attr> [<secondary-attr>] | use-
entire-name | use-script } [pre-fill-username]
        show running-config [all] http
        clear configure http
DESCRIPTION:
```

```
http            Configure HTTP server
SYNTAX:
<local_ip>      The ip address of the host and/or network authorized to
                access the device HTTP server.
<hostname>      Hostname of the host authorized to access the device
                HTTP server.
<mask>          The IP netmask to apply to <local_ip>.
                Default is 255.255.255.255.
<if_name>       Network interface name.
<port>          The decimal number or name of a TCP or UDP port.
                Default is "http" (80).
<primary-attr>  The DN from the certificate to be used as the username

<secondary-attr> Optional Secondary DN from the certificate to be used in the username
```

hw-module module allow-ip

For the AIP SSC on the ASA 5505, to set the hosts that are allowed to access the management IP address, use the **hw-module module allow-ip** command in privileged EXEC mode.

hw-module module 1 allow-ip *ip_address netmask*

Syntax Description

1	Specifies the slot number, which is always 1.
ip_ address	Specifies the host IP address(es).
netmask	Specifies the subnet mask.

Command Default

In the factory default configuration, the following hosts are allowed to manage the IPS module: 192.168.1.5 through 192.168.1.254.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command is only valid when the SSC status is Up.

These settings are written to the IPS application configuration, not the ASA configuration. You can view these settings from the ASA using the **show module details** command.

You can alternatively use the IPS application **setup** command to configure this setting from the IPS CLI.

Examples

The following example shows how to configure host parameters on the SSC:

```
ciscoasa# hw-module module 1 allow-ip 209.165.201.29 255.255.255.0
```

Related Commands

Command	Description
hw-module module ip	Configures the AIP SSC management address.
show module	Shows module status information.

hw-module module ip

For the AIP SSC on the ASA 5505, to configure the management IP address, use the **hw-module module ip** command in privileged EXEC mode.

hw-module module 1 ip *ip_address netmask gateway*

Syntax Description

1	Specifies the slot number, which is always 1.
gateway	Specifies the gateway IP address.
ip_address	Specifies the management IP address.
netmask	Specifies the subnet mask.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Make sure this address is on the same subnet as the ASA VLAN IP address. For example, if you assigned 10.1.1.1 to the VLAN for the ASA, then assign another address on that network, such as 10.1.1.2, for the IPS management address.

If the management station is on a directly connected ASA network, then set the gateway to be the ASA IP address assigned to the IPS management VLAN. In the example decribed, set the gateway to 10.1.1.1. If the management station is on a remote network, then set the gateway to be the address of an upstream router on the IPS management VLAN.

Note These settings are written to the IPS application configuration, not the ASA configuration. You can view these settings from the ASA using the **show module details** command.You can alternatively use the IPS application **setup** command to configure this setting from the IPS CLI.

Examples

The following example shows how to configure a management address for the IPS module:

```
ciscoasa# hw-module module 1 ip 209.165.200.254
 255.255.255.224 209.165.200.225
```

Related Commands

Command	Description
hw-module module allow-ip	Configures the AIP SSC management host addresses.
show module	Shows module status information.

hw-module module password-reset

To reset the password for the default admin user on the hardware module to the default value, use the **hw-module module password-reset** command in privileged EXEC mode.

hw-module module 1 password-reset

Syntax Description

1	Specifies the slot number, which is always 1.

Command Default

The default username and password depends on your module:

- IPS module—username: **cisco**; password: **cisco**
- CSC module—username: **cisco**; password: **cisco**
- ASA CX module—username: **admin**; password: **Admin123**

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(2)	This command was added.
8.4(4.1)	Support for the ASA CX module was added.

Usage Guidelines

This command is only valid when the hardware module is in the Up state and supports password reset. For IPS, password reset is supported if the module is running IPS Version 6.0 or later. After resetting the password, you should change it to a unique value using the module application. Resetting the module password causes the module to reboot. Services are not available while the module is rebooting, which may take several minutes. You can run the **show module** command to monitor the module state.

The command always prompts for confirmation. If the command succeeds, no other output appears. If the command fails, an error message appears that explains why the failure occurred. The possible error messages are as follows:

```
Unable to reset the password on the module in slot 1
Unable to reset the password on the module in slot 1 - unknown module state
Unable to reset the password on the module in slot 1 - no module installed
Failed to reset the password on the module in slot 1 - module not in Up state
Unable to reset the password on the module in slot 1 - unknown module type
The module in slot 1 does not support password reset
```

```
Unable to reset the password on the module in slot 1 - no application found
The SSM application version does not support password reset
Failed to reset the password on the module in slot 1
```

Examples

The following example resets a password on a hardware module in slot 1:

```
ciscoasa(config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

Related Commands

Command	Description
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the module software.
hw-module module reset	Shuts down and resets the module hardware.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module recover

To load a recovery software image from a TFTP server to an installed module, or to configure network settings to access the TFTP server, use the **hw-module module recover** command in privileged EXEC mode. You might need to recover a module using this command if, for example, the module is unable to load a local image.

hw-module module 1 recover { **boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *module_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*] }

Syntax Description

1	Specifies the slot number, which is always 1.
boot	Initiates recovery of this module and downloads a recovery image according to the **configure** keyword settings. The module then reboots from the new image.
configure	Configures the network parameters to download a recovery image. If you do not enter a network parameter after the **configure** keyword, you are prompted for all parameters. This command prompts you for the URL for the TFTP server, the management interface IP address and netmask, gateway address, and VLAN ID. These network parameters are configured in ROMMON; the network parameters you configured in the module application configuration are not available to ROMMON, so you must set them separately here.
gateway *gateway_ip_address*	(Optional) The gateway IP address for access to the TFTP server through the SSM management interface.
ip *module_address*	(Optional) The IP address of the module management interface.
stop	Stops the recovery action, and stops downloading the recovery image. The module boots from the original image. You must enter this command within 30 to 45 seconds after starting recovery using the **hw-module module recover boot** command. If you issue the **stop** command after this period, it might cause unexpected results, such as the module becoming unresponsive.
url *tfp_url*	(Optional) The URL for the image on a TFTP server, in the following format: **tftp:**//*server*/[*path*/]*filename*
vlan *vlan_id*	(Optional) Specifies the VLAN ID for the management interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If the module suffers a failure, and the module application image cannot run, you can reinstall a new image on the module from a TFTP server.

Note Do not use the **upgrade** command within the module software to install the image.

Be sure the TFTP server that you specify can transfer files up to 60 MB in size. This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

This command is only available when the module is in the Up, Down, Unresponsive, or Recovery state. See the **show module** command for state information.

You can view the recovery configuration using the **show module 1 recover** command.

Note This command is not supported on these modules: ASA CX, ASA FirePOWER.

Examples

The following example sets the module to download an image from a TFTP server:

```
ciscoasa# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

The following example recovers the module:

```
ciscoasa# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
hw-module module reset	Shuts down a module and performs a hardware reset.
hw-module module reload	Reloads the module software.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module recover (ASA 5506W-X)

To load recover the default configuration or access ROMMON to load a new image on the wireless access point on a ASA 5506W-X, use the **hw-module module recover** command in privileged EXEC mode.

hw-module module wlan recover [**configuration** | **image**]

Syntax Description

configuration	Resets the wireless access point to the factory default configuration.
image	Sessions into the module console so you can access ROMMON and perform a TFTP upgrade procedure.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

The **image** keyword sessions to the access point CLI over the backplane and reloads the access point. When the access point boots, you can escape the boot process to access ROMMON and perform a TFTP image download. See Reloading the Access Point Image > Using the CLI for detailed steps.

Examples

The following example recovers an image on the access point:

```
ciscoasa# hw-module module wlan recover image
WARNING: Image recovery cannot be carried out via CLI command on this module.
Do you want to reset the module and session into the module console to carry out the image
 recovery?[confirm]
Resetting the module and sessioning into the module console
```

Related Commands

Command	Description
hw-module module wlan reset	Shuts down a module and performs a hardware reset.

hw-module module reload

To reload module software for a physical module, use the **hw-module module reload** command in privileged EXEC mode.

hw-module module 1 reload

Syntax Description

1	Specifies the slot number, which is always 1.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.4(4.1)	Support for the ASA CX module was added.
9.2(1)	Support for the ASA FirePOWER module was added.

Usage Guidelines

This command differs from the **hw-module module reset** command, which also performs a hardware reset before reloading the module.

This command is only valid when the module status is Up. See the **show module** command for state information.

Examples

The following example reloads the module in slot 1:

```
ciscoasa# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading. Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.

Command	Description
hw-module module reset	Shuts down a module and performs a hardware reset.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module reset

To reset the module hardware and then reload the module software, use the **hw-module module reset** command in privileged EXEC mode.

hw-module module { **1** | **wlan** } **reset**

Syntax Description

1	Specifies the slot number, which is always 1.
wlan	For the ASA 5506W-X, specifies the wireless access point.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.4(4.1)	Support for the ASA CX module was added.
9.2(1)	Support for the ASA FirePOWER module was added.
9.4(1)	The **wlan** keyword was added.

Usage Guidelines

When the module is in an Up state, the **hw-module module reset** command prompts you to shut down the software before resetting.

You can recover a module (if supported) using the **hw-module module recover** command. If you enter the **hw-module module reset** command while the module is in a Recover state, the module does not interrupt the recovery process. The **hw-module module reset** command performs a hardware reset of the module, and the module recovery continues after the hardware reset. You might want to reset the module during recovery if the module hangs; a hardware reset might resolve the issue.

This command differs from the **hw-module module reload** command, which only reloads the software and does not perform a hardware reset.

This command is only valid when the module status is Up, Down, Unresponsive, or Recover. See the **show module** command for state information.

Examples

The following example resets an module in slot 1 that is in the Up state:

```
ciscoasa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting. Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the module software.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module shutdown

To shut down the module software, use the **hw-module module shutdown** command in privileged EXEC mode.

hw-module module 1 shutdown

Syntax Description

1	Specifies the slot number, which is always 1.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.4(4.1)	Support for the ASA CX module was added.
9.2(1)	Support for the ASA FirePOWER module was added.

Usage Guidelines

Shutting down the module software prepares the module to be safely powered off without losing configuration data.

This command is only valid when the module status is Up or Unresponsive. See the **show module** command for state information.

Examples

The following example shuts down a module in slot 1:

```
ciscoasa# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
ciscoasa#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.

Command	Description
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the module software.
hw-module module reset	Shuts down a module and performs a hardware reset.
show module	Shows module information.