

mf – mz

- mfib forwarding, on page 2
- migrate, on page 3
- min-object-size, on page 5
- mkdir, on page 7
- mobile-device portal, on page 9
- mode, on page 10
- monitor-interface, on page 12
- more, on page 14
- mount type cifs, on page 17
- mount type ftp, on page 19
- mroute, on page 21
- mschapv2-capable, on page 23
- msie-proxy except-list, on page 25
- msie-proxy local-bypass, on page 27
- msie-proxy lockdown, on page 28
- msie-proxy method, on page 30
- msie-proxy pac-url, on page 32
- msie-proxy server, on page 34
- mtu, on page 36
- mtu cluster, on page 38
- multicast boundary, on page 40
- multicast-routing, on page 42
- mus, on page 44
- mus host, on page 46
- mus password, on page 48
- mus server, on page 50

mfib forwarding

To reenable MFIB forwarding on an interface, use the **mfib forwarding** command in interface configuration mode. To disable MFIB forwarding on an interface, use the **no** form of this command.

mfibforwarding
nomfibforwarding

Syntax Description

This command has no arguments or keywords.

Command Default

The **multicast-routing** command enables MFIB forwarding on all interfaces 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
7.1(1)	This command was added.

Usage Guidelines

When you enable multicast routing, MFIB forwarding is enabled on all interfaces by default. Use the **no** form of the command to disable MFIB forwarding on a specific interface. Only the **no** form of the command appears in the running configuration.

When MFIB forwarding is disabled on an interface, the interface does not accept any multicast packets unless specifically configured through other methods. IGMP packets are also prevented when MFIB forwarding is disabled.

Examples

The following example disables MFIB forwarding on the specified interface:

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing.
pim	Enables PIM on an interface.

migrate

To migrate a LAN-to-LAN (IKEv1) or remote access configuration (SSL or IKEv1) to IKEv2, use the migrate command from global configuration mode:

migrate { **l2l** | **remote-access** { **ikev2** | **ssl** } | **overwrite** }

Syntax Description

l2l	Migrates the IKEv1 LAN-to-LAN configuration to IKEv2.
remote-access	Specifies remote access configuration.
ikev2	Migrates the remote access IKEv1 configuration to IKEv2.
ssl	Migrates the remote access SSL configuration to IKEv2.
overwrite	Overwrites existing IKEv2 configuration.

Command Default

There is no default value or behavior.

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
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

The **migrate l2l** command migrates all LAN-to-LAN IKEv1 configuration to IKEv2.

If you use the **overwrite** keyword, the ASA overwrites any existing IKEv2 configuration with migrated commands instead of merging them.

The **migrate remote-access** command migrates the IKEv1 or SSL settings to IKEv2, but you must still perform these configuration tasks:

- Load the Secure Client package file(s) in webvpn configuration mode.
- Configure the Secure Client profiles and specify them for group policies.
- Associate any customization objects you used for IKEv1 connections with the tunnel group(s) used for IKEv2 connections.

- Specify server authentication identity certificates (trustpoints) using the **crypto ikev2 remote-access trust-point** command. The ASA uses the trustpoint to authenticate itself to remote Secure Clients connecting with IKEv2.
- Specify IKEv2 and/or SSL for any tunnel groups or group policies you may have configured in addition to the default ones (the DefaultWEBVPNGroup tunnel-group and default group-policy are configured to allow IKEv2 or SSL).
- Configure group aliases or group URLs in the tunnel-groups to enable the clients to connect to groups other than the default group.
- Update any external group policies and/or user records.
- Any other global, tunnel group, group policy settings to change client behavior.
- Configure the port to be used by the client to download files and/or perform software upgrades for IKEv2 using the **crypto ikev2 enable** <interface> [client-services [port]] command.

Related Commands

Command	Description
crypto ikev2 enable	Enables IKEv2 negotiation on the interface on which the IPsec peers communicate.
show run crypto ikev2	Displays IKEv2 configuration information.

min-object-size

To set a minimum size for objects that the ASA can cache for WebVPN sessions, use the min-object-size command in cache mode. To change the size, use the command again. To set no minimum object size, enter a value of zero (0).

min-object-size*integerrange*

Syntax Description

integer	0 - 10000
range	KB.

Command Default

The default size is 0 KB.

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 minimum object size must be smaller than the maximum object size. The ASA calculates the size after compressing the object, if cache compression is enabled.

Examples

The following example shows how to set a maximum object size of 40 KB:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# min-object-size
 40
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.

Command	Description
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.

mkdir

To create a new directory, use the **mkdir** command in privileged EXEC mode.

mkdir [/ **noconfirm**] [**disk0:** | **disk1:** | | **flash:**] *path*

Syntax Description

noconfirm	(Optional) Suppresses the confirmation prompt.
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) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series adaptive security appliances, the **flash** keyword is aliased to **disk0**.
path	The name and path of the directory to create.

Command Default

If you do not specify a path, the directory is created in the current working 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.

Usage Guidelines

If a directory with the same name already exists, then the new directory is not created.

Examples

The following example shows how to make a new directory called “backup”:

```
ciscoasa# mkdir backup
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
rmdir	Removes the specified directory.

Command	Description
pwd	Display the current working directory.

mobile-device portal

To change the clientless vpn access web portal from the mini-portal to the full-browser portal, for all mobile devices, use the **mobile-device portal** command from webvpn configuration mode. You will only need to make this configuration for smart phones running older operating systems such as Windows CE. You will not need to configure this option using modern smart phones as they use the full-browser portal by default.

mobile-device portal { **full** }
no mobile-device portal { **full** }

Syntax Description

mobile-device portal {full}	Changes the clientless vpn access portal from the mini-portal to the full-browser portal for all mobile devices.

Command Default

Before you run the command, the default behavior is that some mobile devices will get clientless vpn access through the mini-portal and some will use the full portal.

Command Modes

The 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(5)	This command was added simultaneously in 8.2(5) and 8.4(2).
8.4(2)	This command was added simultaneously in 8.2(5) and 8.4(2).

Usage Guidelines

Use this command only if you are recommended to do so by Cisco Technical Assistance Center (TAC).

Examples

Changes the clientless vpn access portal to a full-browser portal for all mobile devices.

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

Related Commands

Command	Description
show running-config webvpn	Displays the running configuration for webvpn.

mode

To set the security context mode to single or multiple, use the **mode** command in global configuration mode. You can partition a single ASA into multiple virtual devices, known as security contexts. Each context behaves like an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone appliances. In single mode, the ASA has a single configuration and behaves as a single device. In multiple mode, you can create multiple contexts, each with its own configuration. The number of contexts allowed depends on your license.

mode { **single** | **multiple** } [**noconfirm**]

Syntax Description

multiple	Sets multiple context mode.
noconfirm	(Optional) Sets the mode without prompting you for confirmation. This option is useful for automated scripts.
single	Sets the context mode to single.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes 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

In multiple context mode, the ASA includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone device (see the **config-url** command to identify the context configuration location). The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. 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 contexts from the server), it uses one of the contexts that is designated as the admin context.

When you change the context mode using the **mode** command, you are prompted to reboot.

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the **mode** command.

When you convert from single mode to multiple mode, the ASA converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal Flash memory). The original running configuration is saved as old_running.cfg (in the root directory of the internal Flash memory). The original startup configuration is not saved. The ASA automatically adds an entry for the admin context to the system configuration with the name "admin."

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the ASA; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device.

Not all features are supported in multiple context mode. See the CLI configuration guide for more information.

Examples

The following example sets the mode to multiple:

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

The following example sets the mode to single:

```
ciscoasa(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

Related Commands

Command	Description
context	Configures a context in the system configuration and enters context configuration mode.
show mode	Shows the current context mode, either single or multiple.

monitor-interface

To enable health monitoring on a specific interface, use the **monitor-interface** command in global configuration mode. To disable interface monitoring, use the **no** form of this command.

monitor-interface { *if_name* | **service-module** }
no monitor-interface { *if_name* **service-module** }

Syntax Description

if_name	Specifies the name of the interface being monitored.
service-module	Monitors the service module. If you do not want a hardware module failure, such as the ASA FirePOWER module, to trigger failover, you can disable module monitoring using the **no** form of this command.

Command Default

Monitoring of physical interfaces and the service module 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.
9.3(1)	The service-module keyword was added.

Usage Guidelines

The number of interfaces that can be monitored for the ASA is platform dependent and can be determined by viewing the **show failover** command output.

Hello messages are exchanged during every interface poll frequency time period between the ASA failover pair. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds).

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.

- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

In Active/Active failover, this command is only valid within a context.

Examples

The following example enables monitoring on an interface named “inside”:

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure monitor-interface	Restores the default interface health monitoring for all interfaces.
failover interface-policy	Specifies the number or percentage of monitored interface that must fail for failover to occur.
failover polltime	Specifies the interval between hello messages on an interface (Active/Standby failover).
polltime interface	Specifies the interval between hello messages on an interface (Active/Active failover).
show running-config monitor-interface	Displays the **monitor-interface** commands in the running configuration.

more

To display the contents of a file, use the **more** command in privileged EXEC mode.

more { **/ascii** | **/binary** | **/ebcdic** / **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **system:** | **tftp:** } *filename*

Syntax Description

/**ascii**	(Optional) Displays a binary file in binary mode and an ASCII file in binary mode.
/binary	(Optional) Displays any file in binary mode.
/**ebcdic**	(Optional) Displays binary files in EBCDIC.
disk0*:*	(Optional) Displays a file on the internal Flash memory.
disk1:	(Optional) Displays a file on the external Flash memory card.
filename	Specifies the name of the file to display.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series adaptive security appliance, the **flash** keyword is aliased to **disk0**.
ftp:	(Optional) Displays a file on an FTP server.
http:	(Optional) Displays a file on a website.
https:	(Optional) Displays a file on a secure website.
system:	(Optional) Displays the file system.
tftp:	(Optional) Displays a file on a TFTP server.

Command Default

ASCII 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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **more filesystem:** command prompts you to enter the alias of the local directory or file systems.

Note When you view a configuration file that you have saved using the **more** command, tunnel-group passwords in the configuration file appear in clear text.

Examples

The following example shows how to display the contents of a local file named “test.cfg”:

```
ciscoasa# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
```

```
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

Command	Description
cd	Changes to the specified directory.
pwd	Displays the current working directory.

mount type cifs

To make a Common Internet File System (CIFS) accessible to the security appliance, use the **mount type cifs** command in global configuration mode. This command lets you enter mount cifs configuration mode. To un-mount the CIFS network file system, use the **no** form of this command.

mount *name* **type cifs server** *server-name* **share** *share* { **status enable** | **status disable** } [**domain** *domain-name*] **username** *username* **password** *password*
[**mount**] **mount** *name* **type cifs server** *server-name* **share** *share* { **status enable** | **status disable** } [**domain** *domain-name*] **username** *username* **password** *password*

Syntax Description

domain *domain-name*	(Optional) For CIFS file systems only, this argument specifies the Windows NT domain name. A maximum of 63 characters is permitted.
name	Specifies the name of an existing file system to be assigned to the Local CA.
password password	Identifies the authorized password for file-system mounting.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the CIFS file-system server.
share *sharename*	Explicitly identifies a specific server share (a folder) by name to access file data within a server.
status enable or **disable**	Identifies the state of the file system as mounted or un-mounted (available or unavailable).
user *username*	The authorized username for file-system mounting.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes 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

The **mount** command uses the Installable File System (IFS) to mount the CIFS file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

The **mount** command attaches the CIFS file system on the security appliance to the UNIX file tree. Conversely, the **no mount** command detaches it.

The *mount-name* specified in the **mount** command is used by other CLI commands to refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage for the Local Certificate Authority, needs the mount name of an existing mounted file system to save database files to non-flash storage.

The CIFS remote file-access protocol is compatible with the way applications share data on local disks and network file servers. Running over TCP/IP and using the Internet's global DNS, CIFS is an enhanced version of Microsoft's open, cross-platform Server Message Block (SMB) protocol, the native file-sharing protocol in the Windows operating systems.

Always exit from the root shell after using the **mount** command. The **exit** keyword in mount-cifs-config mode returns the user to global configuration mode.

In order to reconnect, remap your connections to storage.



Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

The following example mounts *cifs://amer;chief:big-boy@myfiler02/my_share* as the label, *cifs_share:*

```
ciscoasa
(config)#
mount cifs_share type CIFS

ciscoasa (config-mount-cifs)#
server myfiler02a
```

Related Commands

Command	Description
debug cifs	Logs CIFS debug messages.
debug ntdomain	Logs Web VPN NT Domain debug messages
debug webvpn cifs	Logs WebVPN CIFS debug messages.
dir all-filesystems	Displays the files of all filesystems mounted on the ASA.

mount type ftp

To make a File Transfer Protocol (FTP) file system accessible to the security appliance, use the **mount type ftp** command in global configuration mode to enter mount FTP configuration mode. The **no mount type ftp** command is used to unmount the FTP network file system.

[**no**] **mount** *name* **type ftp server** *server-name* **path** *pathname* { **status enable** | **status disable** } { **mode active** | **mode passive** } **username** *username* **password** *password*

Syntax Description

mode active or **passive**	Identifies the FTP transfer mode as either active or passive.
no	Removes an already mounted FTP file system, rendering it inaccessible.
password password	Identifies the authorized password for file-system mounting.
path *pathname*	Specifies the directory pathname to the specified FTP file-system server. The pathname cannot contain spaces.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the FTPFS file-system server.
status enable or **disable**	Identifies the state of the file system as mounted or unmounted (available or unavailable).
username *username*	Specifies the authorized username for file-system mounting.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes 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

The **mount** *name* **type ftp** command uses the Installable File System (IFS) to mount the specified network file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

To confirm that the FTP file system actually is mounted, use the **dir all-filesystems** instruction

The mount-name specified in the **mount** command is used when other CLI commands refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage

for the local certificate authority, needs the mount name of a mounted file system to save database files to non-flash storage.

Note Using the **mount** command when you create an FTP-type mount requires that the FTP server must have a UNIX directory listing style. Microsoft FTP servers have the MS-DOS directory listing style as their default.

Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

This example mounts *ftp://amor;chief:big-kid@myfiler02* as the label, *my ftp:*

```
ciscoasa
(config)#
mount myftp type ftp server myfiler02a path status enable username chief password big-kid
```

Related Commands

Command	Description
debug webvpn	Logs WebVPN debugging messages.
ftp mode passive	Controls interaction between the FTP client on the ASA and the FTP server.

mroute

To configure a static multicast route, use the **mroute** command in global configuration mode. To remove a static multicast route, use the **no** form of this command.

mroute *src smask* { *in_if_name* [**dense** *output_if_name*] | *rpf_addr* } [*distance*]
no *mroute src smask* { *in_if_name* [**dense** *output_if_name*] | *rpf_addr* } [*distance*]

Syntax Description

dense *output_if_name*	(Optional) The interface name for dense mode output. The **dense** *output_if_name* keyword and argument pair is only supported for SMR stub multicast routing (igmp forwarding).
distance	(Optional) The administrative distance of the route. Routes with lower distances have preference. The default is 0.
in_if_name	Specifies the incoming interface name for the mroute.
rpf_addr	Specifies the incoming interface for the mroute. If the RPF address PIM neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-addr* argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system.
smask	Specifies the multicast source network address mask.
src	Specifies the IP address of the multicast source.

Command Default

No default behavior or values.

Command Modes

The following table shows the 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

This command lets you statically configure where multicast sources are located. The ASA expects to receive multicast packets on the same interface as it would use to send unicast packets to a specific source. In some cases, such as bypassing a route that does not support multicast routing, multicast packets may take a different path than the unicast packets.

Static multicast routes are not advertised or redistributed.

Use the **show mroute** command displays the contents of the multicast route table. Use the **show running-config mroute** command to display the mroute commands in the running configuration.

Examples

The following example shows how configure a static multicast route using the **mroute** command:

```
ciscoasa(config)# mroute 172.16.0.0 255.255.0.0 inside
```

Related Commands

Command	Description
clear configure mroute	Removes the **mroute** commands from the configuration.
show mroute	Displays the IPv4 multicast routing table.
show running-config mroute	Displays the **mroute** commands in the configuration.

mschapv2-capable

To enable MS-CHAPv2 authentication requests to the RADIUS server, use the **mschapv2-capable** command in aaa-server host configuration mode. To disable MS-CHAPv2, use the **no** form of this command.

mschapv2-capable
nomschapv2-capable

Syntax Description

This command has no arguments or keywords.

Command Default

MS-CHAPv2 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
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

To enable MS-CHAPv2 as the protocol used between the ASA and the RADIUS server for a VPN connection, password management must be enabled in the tunnel-group general-attributes. Enabling password management generates an MS-CHAPv2 authentication request from the ASA to the RADIUS server. See the description of the **password-management** command for details.

If you use double authentication and enable password management in the tunnel group, then the primary and secondary authentication requests include MS-CHAPv2 request attributes. If a RADIUS server does not support MS-CHAPv2, then you can configure that server to send a non-MS-CHAPv2 authentication request by using the **no mschapv2-capable** command.

Examples

The following example disables MS-CHAPv2 for the RADIUS server authsrv1.cisco.com:

```
ciscoasa(config)# aaa-server rsaradius protocol radius
ciscoasa(config-aaa-server-group)# aaa-server rsaradius (management) host authsrv1.cisco.com
ciscoasa(config-aaa-server-host)# key secretpassword
ciscoasa(config-aaa-server-host)# authentication-port 21812
ciscoasa(config-aaa-server-host)# accounting-port 21813
ciscoasa(config-aaa-server-host)# no mschapv2-capable
```

Related Commands

Command	Description
aaa-server host	Identifies a AAA server for a AAA server group.
password-management	When you configure the password-management command, the ASA notifies the remote user at login that the user's current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password.
secondary-authentication-server-group	Specifies the secondary AAA server group, which cannot be an SDI server group.

msie-proxy except-list

To configure browser proxy exception list settings for a local bypass on the client device, enter the **msie-proxy except-list** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy except-list { **value** *server* [*:port*] | **none** }
nomsie-proxyexcept-list

Syntax Description

none	Indicates that there is no IP address/hostname or port and prevents inheriting an exception list.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client device. The port number is optional.

Command Default

By default, msie-proxy except-list 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
Group-policy Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to set a Microsoft Internet Explorer proxy exception list, consisting of the server at IP address 192.168.20.1, using port 880, for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy local-bypass

To configure browser proxy local-bypass settings for a client device, enter the **msie-proxy local-bypass** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy local-bypass { **enable** | **disable** }
no msie-proxy local-bypass { **enable** | **disable** }

Syntax Description

disable	Disables browser proxy local-bypass settings for a client device.
enable	Enables browser proxy local-bypass settings for a client device.

Command Default

By default, msie-proxy local-bypass 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
Group-policy Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to enable Microsoft Internet Explorer proxy local-bypass for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
```

ciscoasa(config-group-policy)#

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy lockdown

To hide the Connections tab in Microsoft Internet Explorer and the system proxy tab in the Settings app for the duration of an AnyConnect VPN session or to leave it unchanged, use the **msie-proxy lockdown** command in group-policy configuration mode.

msie-proxy lockdown [**enable** | **disable**]

Syntax Description

disable	Leaves the Connections tab in Microsoft Internet Explorer and system proxy tab in the Settings app unchanged.
enable	Hides the Connections tab in Microsoft Internet Explorer and system proxy tab in the Settings app for the duration of an AnyConnect VPN session.

Command Default

The default value of this command in the default group policy is enable. Each group policy inherits its default values from the default group policy.

Command Modes

The 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	• Yes	—	—

Command History

Release	Modification
8.2(3)	This command was added.

Usage Guidelines

Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. In addition, from Windows 10 version 1703 (or later), enabling this feature also hides the system proxy tab in the Settings app for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab in Microsoft Internet Explorer and system proxy tab in the Settings app unchanged.

To use this feature, you must also specify a private-side proxy.

Note Hiding the system proxy tab in the Settings app for the duration of an AnyConnect VPN session needs AnyConnect version 4.7.03052 or later.

This command makes a temporary change to the user registry for the duration of the AnyConnect VPN session. When AnyConnect closes the VPN session, it returns the registry to the state it was in before the session.

You might enable this feature to prevent users from specifying a proxy service and changing LAN settings. Preventing user access to these settings enhances endpoint security during the AnyConnect session.

Refer to the Cisco Secure Client Administrator Guide , or the release notes for your mobile device for further information about proxy settings.

Examples

The following example hides the Connections tab for the duration of the AnyConnect session:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

The following example leaves the Connections tab unchanged:

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

Related Commands

Command	Description
msie-proxy except-list	Specifies an exception list of proxy servers for browser on the client device.
msie-proxy local-bypass	Bypasses the local browser proxy settings configured on the client device.
msie-proxy method	Specifies the browser proxy actions for a client device.
msie-proxy pac-url	Specifies a URL from which to retrieve a proxy auto-configuration file that defines the proxy servers.
msie-proxy server	Configures proxy server for browser on the client device.
show running-config group-policy	Shows the group policy settings in the running configuration.

msie-proxy method

To configure the browser proxy actions ("methods") for a client device, enter the **msie-proxy method** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]
no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url** }



Note See the Usage Guidelines section for qualifications that apply to this syntax.

Syntax Description

auto-detect	Enables the use of automatic proxy server detection in the browser for the client device.
no-modify	Leaves the HTTP browser proxy server setting in the browser unchanged for this client device.
no-proxy	Disables the HTTP proxy setting in the browser for the client device.
use-pac-url	Directs the browser to retrieve the HTTP proxy server setting from the proxy auto-configuration file URL specified in the **msie-proxy pac-url** command.
use-server	Sets the HTTP proxy server setting in the browser to use the value configured in the **msie-proxy server** command.

Command Default

The default method is use-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
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The use-pac-url option was added.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number can contain up to 100 characters.

This command supports the following combinations of options:

- **[no] msie-proxy method no-proxy**
- **[no] msie-proxy method no-modify**
- **[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]**

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. The .pac file resides on a web server. When you specify **use-pac-url**, the browser uses the .pac file to determine the proxy settings. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to configure auto-detect as the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

The following example configures the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup to use the server QAserver, port 1001 as the server for the client PC:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server QAserver:port 1001
ciscoasa(config-group-policy)# msie-proxy method use-server
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy pac-url	Specifies a URL from which to retrieve a proxy auto-configuration file.
msie-proxy server	Configures a browser proxy server and port for a client device.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy pac-url

To tell a browser where to look for proxy information, enter the **msie-proxy pac-url** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy pac-url { **none** | **value** *url* }
nomsie-proxypac-url

Syntax Description

none	Specifies that there is no URL value.
value *url*	Specifies the URL of the website at which the browser can get the proxy auto-configuration file that defines the proxy server or servers to use.

Command Default

The default value 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-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Requirements

To use the proxy auto-configuration feature, the remote user must use the Cisco AnyConnect VPN Client. To enable the use of the proxy auto-configuration URL, you must also configure the **msie-proxy method** command with the **use-pac-url** option.

Why Use This Command

Many network environments define HTTP proxies that connect a web browser to a particular network resource. The HTTP traffic can reach the network resource only if the proxy is specified in the browser and the client routes the HTTP traffic to the proxy. SSLVPN tunnels complicate the definition of HTTP proxies because the proxy required when tunneled to an enterprise network can differ from that required when connected to the Internet via a broadband connection or when on a third-party network.

In addition, companies with large networks might need to configure more than one proxy server and let users choose between them, based on transient conditions. By using .pac files, an administrator can author a single script file that determines which of numerous proxies to use for all client computers throughout the enterprise.

The following are some examples of how you might use a PAC file:

- Choosing a proxy at random from a list for load balancing.

- Rotating proxies by time of day or day of the week to accommodate a server maintenance schedule.
- Specifying a backup proxy server to use in case the primary proxy fails.
- Specifying the nearest proxy for roaming users, based on the local subnet.

How to Use the Proxy Auto-Configuration Feature

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file. Then, when you specify **use-pac-url** in the **msie-proxy method** command, the browser uses the .pac file to determine the proxy settings.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to configure a browser to get its proxy setting from the URL www.example.com for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

The following example disables the proxy auto-configuration feature for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url none
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy method	Configures the browser proxy actions (“methods”) for a client device.
msie-proxy server	Configures a browser proxy server and port for a client device.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy server

To configure a browser proxy server and port for a client device, enter the **msie-proxy server** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy server { **value** *server* [*:port*] | **none** }
nomsie-proxyserver

Syntax Description

none	Indicates that there is no IP address/hostname or port specified for the proxy server and prevents inheriting a server.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client device. The port number is optional.

Command Default

By default, no msie-proxy server 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
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to configure the IP address 192.168.10.1 as a Microsoft Internet Explorer proxy server, using port 880, for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

mtu

To specify the maximum transmission unit for an interface, use the **mtu** command in global configuration mode. To reset the MTU block size to 1500 for Ethernet interfaces, use the **no** form of this command. This command supports IPv4 and IPv6 traffic.

mtu*interface_namebytes*
nomtu*interface_namebytes*

Syntax Description

bytes	Number of bytes in the MTU; valid values are from 64 to 9198 bytes (9000 for the Secure Client and Firepower 9300 ASA security module).
interface_name	Internal or external network interface name.

Command Default

The default *bytes* is 1500 for Ethernet 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
Global configuration	—	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.1(6)	The maximum MTU was changed from 65535 to 9198 (or 9000, depending on your model).

Usage Guidelines

The **mtu** command lets you to set the payload size (not including Layer 2 headers or VLAN tagging) that is sent on a connection. Data that is larger than the MTU value is fragmented before being sent. The default MTU is 1500 bytes for Ethernet interfaces (which is also the maximum without jumbo frame reservation). In this case, the size of the packet with Layer 2 headers (14 bytes) and VLAN tagging (4 bytes) is 1518 bytes. This value is sufficient for most applications, but you can pick a lower number if network conditions require it.

The ASA supports IP path MTU discovery (as defined in RFC 1191), which allows a host to dynamically discover and cope with the differences in the maximum allowable MTU size of the various links along the path. Sometimes, the ASA cannot forward a datagram because the packet is larger than the MTU that you set for the interface, but the “don’t fragment” (DF) bit is set. The network software sends a message to the sending host, alerting it to the problem. The host has to fragment packets for the destination so that they fit the smallest packet size of all the links along the path.

When using the Layer 2 Tunneling Protocol (L2TP), we recommend that you set the MTU size to 1380 to account for the L2TP header and IPsec header length.

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.

Starting in Version 9.1(6), the maximum MTU that the ASA can use is 9198 bytes. This value does not include the Layer 2 header. Formerly, the ASA let you specify the maximum MTU as 65535 bytes, which was inaccurate and could cause problems. If your MTU was set to a value higher than 9198, then the MTU is automatically lowered when you upgrade. In some cases, this MTU change can cause an MTU mismatch; be sure to set any connecting equipment to use the new MTU value.

Examples

This example shows how to specify the MTU for an interface:

```
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
ciscoasa(config)# mtu inside 8192
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

Related Commands

Command	Description
clear configure mtu	Clears the configured maximum transmission unit values on all interfaces.
show running-config mtu	Displays the current maximum transmission unit block size.

mtu cluster

To set the maximum transmission unit of the cluster control link, use the **mtu cluster** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mtu cluster *bytes*
no mtu cluster [*bytes*]

Syntax Description

bytes Specifies the maximum transmission unit for the cluster control link interface, between 64 and 65,535 bytes. We do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation.The default MTU is 1500 bytes.

Command Default

The default MTU is 1500 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
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.22(1)	A ping was added to test the MTU on the cluster control link when a node joins.
9.24(1)	Pings of smaller sizes were added to test the MTU on the cluster control link when a node joins.

Usage Guidelines

We suggest setting the MTU to 1600 bytes or greater, which requires you to enable jumbo frame reservation using the **jumbo-frame reservation** command.

This command is a global configuration command, but is also part of the bootstrap configuration, which is not replicated between units.

When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size matching the cluster control link MTU. If the initial ping fails, the ASA tries a ping using a smaller packet size (the MTU divided by 2, then by 4, then by 8) until a ping succeeds. A notification is generated so you can fix the MTU mismatch on connecting switches and try again.

Examples

The following example sets the cluster control link MTU to 9000 bytes:

```
ciscoasa(config)# mtu cluster 9000
```

Related Commands

Command	Description
cluster-interface	Identifies the cluster control link interface.
jumbo frame-reservation	Enables use of jumbo Ethernet frames.

multicast boundary

To configure a multicast boundary for administratively-scoped multicast addresses, use the **multicast boundary** command in interface configuration mode. To remove the boundary, use the **no** form of this command. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains.

multicast boundary *acl* [**filter-autorp**]
no multicast boundary *acl* [**filter-autorp**]

Syntax Description

acl	Specifies an access list name or number. The access list defines the range of addresses affected by the boundary. Use only standard ACLs with this command; extended ACLs are not supported.
filter-autorp	Filters Auto-RP messages denied by the boundary ACL. If not specified, all Auto-RP messages are passed.

Command Default

No default behavior or values.

Command Modes

The 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

Use this command to configure an administratively scoped boundary on an interface to filter multicast group addresses in the range defined by the *acl* argument. A standard access list defines the range of addresses affected. When this command is configured, no multicast data packets are allowed to flow across the boundary in either direction. Restricting multicast data packet flow enables reuse of the same multicast group address in different administrative domains.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Examples

The following example sets up a boundary for all administratively scoped addresses and filters the Auto-RP messages:

```
ciscoasa(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
ciscoasa(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# multicast boundary boundary_test filter-autorp
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

multicast-routing

To enable IP multicast routing on the ASA, use the **multicast routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

multicast-routing
nomulticast-routing

Syntax Description

This command has no arguments or keywords.

Command Default

The **multicast-routing** command enables PIM and IGMP on all interfaces 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.

Usage Guidelines

The **multicast-routing** command enables PIM and IGMP on all interfaces.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.If the security appliance is the PIM RP, use the untranslated outside address of the security appliance as the RP address.

The number of entries in the multicast routing tables are limited by the amount of RAM on the system. <xref> lists the maximum number of entries for specific multicast tables based on the amount of RAM on the security appliance. Once these limits are reached, any new entries are discarded.

Table 1: Entry Limits for Multicast Tables (Combined Static and Dynamic Entries)

Table	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP Groups	1000	3000	5000

Table	16 MB	128 MB	128+ MB
PIM Routes	3000	7000	12000

Examples

The following example enables IP multicast routing on the ASA:

```
ciscoasa(config)# multicast-routing
```

Related Commands

Command	Description
igmp	Enables IGMP on an interface.
pim	Enables PIM on an interface.

mus

To specify the IP range and interface on which the ASA identifies the WSA, use the **mus** command in global configuration mode. To turn the service off, use the **no** form of this command. This command supports IPv4 and IPv6 traffic. Only WSAs found on the specified subnet and interface are registered.

mus *IPv4 address IPv4 mask interface_name*
no mus *IPv4 address IPv4 mask interface_name*

Note 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 AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

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
8.3(1)	This command was added.

Usage Guidelines

The following commands are possible:

- A.B.C.D—The IP address of WSA authorized to access ASA.
- host—The client periodically checks connectivity to the Web Security appliance by sending a request to a fictitious host. By default, the fictitious host URL is mus.cisco.com. When AnyConnect Security Mobility is enabled, the Web Security appliance intercepts requests destined for the fictitious host and replies to the client.
- password—Configure WSA password.
- server—Configure WSA server

Examples

The following example allows WSA servers on the 1.2.3.x subnet to access secure mobility solutions on the *inside* interface:

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

Related Commands

Command	Description
mus password	Sets up shared secret for AnyConnect Secure Mobility communications.
mus server	Specifies the port on which the ASA listens for WSA communication.
show webvpn mus	Displays information about the active WSA connection security appliance.

mus host

To specify the MUS hostname on the ASA, enter the **mus host** command in global configuration mode. This is the telemetry URL sent from the ASA to the Secure Client. The Secure Clients use this URL to contact the WSA in the private network for MUS-related services. To remove any commands entered with this command, use the **no mus host** command.

mus host *host name*
nomushost

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
8.3(1)	This command was added.

Usage Guidelines

You can enable AnyConnect Secure Mobility for a given port. The WSA port values are 1 through 21000. If a port is not specified in the command, port 11999 is used.

You must configure AnyConnect Secure Mobility shared secret before executing this command.

Note 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 AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

Examples

The following example shows how to enter the AnyConnect Secure Mobility host and WebVPN command submode:

```
ciscoasa(config)# webvpn

ciscoasa(config-webvpn)# mus 0.0.0.0 0.0.0.0 inside

ciscoasa(config-webvpn)# mus password abcdefgh123
```

```
ciscoasa(config-webvpn)# mus server enable 960 # non-default port

ciscoasa(config-webvpn)# mus host mus.cisco.com
```

Related Commands

Command	Description
mus	Specifies the IP range and interface on which the ASA identifies the WSA.
mus password	Sets up shared secret for AnyConnect Secure Mobility communications.
show webvpn mus	Displays information about the active WSA connection security appliance.

mus password

To set up shared secred for AnyConnect Secure Mobility communications, enter the **mus password** command in global configuration mode. To remove the shared secred, use the **no mus password** command.

muspassword
nomuspassword



Note 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 AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

Syntax Description

This command has no arguments or keywords.

Command Default

.The valid password is defined by the regular expression [0-9, a-z, A-Z,:;_/-]{8,20}. The overall length of the shared secret password is a minimum of 8 characters and maximum of 20 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 configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

This WebVPN submode lets you configure global settings for WebVPN. You can set up the shared secret for AnyConnect Secure Mobility communications.

Examples

The following example shows how to enter an AnyConnect Secure Mobility password and WebVPN command submode:

```
ciscoasa
(config)#
 mus password <password_string>
ciscoasa
(config-webvpn)#
```

Related Commands

Command	Description
mus	Specifies the IP range and interface on which the ASA identifies the WSA.
mus server	Specifies the port on which the ASA listens for WSA communication.
show webvpn mus	Displays information about the active WSA connection security appliance.

mus server

To specify the port on which the ASA listens for WSA communication, enter the **mus server** command in global configuration mode. To remove any commands entered with this command, use the **no mus server** command.

musserverenable
nomusserverenable



Note 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 AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

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
8.3(1)	This command was added.

Usage Guidelines

You must specify a port the AnyConnect Secure Mobility service uses. The communication between the ASA and the WSA is by a secure SSL connection on a port specified by the administrator with values of 1 through 21000.

You must configure AnyConnect Secure Mobility shared secret before executing this command.

Examples

The following example shows how to enter the AnyConnect Secure Mobility password and WebVPN command submode:

```
ciscoasa
(config-webvpn)#
mus server enable
?
webvpn mode commands/options
```

```
 port Configure WSA port
ciscoasa(config-webvpn)# mus server enable port 12000
```

Related Commands

Command	Description
mus	Specifies the IP range and interface on which the ASA identifies the WSA.
mus password	Sets up shared secret for AnyConnect Secure Mobility communications.
show webvpn mus	Displays information about the active WSA connection security appliance.