

W - Z

- wccp, on page 2
- wccp redirect, on page 4
- web-agent-url (Deprecated), on page 5
- web-applications, on page 7
- web-bookmarks, on page 9
- web update-type, on page 11
- web update-url, on page 13
- webvpn (global), on page 15
- webvpn (group-policy attributes, username attributes), on page 17
- whitelist, on page 20
- who, on page 22
- window-variation, on page 23
- wins-server, on page 25
- without-csd, on page 26
- write erase, on page 28
- write memory, on page 30
- write net, on page 32
- write standby, on page 34
- write terminal, on page 36
- xlate block-allocation, on page 38
- xlate per-session, on page 40
- zone, on page 43
- zonelabs-integrity fail-close, on page 45
- zonelabs-integrity fail-open, on page 47
- zonelabs-integrity fail-timeout, on page 49
- zonelabs-integrity interface, on page 51
- zonelabs-integrity port, on page 53
- zonelabs-integrity server-address, on page 55
- zonelabs-integrity ssl-certificate-port, on page 57
- zonelabs-integrity ssl-client-authentication, on page 59
- zone-member, on page 61

wccp

To allocate space and to enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **wccp** command in global configuration mode. To disable the service group and deallocate space, use the no form of this command.

wccp { **web-cache** | *service-number* } [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
no wccp { **web-cache** | *service-number* } [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]]

Syntax Description

access-list	Specifies the name of the access list.
group-list	(Optional) Access list that determines which web caches are allowed to participate in the service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
password	(Optional) Specifies Message Digest 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded.
password	Specifies the password to be used for authentication. The password argument can be up to seven characters in length.
redirect-list	(Optional) Used with an access list that controls traffic redirected to this service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list. The access list should only contain network addresses. Port-specific entries are not supported
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 254 and up to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the **web-cache** keyword.
web-cache	Specifies the web-cache service. **Note** Web cache counts as one service. The maximum number of services, including those assigned with the service-number argument, are 256.

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
7.2(1)	This command was added.

Examples

The following example shows how to enable WCCP for participation in a service group:

```
ciscoasa(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

wccp redirect

To enable packet redirection on the ingress of an interface using Web Cache Communication Protocol (WCCP), use the **wccp redirect** command. To disable WCCP redirection, use the no form of this command.

wccp interface *interface_name service* **redirect in**
no wccp interface *interface_name service* **redirect in**

Syntax Description

in	Specifies redirection when packet comes into this interface
interface_name	Name of the interface where packets should be redirected..
service	Specifies the service group. You can specify the **web-cache** keyword, or you can specify the identification number (from 0 to 99) of the service.

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
7.2(1)	This command was added.

Examples

The following example shows how to enable WCCP redirection on the inside interface for the web-cache service:

```
ciscoasa(config)# wccp interface inside web-cache redirect in
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp	Enables support of WCCP with service groups.

web-agent-url (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify the SSO server URL to which the ASA makes SiteMinder-type SSO authentication requests, use the **web-agent-url** command in config-webvpn-sso-siteminder mode.

To remove an SSO server authentication URL, use the **no** form of this command.

web-agent-url *url*
no web-agent-url *url*

Note This command is required for SiteMinder-type SSO authentication.

Syntax Description

url	Specifies the authentication URL of the SiteMinder-type SSO server. Must contain http:// or https://.

Command Default

By default, an authentication URL is 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
Config-webvpn-sso-siteminder	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single-sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The SSO server has a URL that handles authentication requests.

This command applies only to the SiteMinder type of SSO server.

Use the **web-agent-url** command to configure the ASA to send authentications to this URL. Before configuring the authentication URL, you must create the SSO server using the **sso-server** command.

For https communication between the security appliance and SSO-server, make sure that the SSL encryption settings match on both sides. On the security appliance, verify this with the **ssl encryption** command.

Examples

The following example, entered in config-webvpn-sso-siteminder mode, specifies an authentication URL of http://www.example.com/webvpn:

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
ciscoasa(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder-type SSO server.
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.
ssl encryption	Specifies the encryption algorithms the SSL/TLS protocol uses.
sso-server	Creates a single sign-on server.

web-applications

To customize the Web Application box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-applications** command from webvpn customization mode:

web-applications { **title | message | dropdown** } { **text | style** } *value*
[**no**] **web-applications** { **title | message | dropdown** } { **text | style** } *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

title	Specifies you are changing the title.
message	Specifies you are changing the message displayed under the title.
dropdown	Specifies you are changing the drop down box.
text	Specifies you are changing the text.
style	Specifies you are changing the HTML style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Command Default

The default title text is “Web Application”.

The default title style is background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text is “Enter Web Address (URL)”.

The default message style is background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is “Web 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	• Yes	—	• Yes	— s	—

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 “Applications”, and the color of the text to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-applications title text Applications
ciscoasa(config-webvpn-custom)# web-applications title 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.

web-bookmarks

To customize the Web Bookmarks title or links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-bookmarks** command from webvpn customization mode:

web-bookmarks { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }
[**no**] { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

link	Specifies you are changing the links.
title	Specifies you are changing the title.
style	Specifies you are changing the HTML style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 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 “Web 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	• 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 Web Bookmarks title to “Corporate Web Bookmarks”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-bookmarks title text Corporate Web 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.
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 update-type

To specify the address types (IPv4 or IPv6) that you want to update when using the DDNS Web update method, use the **web update-type** command in ddns update method configuration mode. To restore the default, use the **no** form of this command.

web update-type { **ipv4 | ipv6** [**all**] **| both** [**all**] }
no web update-type [**ipv4 | ipv6** [**all**] **| both** [**all**]]

Syntax Description

ipv4	Updates the IPv4 address.
ipv6	Updates the latest IPv6 address.
all	Updates all IPv6 addresses.
both	Updates the IPv4 address and the latest IPv6 address.

Command Default

The default is **both all** .

Command Modes

The 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 configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.15(1)	Command added.

Usage Guidelines

When an interface uses DHCP IP addressing, the assigned IP address can change when the DHCP lease is renewed. When the interface needs to be reachable using a fully qualified domain name (FQDN), the IP address change can cause the DNS server resource records (RRs) to become stale. Dynamic DNS (DDNS) provides a mechanism to update DNS RRs whenever the IP address or hostname changes. You can also use DDNS for static or PPPoE IP addressing.

DDNS updates the following RRs on the DNS server: the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names.

The ASA supports the following DDNS update methods: Standard DDNS (see the **ddns** command) and Web (using the **web update-url** command). The Web update method uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/). With this method when the IP address or hostname changes, the ASA sends an HTTP request directly to a DNS provider with which you have an account.

Examples

The following example configures the web type method and sets the IP address type to IPv4:

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>

  web update-type ipv4
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

Related Commands

Command	Description
ddns update	Associates a DDNS method with an interface.
ddns update hostname	Specifies the hostname for the interface.
ddns update method	Creates a DDNS update method.
interval maximum	Configures the update interface between DNS requests.
web update-url	Sets the DDNS update method to Web and sets the update URL.

web update-url

To specify the web update method for DDNS along with the web type URL, use the **web update-url** command in ddns update method configuration mode. To remove the method, use the **no** form of this command.

web update-url https: *//username:password@provider-domain/path* **?hostname=<h>&myip=<a>**
no web update-url https: *//username:password@provider-domain/path* **?hostname=<h>&myip=<a>**

Syntax Description

username	The username at the DDNS provider.
password	The password for this username.
provider-domain	The DDNS provider domain.
path	The path required at the DDNS domain. Check with your DDNS provider for the correct path.
?hostname=<h>&myip=<a>	Before entering the question mark (?) character, press the control (Ctrl) key and the v key together on your keyboard. This will allow you to enter the **?** without the software interpreting the **?** as a help query. Although these keywords look like arguments, you need to enter this text verbatim at the end of the URL. The ASA will automatically replace the <h> and <a> fields with the hostname and IP address when it sends the 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
Ddns update method configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.15(1)	Command added.

Usage Guidelines

When an interface uses DHCP IP addressing, the assigned IP address can change when the DHCP lease is renewed. When the interface needs to be reachable using a fully qualified domain name (FQDN), the IP address change can cause the DNS server resource records (RRs) to become stale. Dynamic DNS (DDNS)

provides a mechanism to update DNS RRs whenever the IP address or hostname changes. You can also use DDNS for static or PPPoE IP addressing.

DDNS updates the following RRs on the DNS server: the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names.

The ASA supports the following DDNS update methods: Standard DDNS (see the **ddns** command) and Web (using the **web update-url** command). The Web update method uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/). With this method when the IP address or hostname changes, the ASA sends an HTTP request directly to a DNS provider with which you have an account.

You can also specify the address types (IPv4 or IPv6) that you want to update using the **web update-type** command.

The web method for DDNS also requires you to identify the DDNS server root CA to validate the DDNS server certificate for the HTTPS connection. For example:

```
crypto ca trustpoint DDNS_Trustpoint
   enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

Examples

The following example configures the web type method:

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

Related Commands

Command	Description
ddns update	Associates a DDNS method with an interface.
ddns update hostname	Specifies the hostname for the interface.
ddns update method	Creates a DDNS update method.
interval maximum	Configures the update interface between DNS requests.
web update-type	Specifies the address types (IPv4 or IPv6) that you want to update.

webvpn (global)

To enter webvpn mode, in global configuration mode, enter the **webvpn** command. To remove any commands entered with this command, use the **no webvpn** command. These **webvpn** commands apply to all WebVPN users.

These **webvpn** commands let you configure AAA servers, default group policies, default idle timeout, http and https proxies, and NBNS servers for WebVPN, as well as the appearance of WebVPN screens that end users see.

webvpn
no webvpn

Syntax Description

This command has no arguments or keywords.

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
Global configuration	• 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 WebVPN mode lets you configure global settings for WebVPN. WebVPN mode, which you enter from either group-policy mode or username mode, lets you customize a WebVPN configuration for specific users or group policies. The ASA clientless SSL VPN configuration supports only one http-proxy and one https-proxy command each.



Note You must enable browser caching for WebVPN to work.

Examples

The following example shows how to enter WebVPN command mode:

```
ciscoasa
(config)#
 webvpn
```

```
ciscoasa
(config-webvpn)#
```

webvpn (group-policy attributes, username attributes)

To enter this webvpn mode, use the **webvpn** command in group-policy attributes configuration mode or in username attributes configuration mode. To remove all commands entered in webvpn mode, use the **no** form of this command. These webvpn commands apply to the username or group policy from which you configure them.

Webvpn commands for group policies and usernames define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter.

webvpn
no webvpn

Syntax Description

This command has no arguments or keywords.

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
Group-policy attributes configuration	Yes	—	Yes	—	—
Username attributes configuration	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

Webvpn mode, which you enter from global configuration mode, lets you configure global settings for WebVPN. The **webvpn** command in group-policy attributes configuration mode or username attributes configuration mode applies the settings specified in the webvpn command to the group or user specified in the parent command. In other words, entering webvpn mode from group-policy or username mode enables you customize a WebVPN configuration for specific users or group policies.

The webvpn attributes applied to a specific group policy in group-policy attributes mode override those specified in the default group policy. The WebVPN attributes applied to a specific user in username attributes mode override both the settings in the default group policy and those in the group policy assigned to that user. Essentially, these commands allow you adjust the settings that would otherwise be inherited from the default

group or a specified group policy. For information about WebVPN settings, refer to the **webvpn** command in global configuration mode.

Note The **keepout** command is supported only in the global webvpn configuration context. This command is not supported in the group-policy attributes or username attributes configuration modes.

The following table lists the attributes you can configure in webvpn group-policy attributes and username attributes mode. See the individual command descriptions for details.

Attribute	Description
auto-signon	Configures the ASA to automatically pass WebVPN user login credentials on to internal servers, providing a single sign-on method for WebVPN users.
customization	Specifies a preconfigured WebVPN customization to apply.
deny-message	Specifies a message to display to the user when access is denied.
filter	Identifies the access list to be used for WebVPN connections.
functions	Configures file access and file browsing, MAPI Proxy, and URL entry over WebVPN.
homepage	Sets the URL of the web page that displays when WebVPN users log in.
html-content-filter	Identifies Java, ActiveX, images, scripts, and cookies to filter for WebVPN sessions.
http-comp	Specifies the HTTP compression algorithm to use.
keep-alive-ignore	Specifies the maximum object size to ignore for updating the session.
port-forward	Enables WebVPN application access.
port-forward-name	Configures the display name that identifies TCP port forwarding to end users.
sso-server	Configures the SSO server name.
svc	Configures SSL VPN Client attributes.
url-list	Identifies a list of servers and URLs that users can access via WebVPN.

Examples

The following example shows how to enter webvpn mode for the group policy named “FirstGroup”:

```
ciscoasa
(config)#
group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-webvpn)#
```

The following example shows how to enter webvpn mode for the username named “test”:

```
ciscoasa
```

```
(config)#
group-policy test attributes
ciscoasa
(config-username)#
 webvpn
ciscoasa(config-webvpn)#
```

Related Commands

clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy attributes	Enters config-group-policy mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn 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 config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

whitelist

For Cloud Web Security, to perform the whitelist action on the class of traffic, use the **whitelist** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map type inspect scansafe** command, then the **parameters** command. To disable whitelisting, use the **no** form of this command.

whitelist
no 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
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Identify the traffic you want to whitelist using the **class-map type inspect scansafe** command. Use the inspection class map in the **policy-map type inspect scansafe** command, and specify the **whitelist** action for the class. Call the inspection policy map in the **inspect scansafe** command.

Examples

The following example whitelists the same users and groups for the HTTP and HTTPS inspection policy maps:

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
```

```
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

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.
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.

who

To display active Telnet administration sessions on the ASA, use the **who** command in privileged EXEC mode.

who [*local_ip*]

Syntax Description

local_ip	(Optional) Specifies to limit the listing to one internal IP address or network address, 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **who** command allows you to display the TTY_ID and IP address of each Telnet client that is currently logged into the ASA.

Examples

This example shows the output of the **who** command when a client is logged into the ASA through a Telnet session:

```
ciscoasa# who
0: 100.0.0.2
ciscoasa# who 100.0.0.2
0: 100.0.0.2
ciscoasa#
```

Related Commands

Command	Description
kill	Terminate a Telnet session.
telnet	Adds Telnet access to the ASA console and sets the idle timeout.

window-variation

To drop a connection with a window size variation, use the **window-variation** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

window variation { **allow-connection | drop-connection** }
no window variation { **allow-connection | drop-connection** }

Syntax Description

allow-connection	Allows the connection.
drop-connection	Drops the connection.

Command Default

The default action is to allow the connection.

Command Modes

The 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 **window-variation** command in tcp-map configuration mode to drop all connections with a window size that has been shrunk.

The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without having accepted too much data. From the TCP specification, “shrinking the window” is strongly discouraged. When this condition is detected, the connection can be dropped.

Examples

The following example shows how to drop all connections with a varied window size:

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# window-variation drop-connection
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.
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.

wins-server

To set the IP address of the primary and secondary WINS servers, use the **wins-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a WINS server from another group policy. To prevent inheriting a server, use the **wins-server none** command.

wins-server value { *ip_address* } [*ip_address*] | **none**
no wins-server

Syntax Description

none	Sets wins-servers to a null value, thereby allowing no WINS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary WINS 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

Every time you issue the **wins-server** command you overwrite the existing setting. For example, if you configure WINS server x.x.x.x and then configure WINS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole WINS server. The same holds true for multiple servers. To add a WINS server rather than overwrite previously configured servers, include the IP addresses of all WINS servers when you enter this command.

Examples

The following example shows how to configure WINS servers with the IP addresses 10.10.10.15, 10.10.10.30, and 10.10.10.45 for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

without-csd

To exempt certain users from running the Hostscan application of Cisco Secure Desktop on a per connection profile basis if they enter one of the entries in the group-urls table to establish the VPN session, use the **without-csd** command in tunnel webvpn configuration mode. To remove this command from the configuration, use the **no** form of the command.

without-csd [**anyconnect**]
no without-csd [**anyconnect**]

Syntax Description

anyconnect	(Optional) Changes the command to affect only AnyConnect connections.

Command Default

No default values. If installed, Hostscan 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
Tunnel webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.2(1)	The **anyconnect** keyword was added.

Usage Guidelines

This command prevents the Hostscan application of Cisco Secure Desktop from running on the endpoint if the user enters a URL in the url-group list configured on this connection profile (called a tunnel group in the CLI). Entering this command prevents the detection of endpoint conditions for these sessions, so you may need to adjust the dynamic access policy (DAP) configuration.

Examples

The first command in the following example creates a group-url in which “example.com” is the domain of the ASA and “no-csd” is the unique portion of the URL. When the user enters this URL, the ASA assigns this connection profile to the session. The **group-url** command is required for the **without-csd** command to have an effect. The **without-csd** command exempts the user from running Cisco Secure Desktop.

```
ciscoasa(config-tunnel-webvpn)# group-url https://example.com/no-csd enable
ciscoasa(config-tunnel-webvpn)# without-csd
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
csd enable	Enables Cisco Secure Desktop for all connection profiles that do not have a without-csd command.
csd image	Copies the Cisco Secure Desktop image named in the command, from the flash drive specified in the path to the running configuration.
group-url	Creates a group-url unique to this connection profile.

write erase

To erase the startup configuration, use the **write erase** command in privileged EXEC mode. The running configuration remains intact.

write erase

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

This command is not supported within a security context. Context startup configurations are identified by the config-url command in the system configuration. If you want to delete a context configuration, you can remove the file manually from the remote server (if specified) or clear the file from Flash memory using the **delete** command in the system execution space.

For the ASA Virtual, this command restores the deployment configuration (the initial virtual deployment settings) after a **reload**. To erase the configuration completely, use the **clear configure all** command. To erase the deployment configuration and apply the same factory default configuration as for the ASA appliances, see **configure factory-default**.



Note The ASA Virtual boots the current running image, so you are not reverted to the original boot image.Do not save the configuration before you reload.

For the ASA Virtual in a failover pair, first power off the standby unit. To prevent the standby unit from becoming active, you must power it off. If you leave it on, when you erase the active unit configuration, then the standby unit becomes active. When the former active unit reloads and reconnects over the failover link, the old configuration will sync from the new active unit, wiping out the deployment configuration you wanted. After the active unit reloads, you can power on the standby unit. The deployment configuration will then sync to the standby unit.

Examples

The following example erases the startup configuration:

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm] y
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
delete	Removes a file from Flash memory.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

write memory

To save the running configuration to the startup configuration, use the **write memory** command in privileged EXEC mode.

write memory [**all** [**/noconfirm**]]

Syntax Description

/noconfirm	Eliminates the confirmation prompt when you use the **all** keyword.
all	From the system execution space in multiple context mode, this keyword saves all context configurations as well as the system 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	You can now save all context configurations with the **all** keyword.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line. Changes are only preserved between reboots if you save them to the startup configuration, which is the configuration loaded into running memory at startup. The location of the startup configuration for single context mode and for the system in multiple context mode can be changed from the default location (a hidden file) to a location of your choosing using the **boot config** command. For multiple context mode, a context startup configuration is at the location specified by the **config-url** command in the system configuration.

In multiple context mode, you can enter the **write memory** command in each context to save the current context configuration. To save all context configurations, enter the **write memory all** command in the system execution space. Context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server specified by the **config-url** command, except for HTTP and HTTPS URLs, which do not allow you to save the configuration back to the server. After the ASA saves each context with the **write memory all** command, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

```
The context 'context a' could not be saved due to Unavailability of resources
```

- For contexts that are not saved because the remote destination is unreachable, the following message appears:

```
The context 'context a' could not be saved due to non-reachability of destination
```

- For contexts that are not saved because the context is locked, the following message appears:

```
Unable to save the configuration for the following contexts as these contexts are locked.
context ‘a’ , context ‘x’ , context ‘z’ .
```

A context is only locked if another user is already saving the configuration or in the process of deleting the context.

- For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:

```
Unable to save the configuration for the following contexts as these contexts have read-only
 config-urls:
context ‘a’ , context ‘b’ , context ‘c’ .
```

- For contexts that are not saved because of bad sectors in the Flash memory, the following message appears:

```
The context 'context a' could not be saved due to Unknown errors
```

Because the system uses the admin context interfaces to access context startup configurations, the **write memory** command also uses the admin context interfaces. The **write net** command, however, uses the context interfaces to write a configuration to a TFTP server.

The **write memory** command is equivalent to the **copy running-config startup-config** command.

Examples

The following example saves the running configuration to the startup configuration:

```
ciscoasa# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454
19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
ciscoasa#
```

Related Commands

Command	Description
admin-context	Sets the admin context.
configure memory	Merges the startup configuration with the running configuration.
config-url	Specifies the location of the context configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
write net	Copies the running configuration to a TFTP server.

write net

To save the running configuration to a TFTP server, use the **write net** command in privileged EXEC mode.

write net [*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 **write 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 your TFTP server does not support this type of URL, use the **copy running-config tftp** command instead. If you specified the TFTP server address using the **tftp-server** command, you can enter the filename alone preceded by a colon (:).
server **:**	Sets the TFTP server IP address or name. This address overrides the address you set in the **tftp-server** command, if present. 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line.

In multiple context mode, this command saves only the current configuration; you cannot save all contexts with a single command. You must enter this command separately for the system and for each context. The **write net** command uses the context interfaces to write a configuration to a TFTP server. The **write memory** command, however, uses the admin context interfaces to save to the startup configuration because the system uses the admin context interfaces to access context startup configurations.

The **write net** command is equivalent to the **copy running-config tftp** command.

Examples

The following example sets the TFTP server and filename in the **tftp-server** command:

```
ciscoasa# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
ciscoasa# write net
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command is not populated.

```
ciscoasa# write net 10.1.1.1:/configs/contextbackup.cfg
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command supplies the directory name, and the server address is overridden.

```
ciscoasa# tftp-server 10.1.1.1 configs
ciscoasa# write net 10.1.2.1:context.cfg
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
copy running-config tftp	Copies the running configuration to a TFTP server.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write memory	Saves the running configuration to the startup configuration.

write standby

To copy the ASA or context running configuration to the failover standby unit, use the **write standby** command in privileged EXEC mode.

write 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	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You should only use this command if the configuration on the standby unit or failover group becomes out-of-sync with the configuration of the active unit or failover group. This typically happens when commands are entered on the standby unit or failover group directly.

For Active/Standby failover, the **write standby** command entered on the active unit writes the running configuration of the active failover unit to the running configuration on the standby unit.

For Active/Active failover, the **write standby** command behaves as follows:

- If you enter the **write standby** command in the system execution space, the system configuration and the configurations for all of the security contexts on the ASA are written to the peer unit. This includes configuration information for security contexts that are in the standby state. You must enter the command in the system execution space on the unit that has failover group 1 in the active state.
- If you enter the **write standby** command in a security context, only the configuration for the security context is written to the peer unit. You must enter the command in the security context on the unit where the security context appears in the active state.

The **write standby** command replicates the configuration to the running configuration of the peer unit; it does not save the configuration to the startup configuration. To save the configuration changes to the startup configuration, use the **copy running-config startup-config** command on the same unit that you entered the **write standby** command. The command will be replicated to the peer unit and the configuration saved to the startup configuration.

When Stateful Failover is enabled, the **write standby** command also replicates state information to the standby unit after the configuration replication is complete. In multiple context mode, enter **write standby** within the context to replicate state information.



Note After you enter the write standby command, the failover interfaces will go down momentarily while the configuration becomes re-synchronized. This can also cause a temporary failure of the failover state interface to be detected.

Examples

The following example writes the current running configuration to the standby unit:

```
ciscoasa# write standby
Building configuration...
[OK]
ciscoasa#
```

Related Commands

Command	Description
failover reload-standby	Forces the standby unit to reboot.

write terminal

To show the running configuration on the terminal, use the **write terminal** command in privileged EXEC mode.

write 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 is equivalent to the show running-config command.

Examples

The following example writes the running configuration to the terminal:

```
ciscoasa# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.

Command	Description
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

xlate block-allocation

To configure the port block allocation characteristics for carrier-grade or large-scale PAT, use the **xlate block-allocation** command in global configuration mode. To return to default values, use the **no** form of this command.

xlate block-allocation { **size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds* }
no xlate block-allocation { **size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds* }

Syntax Description

size *value*	The block allocation size, which is the number of ports in each block. The range is 32-4096. The default is 512. If you do not use the default, ensure that the size you choose divides evenly into 64,512 (the number of ports in the 1024-65535 range). Otherwise, there will be ports that cannot be allocated. For example, if you specify 100, there will be 12 unused ports.
maximum-per-host *number*	The maximum blocks that can be allocated per host. The limit is per protocol, so a limit of 4 means at most 4 UDP blocks, 4 TCP blocks, and 4 ICMP blocks per host. The range is 1-8, the default is 4.
pba-interim-logging *seconds*	Enable interim logging. By default, the system generates syslog messages during port block creation and deletion. If you enable interim logging, the system generates message 305017 at the interval you specify. The messages report all active port blocks allocated at that time, including the protocol (ICMP, TCP, UDP) and source and destination interface and IP address, and the port block. You can specify an interval from 21600-604800 seconds (6 hours to 7 days).

Command Default

The default allocation size is 512. The default per-host maximum is 4.

Command Modes

The following table shows the modes 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(1)	This command was added.
9.12(1)	The **pba-interim-logging** command was added.

Usage Guidelines

For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). If you allocate a block of ports, subsequent connections from the host use new randomly-selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Blocks are freed when the last xlate that uses a port in the block is removed.

Port blocks are allocated in the 1024 - 65535 range only. Thus, if an application requires a low port number (1 - 1023), it might not work. For example, an application requesting port 22 (SSH) will get a mapped port within the range of 1024-65535 and within the block allocated to the host.

The **xlate block-allocation** command configures the characteristics of these port blocks. Use the block-allocation keyword on the **nat** command to enable port block allocation per PAT rule when using a PAT pool.

As with all NAT changes, if you replace an existing rule with one that uses port block allocation, you must clear xlates related to the replaced rule to have the new rule take effect. You can clear them explicitly or simply wait for them to time out. However, when operating in a cluster, you must reload the cluster so that the units can distribute blocks correctly.

If you are switching between a regular PAT and block allocation PAT rule, for object NAT, you must first delete the rule, then clear xlates. You can then create the new object NAT rule. Otherwise, you will see pat-port-block-state-mismatch drops in the **show asp drop** output.

Examples

The following example changes the port block allocation characteristics and implements port block allocation for a PAT pool in an object NAT rule:

```
xlate block-allocation size 128
xlate block-allocation maximum-per-host 6
xlate block-allocation pba-interim-logging 21600
object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_host
   host 10.111.10.15
object network src_host
   nat dynamic pat-pool mapped-pat-pool block-allocation
```

Related Commands

Command	Description
nat (global)	Adds a twice NAT rule.
nat (object)	Adds an object NAT rule.
show local-host	Shows the port blocks allocated to hosts.
show running-config xlate	Shows the **xlate** configuration.

xlate per-session

To use multi-session PAT, use the **xlate per-session** command in global configuration mode. To remove a multi-session PAT rule, use the **no** form of this command.

xlate per-session { **permit | deny** } { **tcp | udp** } *source_ip* [*operator src_port*] *destination_ip operator dest_port*
no xlate per-session { **permit | deny** } { **tcp | udp** } *source_ip* [*operator src_port*] *destination_ip operator dest_port*

Syntax Description

deny	Creates a deny rule.
destination_ip	For the destination IP address, you can configure the following: • **host** *ip_address* —Specifies an IPv4 host address. • *ip_address mask* —Specifies an IPv4 network address and subnet mask. • *ipv6-address/prefix-length* —Specifies an IPv6 host or network address and prefix. • **any4** and **any6**—**any4** specifies only IPv4 traffic; and **any6** specifies any6 traffic.
operator dest_port	The *operator* matches the port numbers used by the destination. The permitted operators are as follows: • 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`
operator src_port	(Optional) The *operator* matches the port numbers used by the source. The permitted operators are as follows: • 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`

permit	Creates a permit rule.
source_ip	For the source IP address, you can configure the following: • **host** *ip_address* —Specifies an IPv4 host address. • *ip_address mask* —Specifies an IPv4 network address and subnet mask. • *ipv6-address/prefix-length* —Specifies an IPv6 host or network address and prefix. • **any4** and **any6**—**any4** specifies only IPv4 traffic; and **any6** specifies any6 traffic.
tcp	Specifies TCP traffic.
udp	Specifies UDP traffic.

Command Default

By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. The following default rules are installed:

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

You cannot remove these rules, and they always exist after any manually-created rules. Because rules are evaluated in order, you can override the default rules. For example, to completely negate these rules, you could add the following deny rules:

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq 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
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The per-session PAT feature improves the scalability of PAT and, for clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For "hit-and-run" traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address. Without the per-session feature, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With the per-session feature, the connection rate for one address for an IP protocol is 65535/*average-lifetime* .

By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. For traffic that can benefit from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT be creating a per-session deny rule.

When you add a per-session PAT rule, the rule is placed above the default rules, but below any other manually-created rules. Be sure to create your rules in the order you want them applied.

Examples

The following example creates a deny rule for H.323 traffic, so that it uses multi-session PAT:

```
ciscoasa(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
ciscoasa(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

Related Commands

Command	Description
clear configure xlate	Clears the **xlate per-session** rules.
nat (global)	Adds a twice NAT rule.
nat (object)	Adds an object NAT rule.
show running-config xlate	Shows the **xlate per-session** rules.

zone

To add a traffic zone, use the **zone** command in global configuration mode. To remove the zone, use the **no** form of this command.

zone *name*
no zone *name*

Syntax Description

name	Sets the zone name up to 48 characters in length.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes 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
9.3(2)	This command was added.

Usage Guidelines

You can assign multiple interfaces to a *traffic zone* , which lets traffic from an existing flow exit or enter the ASA on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the ASA as well as external load balancing of traffic to the ASA across multiple interfaces.

Zones allow traffic to and from any interface in the zone, but the security policy itself (access rules, NAT, and so on) is still applied per interface, not per zone. If you configure the same security policy for all interfaces within the zone, then you can successfully implement ECMP and load balancing for that traffic.

You can create a maximum of 256 zones.

Examples

The following example configures an outside zone with 4 member interfaces:

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

Related Commands

Command	Description
clear configure zone	Clears the zone configuration.
clear conn zone	Clears zone connections.
clear local-host zone	Clears zone hosts.
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.
show asp table zone	Shows the accelerated security path tables for debugging purposes.
show conn long	Shows connections information for zones.
show local-host zone	Shows the network states of local hosts within a zone.
show nameif zone	Shows the interface names and zone names.
show route zone	Shows the routes for zone interfaces.
show running-config zone	Shows the zone configuration.
show zone	Shows zone ID, context, security level, and members.
zone	Configures a traffic zone.
zone-member	Assigns an interface to a traffic zone.

zonelabs-integrity fail-close

To configure the ASA so that connections to VPN clients close when the connection between the ASA and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command in global configuration mode.To reinstate the default whereby the VPN connections remain open on failure of the Zone Labs connection, use the **no** form of this command.

zonelabs-integrity fail-close
no zonelabs-integrity fail-close

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the connection remains open on failure.

Command Modes

The following table shows the 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.

Usage Guidelines

If the primary Zone Labs Integrity Firewall Server does not respond to the ASA, the ASA still establishes VPN client connections to the private network by default. It also maintains open, existing connections. This ensures that the enterprise VPN is not disrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command.

To return to the default condition whereby the ASA maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command.

Examples

The following example configures the ASA to close the VPN client connections if the Zone Labs Integrity Firewall Server fails to respond or if the connection is interrupted:

```
ciscoasa(config)# zonelabs-integrity fail-close
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-open	Specifies that VPN client connections to the ASA remain open after the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-timeout	Specifies the time in seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.

zonelabs-integrity fail-open

To keep remote VPN client connections to the ASA open after the connection between the ASA and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command in global configuration mode. To close connections to VPN clients upon failure of the Zone Labs server connection, use the **no** form of this command.

zonelabs-integrity fail-open
no zonelabs-integrity fail-open

Syntax Description

This command has no arguments or keywords.

Command Default

By default, remote VPN connections remain open if the ASA does not establish or maintain a connection to the Zone Labs Integrity Firewall 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	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If the primary Zone Labs Integrity Firewall Server does not respond to the ASA, the ASA still establishes VPN client connections to the private network by default. It also maintains existing open connections. This ensures that the enterprise VPN is not disrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command. To then return to the default condition whereby the ASA maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command or the **no zonelabs-integrity fail-open** command.

Examples

The following example reinstates the default condition whereby the VPN client connections remain open if the connection to the Zone Labs Integrity Firewall Server fails:

```
ciscoasa(config)# zonelabs-integrity fail-open
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the ASA close VPN client connections when the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-timeout	Specifies the time in seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.

zonelabs-integrity fail-timeout

To specify the time in seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Server unreachable, use the **zonelabs-integrity fail-timeout** command in global configuration mode. To restore the default timeout of 10 seconds, use the **no** form of this command without an argument.

zonelabs-integrity fail-timeout *timeout*
no zonelabs-integrity fail-timeout

Syntax Description

timeout	The number of seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Servers unreachable. The acceptable range is from 5 to 20 seconds.

Command Default

The default timeout value 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If the ASA waits for the specified number of seconds without a response from the Zone Labs server, the server is declared nonresponsive. Connections to VPN clients either remain open by default or if configured to do so with the **zonelabs-integrity fail-open** command. If, however, the **zonelabs-integrity fail-close** command has been issued, the connections will close when the ASA declares the Integrity server unresponsive.

Examples

The following example configures the ASA to declare the active Zone Labs Integrity Server to be unreachable after 12 seconds:

```
ciscoasa(config)# zonelabs-integrity fail-timeout 12
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-open	Specifies that VPN client connections to the ASA remain open after the connection between the ASA and the Zone Labs Integrity Firewall Server fails.

Command	Description
zonelabs-integrity fail-close	Specifies that the ASA close VPN client connections when the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.

zonelabs-integrity interface

To specify an ASA interface for communication with the Zone Labs Integrity Server, use the **zonelabs-integrity interface** command in global configuration mode. To reset the Zone Labs Integrity Firewall Server interface back to the default of none, use the **no** form of this command.

zonelabs-integrity interface *interface*
no zonelabs-integrity interface

Syntax Description

interface	Specifies the ASA interface on which the Zone Labs Integrity Firewall Server communicates. It is often an interface name created with the **nameif** command.

Command Default

By default, the Zone Labs Integrity Firewall Server interface is set to 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example configures three Zone Labs Integrity Servers using IP addresses ranging from 10.0.0.5 to 10.0.0.7. The commands also configure the ASA to listen to the server on port 300 and on an interface called inside:

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)# zonelabs-integrity interface inside
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.

Command	Description
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity port

To specify a port on the ASA for communicating with a Zone Labs Integrity Firewall Server, use the **zonelabs-integrity port** command in global configuration mode. To revert to the default port of 5054 for the Zone Labs Integrity Firewall Server, use the **no** form of this command.

zonelabs-integrity port *port_number*
no zonelabs-integrity port *port_number*

Syntax Description

port	Specifies a Zone Labs Integrity Firewall Server port on the ASA.
port_number	The number of the Zone Labs Integrity Firewall Server port. It can range from 10 to 10000.

Command Default

The default Zone Labs Integrity Firewall Server port is 5054.

Command Modes

The following table shows the 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.

Usage Guidelines

The ASA listens to the Zone Labs Integrity Firewall Server on the port and interface configured with the **zonelabs-integrity port** and **zonelabs-integrity interface** commands respectively.

Note The current release of the ASA supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the ASA and then reestablish the client VPN session.

Examples

The following example configures a Zone Labs Integrity Servers using the IP address 10.0.0.5. The commands also configure the ASA to listen to the active Zone Labs server on port 300 instead of the default 5054 port:

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity server-address

To add Zone Labs Integrity Firewall Servers to the ASA configuration, use the **zonelabs-integrity server-address** command in global configuration mode. Specify the Zone Labs server by either IP address or hostname.

To remove Zone Labs Integrity Firewall Servers from the running configuration, use the **no** form of this command without arguments.

zonelabs-integrity server-address { *hostname1* | *ip-address1* }
no zonelabs-integrity server-address

Note While the user interfaces appear to support the configuration of multiple Integrity Servers, the ASA only supports one server at a time in the current release.

Syntax Description

hostname	Specifies the hostname of the Zone Labs Integrity Firewall Server. See the **name** command for hostname guidelines.
ip-address	Specifies the IP address of the Zone Labs Integrity Firewall Server.

Command Default

By default, no Zone Labs Integrity Firewall Servers 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

With this release, you can configure one Zone Labs Integrity Firewall Server. If that server fails, configure another Integrity Server first and then reestablish the client VPN session.

To specify a server by hostname, you must first configure the Zone Labs server name using the **name** command. Before using the **name** command, use the **names** command to enable it.

Note The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the ASA and then reestablish the client VPN session.

Examples

The following example assigns the server name ZL-Integrity-Svr to the IP address 10.0.0.5 and configures a Zone Labs Integrity Server using that name:

```
ciscoasa(config)# names
ciscoasa(config)# name 10.0.0.5 ZL-Integrity-Svr
ciscoasa(config)# zonelabs-integrity server-address ZL-Integrity-Svr
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the ASA close VPN client connections when the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity ssl-certificate-port

To specify an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate, use the **zonelabs-integrity ssl-certificate-port** command in global configuration mode. To revert to the default port number (80), use the **no** form of this command without an argument.

zonelabs-integrity ssl-certificate-port *cert-port-number*
no zonelabs-integrity ssl-certificate-port

Syntax Description

cert-port-number	Specifies a port number on which the ASA expects the Zone Labs Integrity Firewall Server to connect when requesting an SSL certificate.

Command Default

By default, the ASA expects the Zone Labs Integrity Firewall Server to request an SSL certificate on port 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

For SSL communications between the ASA and the Zone Labs Integrity Firewall Server, the ASA is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (ASA) must be authenticated by the client (Zone Labs server). The **zonelabs-integrity ssl-certificate-port** command specifies the port to which the Zone Labs server connects when requesting the SSL server certificate.

Examples

The following example configures port 30 on the ASA to receive SSL certificate requests from the Zone Labs Integrity Server:

```
ciscoasa(config)# zonelabs-integrity ssl-certificate-port 30
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.

Command	Description
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity ssl-client-authentication

To enable authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA, use the **zonelabs-integrity ssl-client-authentication** command in global configuration mode with the *enable* argument. To disable authentication of the Zone Labs SSL certificate, use the *disable* argument or use the **no** form of this command without an argument.

zonelabs-integrity ssl-client-authentication { *enable* | *disable* }
no zonelabs-integrity ssl-client-authentication

Syntax Description

disable	Specifies the IP address of the Zone Labs Integrity Firewall Server.
enable	Specifies that the ASA authenticates the SSL certificate of the Zone Labs Integrity Firewall Server.

Command Default

By default, ASA authentication of the Zone Labs Integrity Firewall Server SSL certificate 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
7.2(1)	This command was added.

Usage Guidelines

For SSL communications between the ASA and the Zone Labs Integrity Firewall Server, the ASA is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (ASA) must be authenticated by the client (Zone Labs server). Authentication of the client certificate is optional, however. You use the **zonelabs-integrity ssl-client-authentication** command to enable or disable ASA authentication of the Zone Lab server (SSL client) certificate.

Examples

The following example configures the ASA to authenticate the SSL certificate of the Zone Labs Integrity Server:

```
ciscoasa(config)# zonelabs-integrity ssl-client-authentication enable
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.

zone-member

To add an interface to a traffic zone, use the **zone-member** command in interface configuration mode. To remove the interface, use the **no** form of this command.

zone-member *name*
no zone-member *name*

Syntax Description

name	Identifies the zone name set by the **zone** 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
9.3(2)	This command was added.

Usage Guidelines

Configure all interface parameters including the name, IP address, and security level. The first interface that you add to a zone determines the security level of the zone. All additional interfaces must have the same security level. To change the security level for interfaces in a zone, you must remove all but one interface, and then change the security levels, and re-add the interfaces.

When you assign an interface to a zone, any connections on that interface are deleted. The connections must be reestablished.

If you remove an interface from a zone, any connections that have the interface as the primary interface are deleted. The connections must be reestablished. If the interface is the current interface, the ASA moves the connections back to the primary interface. The zone route table is also refreshed.

You can add the following types of interfaces to a zone:

- Physical
- VLAN
- EtherChannel
- Redundant

You cannot add the following types of interfaces:

- Management-only
- Management-access
- Failover or state link
- Cluster control link
- Member interfaces in an EtherChannel or redundant interface

An interface can be a member of only one zone.

You can include up to 8 interfaces per zone.

Examples

The following example configures an outside zone with 4 member interfaces:

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

Related Commands

Command	Description
clear configure zone	Clears the zone configuration.
clear conn zone	Clears zone connections.
clear local-host zone	Clears zone hosts.
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.
show asp table zone	Shows the accelerated security path tables for debugging purposes.
show conn long	Shows connections information for zones.
show local-host zone	Shows the network states of local hosts within a zone.
show nameif zone	Shows the interface names and zone names.
show route zone	Shows the routes for zone interfaces.
show running-config zone	Shows the zone configuration.
show zone	Shows zone ID, context, security level, and members.
zone	Configures a traffic zone.
zone-member	Assigns an interface to a traffic zone.