e

echo

To configure echo in a BFD single-hop template, use the echo command in BFD template configuration mode. To disable echo in BFD template for single-hop sessions, use the **no** form of this command.

echo
no echo

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
BFD configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to enable echo mode functionality in a single-hop template only. BFD echo is not supported for IPv6 BFD sessions.

Examples

The following example configures echo for a single-hop BFD template.

```
ciscoasa(config)# bfd-template single-hop template1
ciscoasa(config-bfd)# echo
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.

Command	Description
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

early-message

To allow messages before the H.255 SETUP message during H.323 inspection, use the **early-message** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

early-message*message_type*
no early-message *message_type*

Syntax Description

message_type	The type of message to allow before the H.225 SETUP message. You can enter the following types: • **facility**

Command Default

The command is disabled. Messages before the H.225 SETUP message are not allowed, resulting in dropped connections.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was introduced.

Usage Guidelines

H.460.18 defines a method for traversal of H.323 signaling across network address translators and firewalls. This method allows the H.225 FACILITY message to be sent before the H.225 SETUP message. If you encounter call setup issues, where connections are being closed before being completed when using H.323/H.225, use this command to allow early messages.

Also, ensure that you enable inspection for both H.323 RAS and H.225 (they are both enabled by default).

Examples

The following example shows how to allow early messages:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# early-message FACILITY
```

Related Commands

Command	Description
policy-map type inspect	Creates an inspection policy map.

Command	Description
show running-config policy-map	Display all current policy map configurations.

eigrp log-neighbor-changes

To enable the logging of EIGRP neighbor adjacency changes, use the **eigrp log-neighbor-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-changes
no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for EIGRP IPv6 was added.

Usage Guidelines

The **eigrp log-neighbor-changes** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor changes:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-changes
```

Related Commands

Command	Description
eigrp log-neighbor-warnings	Enables logging of neighbor warning messages.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp log-neighbor-warnings

To enable the logging of EIGRP neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]
no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. Valid values are from 1 to 65535. Repeated warnings are not logged if they occur during this interval.

Command Default

This command is enabled by default. All neighbor warning messages are logged.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for EIGRP IPv6 was added.

Usage Guidelines

The **eigrp log-neighbor-warnings** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor warning messages:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-warnings
```

The following example logs EIGRP neighbor warning messages and repeats the warning messages in 5-minute (300 seconds) intervals:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
eigrp log-neighbor-messages	Enables the logging of changes in EIGRP neighbor adjacencies.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp router-id

To specify router ID used by the EIGRP routing process, use the **eigrp router-id** command in router configuration mode. To restore the default value, use the **no** form of this command.

eigrp router-id *ip-address*
no eigrp router-id [*ip-address*]

Syntax Description

ip-address	Router ID in IP address (dotted-decimal) format. You cannot use 0.0.0.0 or 255.255.255.255 as the router ID.

Command Default

If not specified, the highest-level IP address on the ASA is used as the router ID.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for configuring EIGRP with IPv6 address was added.

Usage Guidelines

If the **eigrp router-id** command is not configured, EIGRP automatically selects the highest IP address on the ASA to use as the router ID when an EIGRP process is started. The router ID is not changed unless the EIGRP process is removed using the **no router eigrp** command or unless the router ID is manually configured with the **eigrp router-id** command.

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. To prevent this, use the **eigrp router-id** command to specify a global address for the router ID.

A unique value should be configured for each EIGRP router.

Examples

The following example configures 172.16.1.3 as a fixed router ID for the EIGRP routing process:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp stub

To configure the EIGRP routing process as a stub routing process, use the **eigrp stub** command in router configuration mode. To remove EIGRP stub routing, use the **no** form of this command.

eigrp stub [**receive-only**] | { [**connected**] [**redistributed**] [**static**] [**summary**] }
no eigrp stub [**receive-only**] | { [**connected**] [**redistributed**] [**static**] [**summary**] }

Syntax Description

connected	(Optional) Advertises connected routes.
receive-only	(Optional) Sets the ASA as a received-only neighbor.
redistributed	(Optional) Advertises routes redistributed from other routing protocols.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.

Command Default

Stub routing is not enabled.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• Yes	• —

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for IPv6 routing was added.

Usage Guidelines

Use the **eigrp stub** command to configure the ASA as a stub where the ASA directs all IP traffic to a distribution router.

Using the **receive-only** keyword restricts the ASA from sharing any of its routes with any other router in the autonomous system; the ASA only receives updates from the EIGRP neighbor. You cannot use any other keyword with the **receive-only** keyword.

You can specify one or more of the **connected**, **static**, **summary**, and **redistributed** keywords. If any of these keywords is used with the **eigrp stub** command, only the route types specified by the particular keyword are sent.

The **connected** keyword permits the EIGRP stub routing process to send connected routes. If the connected routes are not covered by a **network** statement, it may be necessary to redistribute connected routes with the **redistribute** command under the EIGRP process.

The **static** keyword permits the EIGRP stub routing process to send static routes. Without the configuration of this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. You must still redistribute static routes using the **redistribute static** command.

The **summary** keyword permits the EIGRP stub routing process to send summary routes. You can create summary routes manually with the **summary-address eigrp** command or automatically with the **auto-summary** command enabled (this command is enabled by default).

The **redistributed** keyword permits the EIGRP stub routing process to send routes redistributed into the EIGRP routing process from other routing protocols. If you do you configure this option, EIGRP does not advertise redistributed routes.

Examples

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that advertises connected and summary routes:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected summary
```

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that advertises connected and static routes. Sending summary routes is not permitted.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected static
```

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that only receives EIGRP updates. Connected, summary, and static route information is not sent.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 eigrp

ciscoasa(config-router)# eigrp stub receive-only
```

The following example uses the **eigrp stub** command to configure the ASA as an EIGRP stub that advertises routes redistributed into EIGRP from other routing protocols:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub redistributed
```

The following example uses the **eigrp stub** command without any of the optional arguments. When used without arguments, the **eigrp stub** commands advertises connected and static routes by default.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub
```

Related Commands

Command	Description
router eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

eject

To support the removal of an ASA external compact flash device, use the **eject** command in user EXEC mode.

eject [**/noconfirm**] *disk1:*

Syntax Description

disk1:	Specifies the device to eject.
/noconfirm	Specifies that you do not need to confirm device removal before physically removing the external flash device from the ASA.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **eject** command allows you to safely remove a compact flash device from an ASA 5500 series.

The following example shows how to use the **eject** command to shut down *disk1* gracefully before the device is physically removed from the ASA:

```
ciscoasa
#
eject /noconfig disk1:
It is now safe to remove disk1:
ciscoasa
#
show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34
Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"
wef5520 up 5 hours 36 mins
Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

Related Commands

Command	Description
show version	Displays information about the operating system software.

email

To include the indicated e-mail address in the Subject Alternative Name extension of the certificate during enrollment, use the **email** command in crypto ca-trustpoint configuration mode. To restore the default setting, use the **no** form of this command.

email*address*
no email

Syntax Description

address	Specifies the e-mail address. The maximum length is 64 characters.

Command Default

The default setting is not set.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and includes the e-mail address user1@user.net in the enrollment request for the trustpoint central:

```
ciscoasa(config)# crypto ca-trustpoint central
ciscoasa(ca-trustpoint)# email user1@user.net
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca-trustpoint	Enters crypto ca-trustpoint configuration mode.

enable (cluster group)

To enable clustering, use the **enable** command in cluster group configuration mode. To disable clustering, use the **no** form of this command.

enable [**as-slave** | **noconfirm**]
no enable

Syntax Description

as-slave	(Optional) Enables clustering without checking the running configuration for incompatible commands and ensures that the slave joins the cluster with no possibility of becoming the master in any current election. Its configuration is overwritten with the one synced from the master unit.
noconfirm	(Optional) When you enter the **enable** command, the ASA scans the running configuration for incompatible commands for features that are not supported with clustering, including commands that may be present in the default configuration. You are prompted to delete the incompatible commands. If you respond **No**, then clustering is not enabled. Use the **noconfirm** keyword to bypass the confirmation and delete incompatible commands automatically.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

For the first unit enabled, a master unit election occurs. Because the first unit should be the only member of the cluster so far, it will become the master unit. Do not perform any configuration changes during this period.

If you already have a master unit, and are adding slave units to the cluster, you can avoid any configuration incompatibilities (primarily the existence of any interfaces not yet configured for clustering) by using the **enable as-slave** command.

To disable clustering, enter the **no enable** command.

Note If you disable clustering, all data interfaces are shut down, and only the management interface is active. If you want to remove the unit from the cluster entirely (and thus want to have active data interfaces), you need to remove the entire cluster group configuration.

Examples

The following example enables clustering and removes incopatible configuration:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y
INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

enable (user EXEC)

To enter privileged EXEC mode, use the **enable** command in user EXEC mode.

enable [*level*]

Syntax Description

level (Optional) The privilege level between 0 and 15. Not used with enable authentication (the **aaa authentication enable console** command).

Command Default

Enters privilege level 15 unless you are using enable authentication (using the **aaa authentication enable console** command), in which case the default level depends on the level configured for your username.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The default enable password is blank. See the **enable password** command to set the password.

Without enable authentication, when you enter the **enable** command, your username changes to enable_*level* , where the default level is 15. With enable authentication (using the **aaa authentication enable console** command), the username and associated level are preserved. Preserving the username is important for command authorization (the **aaa authorization command** command, using either local or TACACS+).

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode. To use levels in between, enable local command authorization (the **aaa authorization command LOCAL** command) and set the commands to different privilege levels using the **privilege** command. TACACS+ command authorization does not use the privilege levels configured on the ASA.

See the **show curpriv** command to view your current privilege level.

Enter the **disable** command to exit privileged EXEC mode.

Examples

The following example enters privileged EXEC mode:

```
ciscoasa> enable
Password: Pa$$w0rd
ciscoasa#
```

The following example enters privileged EXEC mode for level 10:

```
ciscoasa> enable 10
Password: Pa$$w0rd10
ciscoasa#
```

Related Commands

Command	Description
enable password	Sets the enable password.
disable	Exits privileged EXEC mode.
aaa authorization command	Configures command authorization.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.

enable e-mail proxy (Deprecated)

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

To enable e-mail proxy access on a previously configured interface, use the **enable** command. For e-mail proxies (IMAP4S. POP3S, and SMTPS), use this command in the applicable e-mail proxy configuration mode. To disable e-mail proxy access on an interface, use the **no** form of the command.

enable*ifname*
no enable

Syntax Description

ifname Identifies the previously configured interface. Use the **nameif** command to configure interfaces.

Command Default

There are no default values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Examples

The following example shows how to configure POP3S e-mail proxy on the interface named Outside:

ciscoasa (config)# **pop3s** ciscoasa(config-pop3s)# **enable Outside**

enable gprs

To enable GPRS with RADIUS accounting, use the **enable gprs** command in radius-accounting parameter configuration mode. To disable this command, use the **no** form of this command.

enable gprs
no enable gprs

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Radius-accounting parameter configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command is accessed by using the **inspect radius-accounting** command. The ASA checks for the 3GPP VSA 26-10415 in the Accounting-Request Stop messages to correctly handle secondary PDP contexts. This option is disabled by default. A GTP license is required to enable this feature.

Examples

The following example shows how to enable GPRS with RADIUS accounting:

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# enable gprs
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

enable password

To set the enable password for privileged EXEC mode, use the **enable password** command in global configuration mode.

enable password *password* [**level** *level*] [**pbkdf2** | **encrypted**]

Syntax Description

encrypted (Optional) For 9.6 and earlier, specifies that the password is in encrypted form for passwords 32 characters and fewer. When you define a password in the **enable password** command, the ASA creates an MD5 hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **enable password** command does not show the actual password; it shows the encrypted password followed by the **encrypted** keword. For example, if you enter the password "test," the **show running-config** command output would appear to be something like the following:

```
enable password rvEdRh0xPC8bel7s encrypted
```

The only time you would actually enter the **encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password.

In 9.7 and later, passwords of all lengths use PBKDF2.

level *level* (Optional) Sets a password for a privilege level between 0 and 15.

password Sets the password as a case-sensitive string of 8 to 127 alphanumeric and special characters. You can use any character in the password with the following exceptions:

- No spaces
- No question marks
- You cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected:
  - **abc**user1
  - user**543**
  - user**aaaa**
  - user2**666**

pbkdf2 (Optional) Indicates that the password is encrypted. For 9.6 and earlier, the PBKDF2 (Password-Based Key Derivation Function 2) hash is used only when the password is more than 32 characters in length. In 9.7 and later, all passwords use PBKDF2. When you define a password in the **enable password** command, the ASA creates a PBKDF2 (Password-Based Key Derivation Function 2) hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **enable password** command does not show the actual password; it shows the encrypted password followed by the **pbkdf2** keyword. For example, if you enter a long password, the **show running-config** command output would appear to be something like the following:

```
username pat password rvEdRh0xPC8bel7s pbkdf2
```

The only time you would actually enter the **pbkdf2** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password.

Note that already existing passwords continue to use the MD5-based hash unless you enter a new password.

Command Default

The default password is blank. The default level is 15.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.6(1)	The password length was increased to 127 characters, and the **pbkdf2** keyword was added.
9.7(1)	Passwords of all lengths are now saved to the configuration using the PBKDF2 hash.
9.12(1)	The **no enable password** command is no longer supported.
9.17(1)	The minumum length was changed from 3 to 8 characters. Also you cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected: • **abc**user1 • user**543** • user**aaaa** • user2**666**

Usage Guidelines

The default password for enable level 15 (the default level) is blank, but you are prompted to change it the first time you enter the enable command. You cannot set the password to be blank.

At the CLI, you can access privileged EXEC mode using the **enable** command, the **login** command (with a user at privilege level 2+), or an SSH or Telnet session when you enable **aaa authorization exec auto-enable**. All of these methods require you to set the enable password.

This password change requirement is not enforced for ASDM logins. In ASDM, by default you can log in without a username and with the enable password.

For multiple context mode, you can create an enable password for the system configuration as well as for each context.

To use privilege levels other than the default of 15, configure local command authorization (see the **aaa authorization command** command and specify the **LOCAL** keyword), and set the commands to different privilege levels using the **privilege** command. If you do not configure local command authorization, the enable levels are ignored, and you have access to level 15 regardless of the level you set. See the **show curpriv** command to view your current privilege level.

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode.

Examples

The following example sets the enable password to Pa$$w0rd:

```
ciscoasa(config)# enable password Pa$$w0rd
```

The following example sets the enable password to Pa$$w0rd10 for level 10:

```
ciscoasa(config)# enable password Pa$$w0rd10 level 10
```

The following example sets the enable password to an encrypted password that you copied from another ASA:

```
ciscoasa(config)# enable password jMorNbK0514fadBh pbkdf2
```

Related Commands

Command	Description
aaa authorization command	Configures command authorization.
enable	Enters privileged EXEC mode.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config enable	Shows the enable passwords in encrypted form.

enable webvpn

To enable WebVPN access on a previously configured interface, use the **enable** command. Use this command in webvpn configuration mode.To disable WebVPN on an interface, use the **no** form of the command.

enable*ifname*
no enable

Syntax Description

ifname	Identifies the previously configured interface. Use the **nameif** command to configure interfaces.

Command Default

WebVPN is disabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to enable WebVPN on the interface named Outside:

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

encapsulation

To set the Network Virtualization Endpoint (NVE) instance to use VXLAN or Geneve encapsulation, use the **encapsulation** command in nve configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation
{
vxlan
| **geneve** [**port** *port_number* }
no encapsulation vxlan

Syntax Description

Syntax Description

vxlan	Specifies VXLAN encapsulation.
geneve	Specifies Geneve encapsulation. Geneve is only supported by the ASA virtual.
port *port_number*	For Geneve, sets the port number. The default is 6081.

Command Default

No default value.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nve configuration	• Yes	VXLAN: • Yes	• Yes	VXLAN: • Yes	—

Command History

Release	Modification
9.4(1)	This command was added.
9.17(1)	Added support for **geneve** for the ASA virtual.

Examples

The following example creates NVE instance 1 and sets the encapsulation to VXLAN:

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# encapsulation vxlan
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

encryption

To specify the encryption algorithm in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the encryption command in ikev2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]
no encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

Syntax Description

des	Specifies 56-bit DES-CBC encryption for ESP.
3des	(Default) Specifies the triple DES encryption algorithm for ESP.
aes	Specifies AES with a 128-bit key encryption for ESP.
aes-192	Specifies AES with a 192-bit key encryption for ESP.
aes-256	Specifies AES with a 256-bit key encryption for ESP.
aes-gcm	Specifies AES-GCM algorithm for IKEv2 encryption.
aes-gcm-192	Specifies AES-GCM algorithm for IKEv2 encryption.
aes-gcm-256	Specifies AES-GCM algorithm for IKEv2 encryption.
null	Choose null integrity algorithm if AES-GCM/GMAC is configured as the encryption algorithm.

Command Default

The default is 3DES.

Usage Guidelines

An IKEv2 SA is a key used in Phase 1 to enable IKEv2 peers to communicate securely in Phase 2. After entering the crypto ikev2 policy command, you can use the **encryption** command to set the SA encryption algorithm.

When OSPFv3 encryption is enabled on an interface, a delay may occur when you establish adjacencies while the IPsec tunnel is configured. Use the **show crypto sockets**, **show ipsec policy**, and **show ipsec sa** commands to determine the underlying IPsec tunnel status and to confirm that processing is occurring.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ikev2-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	The AES-GCM algorithm to use for IKEv2 encryption was added.

Examples

The following example enters ikev2-policy configuration mode and sets the encryption to AES-256:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# encryption aes-256
```

Related Commands

Command	Description
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
integrity	Specifies the ESP integrity algorithm in an IKEv2 SA for AnyConnect IPsec connections.
prf	Specifies the pseudo-random function in an IKEv2 SA for AnyConnect IPsec connections.
lifetime	Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections.

endpoint

To add an endpoint to an HSI group for H.323 protocol inspection, use the **endpoint** command in hsi group configuration mode. To disable this feature, use the **no** form of this command.

endpoint*ip_addressif_name*
no endpoint *ip_address if_name*

Syntax Description

if_name	The interface through which the endpoint is connected to the ASA.
ip_address	The IP address of the endpoint to add. A maximum of ten endpoints per HSI group is allowed.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Hsi-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to add endpoints to an HSI group in an H.323 inspection policy map:

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
hsi-group	Creates an HSI group.
hsi	Adds an HSI to the HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

endpoint-mapper

To configure endpoint mapper options for DCERPC inspection, use the **endpoint-mapper** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]
no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

Syntax Description

epm-service-only	Specifies to enforce endpoint mapper service during binding.
lookup-operation	Specifies to enable lookup operation of the endpoint mapper service.
timeout value	Specifies the timeout for pinholes from the lookup operation. The range is from 0:0:1 to 1193:0:0.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure the endpoint mapper in a DCERPC policy map:

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# endpoint-mapper epm-service-only
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **enforcenextupdate** command in ca-crl configuration mode. To permit a lapsed or missing NextUpdate field, use the **no** form of this command.

enforcenextupdate
no enforcenextupdate

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is enforced (on).

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If set, this command requires CRLs to have a NextUpdate field that has not yet lapsed. If not used, the ASA allows a missing or lapsed NextUpdate field in a CRL.

Examples

The following example enters crypto ca-crl configuration mode and requires CRLs to have a NextUpdate field that has not expired for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# enforcenextupdate
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
cache-time	Specifies a cache refresh time in minutes.
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.

enrollment protocol scep cmp est url

To specify automatic enrollment (for SCEP or CMP or EST) to enroll with this trustpoint and to configure enrollment URL, use the **enrollment protocol scep| cmp |est url** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment protocol scep | **cmp** | **est** *url*
no enrollment protocol scep | **cmp** | **est** *url*

Syntax Description

protocol	Distinguishes between a SCEP CA URL, a CMP CA URL, and a EST CA URL.

Command Default

The default setting is off.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-server configuration	• Yes	• Yes	• Yes	• Yes • No (for EST)	—

Command History

Release	Modification
9.7(1)	This command was added.
9.16(1)	This command was modified to include `est` as a valid protocol option.

Usage Guidelines

To be positioned as a Security Gateway device in wireless LTE networks, ASA supports some certificate management functions using the Certificate Management Protocol (CMPv2) in addition to SCEP and Enrollment over Secure Transport (EST). Using CMPv2 for enrollment of ASA device certificates, you can perform manual enrollment, for the first and secondary certificate from the CMPv2-enabled CA, or manual certificate updates, for replacement of a previously issued certificate using the same keypair. The received certificates are stored outside of the conventional configuration and are used in certificate-enabled IPsec configurations.

Examples

The following example shows the enrollment options:

```
(config)
# crypto ca trustpoint new(config-ca-trustpoint)# enrollment ?
crypto-ca-trustpoint mode commands/options: interface   Configure source interface protocol
   Enrollment protocol retry   Polling parameters self   Enrollment will generate a
self-signed certificate terminal   Enroll via the terminal (cut-and-paste)
asa(config-ca-trustpoint)# enrollment protocol ?
```

```
crypto-ca-trustpoint mode commands/options:
  cmp   Certificate Management Protocol Version 2
  est   Enrollment over Secure Transport
  scep  Simple Certificate Enrollment Protocol
asa(config-ca-trustpoint)# enrollment protocol est ?

crypto-ca-trustpoint mode commands/options:
  url CA server enrollment URL
asa(config-ca-trustpoint)# enrollment protocol est url ?

crypto-ca-trustpoint mode commands/options:
  LINE < 477 char  URL
asa(config-ca-trustpoint)# enrollment protocol est url https://xyz.com/est
```

enrollment-retrieval

To specify the time in hours that an enrolled user can retrieve a PKCS12 enrollment file, use the **enrollment-retrieval** command in local crypto ca-server configuration mode. To reset the time to the default number of hours (24), use the **no** form of this command.

enrollment-retrieval*timeout*
no enrollment-retrieval

Syntax Description

timeout	Specifies the number of hours users have to retrieve an issued certificate from the local CA enrollment web page. Valid timeout values range from 1 to 720 hours.

Command Default

By default, the PKCS12 enrollment file is stored and retrievable for 24 hours.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

A PKCS12 enrollment file contains an issued certificate and key pair. The file is stored on the local CA server and is available for retrieval from the enrollment web page for the time period specified with the **enrollment-retrieval** command.

When a user is marked as allowed to enroll, that user has the amount of time to enroll with that password specified in the **otp expiration** command. Once the user enrolls successfully, a PKCS12 file is generated, stored, and a copy is returned through the enrollment web page. The user can return for another copy of the file for any reason (such as when a download fails while trying enrollment) for the command time period specified in the **enrollment-retrieval** command.

Note This time is independent from the OTP expiration period.

Examples

The following example specifies that a PKCS12 enrollment file is available for retrieval from the local CA server for 48 hours after the certificate is issued:

```
ciscoasa(config)# crypto ca server
```

```
ciscoasa
(config-ca-server)
# enrollment-retrieval 48
ciscoasa
(config-ca-server)
#
```

The following example resets the retrieval time back to the default of 24 hours:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no enrollment-retrieval
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to ca-server configuration mode commands, which allow you to configure and manage the local CA.
OTP expiration	Specifies the duration in hours that an issued one-time password for the CA enrollment page is valid.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the CA server.
smtp subject	Specifies the text appearing in the subject field of all e-mails generated by the local CA server.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

enrollment retry count

To specify a retry count, use the **enrollment retry count** command in crypto ca-trustpoint configuration mode. To restore the default setting of the retry count, use the **no** form of the command.

enrollment retry count *number*
no enrollment retry count

Syntax Description

number	The maximum number of attempts to send an enrollment request. The valid values are 0, and 1-100 retries.

Command Default

The default setting for the *number* argument is 0 (unlimited).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

After requesting a certificate, the ASA waits to receive a certificate from the CA. If the ASA does not receive a certificate within the configured retry period, it sends another certificate request. The ASA repeats the request until either it receives a response or reaches the end of the configured retry period. This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and configures an enrollment retry count of 20 retries within the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry count 20
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

Command	Description
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

enrollment retry period

To specify a retry period, use the **enrollment retry period** command in crypto ca trustpoint configuration mode. To restore the default setting of the retry period, use the **no** form of the command.

enrollment retry period *minutes*
no enrollment retry period

Syntax Description

minutes	The number of minutes between attempts to send an enrollment request. The valid range is 1- 60 minutes.

Command Default

The default setting is 1 minute.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

After requesting a certificate, the ASA waits to receive a certificate from the CA. If the ASA does not receive a certificate within the specified retry period, it sends another certificate request. This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and configures an enrollment retry period of 10 minutes within the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry period 10
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns all enrollment parameters to their system default values.
enrollment retry count	Defines the number of retries to requesting an enrollment.

enrollment terminal

To specify cut and paste enrollment with this trustpoint (also known as manual enrollment), use the **enrollment terminal** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment terminal
no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is off.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and specifies the cut-and-paste method of CA enrollment for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

Command	Description
enrollment url	Specifies automatic enrollment (SCEP) with this trustpoint and configures the URL.

enrollment url (Deprecated)

To specify automatic enrollment (SCEP) to enroll with this trustpoint and to configure the enrollment URL, use the **enrollment url** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment url *url*
no enrollment url url

Syntax Description

url	Specifies the name of the URL for automatic enrollment. The maximum length is 1K characters (effectively unbounded).

Command Default

The default setting is off.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and specifies SCEP enrollment at the URL https://enrollsite for trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url https://enrollsite
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

Command	Description
enrollment terminal	Specifies cut-and-paste enrollment with this trustpoint.

eool

To define an action when the End of Options List (EOOL) option occurs in a packet header with IP Options inspection, use the **eool** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

eool action { **allow** | **clear** }
no eool action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the End of Options List IP option.
clear	Remove the End of Options List option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the End of Options List IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

The End of Options List option, which contains just a single zero byte, appears at the end of all options to mark the end of a list of options. This might not coincide with the end of the header according to the header length.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

eou allow (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To enable clientless authentication in a NAC Framework configuration, use the **eou allow** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

eou allow { **audit** | **clientless** | **none** }
no eou allow { **audit** | **clientless** | **none** }

Syntax Description

audit	Performs clientless authentication.
clientless	Performs clientless authentication.
none	Disables clientless authentication.

Command Default

The default configuration contains the **eou allow clientless** configuration.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The **audit** option was added.
9.1(2)	This command was deprecated.

Usage Guidelines

The ASA uses this command only if both of the following are true:

- The group policy is configured to use a NAC Framework NAC policy type.
- A host on the session does not respond to EAPoUDP requests.

Examples

The following example enables the use of an ACS to perform clientless authentication:

```
ciscoasa(config)# eou allow clientless
ciscoasa(config)#
```

The following example shows how to configure the ASA to use an audit server to perform clientless authentication:

```
ciscoasa(config)# eou allow audit
ciscoasa(config)#
```

The following example shows how to disable the use of an audit server:

```
ciscoasa(config)# no eou allow clientless
ciscoasa(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou clientless	Changes the username and password to be sent to the ACS for clientless authentication in a NAC Framework configuration.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou clientless (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the username and password to be sent to the Access Control Server for clientless authentication in a NAC Framework configuration, use the **eou clientless** command in global configuration mode. To use the default value, use the **no** form of this command.

eou clientless username *username* **password** *password*
no eou clientless username *username* **password** *password*

Syntax Description

password	Enter to change the password sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
password	Enter the password configured on the Access Control Server to support clientless hosts. Enter 4-32 ASCII characters.
username	Enter to change the username sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
username	Enter the username configured on the Access Control Server to support clientless hosts. Enter 1-64 ASCII characters, excluding leading and trailing spaces, pound signs (#), question marks (?), quotation marks ("), asterisks (*), and angle brackets (< and >).

Command Default

The default value for both the username and password attributes is clientless.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.

- Clientless authentication is enabled on the ASA.
- NAC is configured on the ASA.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the username for clientless authentication to sherlock:

```
ciscoasa(config)# eou clientless username sherlock
ciscoasa(config)#
```

The following example changes the username for clientless authentication to the default value, clientless:

```
ciscoasa(config)# no eou clientless username
ciscoasa(config)#
```

The following example changes the password for clientless authentication to secret:

```
ciscoasa(config)# eou clientless password secret
ciscoasa(config)#
```

The following example changes the password for clientless authentication to the default value, clientless:

```
ciscoasa(config)# no eou clientless password
ciscoasa(config)#
```

Related Commands

Command	Description
eou allow	Enables clientless authentication in a NAC Framework configuration.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.

eou initialize (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To clear the resources assigned to one or more NAC Framework sessions and initiate a new, unconditional posture validation for each of the sessions, use the **eou initialize** command in privileged EXEC mode.

eou initialize { **all** | **group** *tunnel-group* | **ip** *ip-address* }

Syntax Description

all	Revalidates all NAC Framework sessions on this ASA
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Command Default

No default behavior or values.

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

Use this command if a change occurs in the posture of the remote peers or if the assigned access policies (that is, the downloaded ACLs) change, and you want to clear the resources assigned to the sessions. Entering this command purges the EAPoUDP associations and access policies used for posture validation. The NAC default ACL is effective during the revalidations, so the session initializations can disrupt user traffic. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example initializes all NAC Framework sessions:

```
ciscoasa# eou
initialize all
ciscoasa
```

The following example initializes all NAC Framework sessions assigned to the tunnel group named tg1:

```
ciscoasa# eou
initialize group tg1
ciscoasa
```

The following example initializes the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
ciscoasa# eou
initialize
209.165.200.225
ciscoasa
```

Related Commands

Command	Description
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
debug nac	Enables logging of NAC Framework events.

eou max-retry (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the number of times the ASA resends an EAP over UDP message to the remote computer, use the **eou max-retry** command in global configuration mode. To use the default value, use the **no** form of this command.

eou max-retry *retries*
no eou max-retry

Syntax Description

retries	Limits the number of consecutive retries sent in response to retransmission timer expirations. Enter a value in the range of 1 to 3.

Command Default

The default value is 3.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.
- Clientless authentication is enabled on the ASA.
- NAC is configured on the ASA.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example limits the number of EAP over UDP retransmissions to 1:

```
ciscoasa(config)# eou max-retry 1
ciscoasa(config)#
```

The following example changes the number of EAP over UDP retransmissions to its default value, 3:

```
ciscoasa(config)# no eou max-retry
ciscoasa(config)#
```

Related Commands

eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou port (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the port number for EAP over UDP communication with the Cisco Trust Agent in a NAC Framework configuration, use the eou port command in global configuration mode. To use the default value, use the **no** form of this command.

eou port *port_number*
no eou port

Syntax Description

port_number	Port number on the client endpoint to be designated for EAP over UDP communications. This number is the port number configured on the Cisco Trust Agent. Enter a value in the range of 1024 to 65535.

Command Default

The default value is 21862.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the port number for EAP over UDP communication to 62445:

```
ciscoasa(config)# eou port 62445
ciscoasa(config)#
```

The following example changes the port number for EAP over UDP communication to its default value:

```
ciscoasa(config)# no eou port
ciscoasa(config)#
```

Related Commands

debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
show vpn-session.db	Displays information about VPN sessions, including VLAN mapping and NAC results.
show vpn-session_summary.db	Displays the number IPsec, Cisco Secure Client, and NAC sessions, including VLAN mapping session data.

eou revalidate (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To force immediate posture revalidation of one or more NAC Framework sessions, use the **eou revalidate** command in privileged EXEC mode.

eou revalidate { **all** | **group** *tunnel-group* | **ip** *ip-address* }

Syntax Description

all	Revalidates all NAC Framework sessions on this ASA
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Command Default

No default behavior or values.

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

Use this command if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed. The command initiates a new, unconditional posture validation. The posture validation and assigned access policy that were in effect before you entered the command remain in effect until the new posture validation succeeds or fails. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example revalidates all NAC Framework sessions:

```
ciscoasa# eou
```

```
revalidate all
ciscoasa
```

The following example revalidates all NAC Framework sessions assigned to the tunnel group named tg-1:

```
ciscoasa# eou
revalidate group tg-1
ciscoasa
```

The following example revalidates the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
ciscoasa# eou
revalidate ip
209.165.200.225
ciscoasa
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.

eou timeout (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To change the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration, use the eou timeout command in global configuration mode. To use the default value, use the **no** form of this command.

eou timeout { **hold-period** | **retransmit** } *seconds*
no eou timeout { **hold-period** | **retransmit** }

Syntax Description

hold-period	Maximum time to wait after sending EAPoUDP messages equal to the number of EAPoUDP retries. The **eou initialize** or **eou revalidate** command also clears this timer. If this timer expires, the ASA initiates a new EAP over UDP association with the remote host.
retransmit	Maximum time to wait after sending an EAPoUDP message. A response from the remote host clears this timer. The **eou initialize** or **eou revalidate** command also clears this timer. If the timer expires, the ASA retransmits the EAPoUDP message to the remote host.
seconds	Number of seconds for the ASA to wait. Enter a value in the range of 60 to 86400 for the hold-period attribute, or the range of 1 to 60 for the retransmit attribute.

Command Default

The default value of the **hold-period** option is 180.

The default value of the **retransmit** option is 3.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the wait period before initiating a new EAP over UDP association to 120 seconds:

```
ciscoasa(config)# eou timeout hold-period 120
ciscoasa(config)#
```

The following example changes the wait period before initiating a new EAP over UDP association to its default value:

```
ciscoasa(config)# no eou timeout hold-period
ciscoasa(config)#
```

The following example changes the retransmission timer to 6 seconds:

```
ciscoasa(config)# eou timeout retransmit 6
ciscoasa(config)#
```

The following example changes the retransmission timer to its default value:

```
ciscoasa(config)# no eou timeout retransmit
ciscoasa(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou max-retry	Changes the number of times the ASA resends an EAP over UDP message to the remote computer.

erase

To erase and reformat the file system, use the **erase** command in privileged EXEC mode. This command overwrites all files and erases the file system, including hidden system files, then reinstalls the file system.

erase [**disk0:** | **disk1:** | **flash:**]

Syntax Description

disk0: (Optional) Specifies the internal compact Flash memory card, followed by a colon.

disk1: (Optional) Specifies the external compact Flash memory card, followed by a colon.

flash: (Optional) Specifies the internal Flash memory, followed by a colon.

Caution Erasing the flash memory also removes the licensing information, which is stored in flash memory. Save the licensing information before erasing the flash memory.

On the ASA 5500 series, the **flash** keyword is aliased to **disk0:**.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **erase** command erases all data in the flash memory using the 0xFF pattern and then rewrites an empty file system allocation table to the device.

To delete all visible files (excluding hidden system files), enter the **delete /recursive** command, instead of the **erase** command.

Note On the ASA 5500 series, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information.

Examples

The following example erases and reformats the file system:

```
ciscoasa# erase flash:
```

Related Commands

Command	Description
delete	Removes all visible files, excluding hidden system files.
format	Erases all files (including hidden system files) and formats the file system.

esp

To specify parameters for ESP and AH tunnels for IPsec Pass-Through inspection, use the **esp** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

{ **esp** | **ah** } [**per-client-max** *num*] [**timeout** *time*]
no { **esp** | **ah** } [**per-client-max** *num*] [**timeout** *time*]

Syntax Description

esp	Specifies parameters for the ESP tunnel.
ah	Specifies parameters for the AH tunnel.
per-client-max num	Specifies the maximum number of tunnels from one client.
timeout time	Specifies the idle timeout for the ESP tunnel.

Command Default

This command is disabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to permit UDP 500 traffic:

```
ciscoasa(config)# access-list test-udp-acl extended permit udp any any eq 500
ciscoasa(config)# class-map test-udp-class
ciscoasa(config-pmap-c)# match access-list test-udp-acl
ciscoasa(config)# policy-map type inspect ipsec-pass-thru ipsec-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
ciscoasa(config-pmap-p)# ah per-client-max 16 timeout 00:05:00
ciscoasa(config)# policy-map test-udp-policy
ciscoasa(config-pmap)# class test-udp-class
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

established

To permit return connections on ports that are based on an established connection, use the **established** command in global configuration mode. To disable the established feature, use the **no** form of this command.

established est_protocol *dest_port* [**source_port**] [**permitto protocol port** [**-port**]] [**permitfrom protocol** *port* [**-port**]]
no established est_protocol *dest_port* [**source_port**] [**permitto protocol port** [**-port**]] [**permitfrom protocol** *port* [**-port**]]

Syntax Description

est_protocol	Specifies the IP protocol (UDP or TCP) to use for the established connection lookup.
dest_port	Specifies the destination port to use for the established connection lookup.
permitfrom	(Optional) Allows the return protocol connection(s) originating from the specified port.
permitto	(Optional) Allows the return protocol connections destined to the specified port.
port [-port]	(Optional) Specifies the (UDP or TCP) destination port(s) of the return connection.
protocol	(Optional) IP protocol (UDP or TCP) used by the return connection.
source_port	(Optional) Specifies the source port to use for the established connection lookup.

Command Default

The defaults are as follows:

- *dest_port*—0 (wildcard)
- *source_port*—0 (wildcard)

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The keywords **to** and **from** were removed from the CLI. Use the keywords **permitto** and **permitfrom** instead.

Usage Guidelines

The established command lets you permit return access for outbound connections through the ASA. This command works with an original connection that is outbound from a network and protected by the ASA and a return connection that is inbound between the same two devices on an external host. The established command

lets you specify the destination port that is used for connection lookups. This addition allows more control over the command and provides support for protocols where the destination port is known, but the source port is unknown. The permitto and permitfrom keywords define the return inbound connection.

Caution We recommend that you always specify the established command with the permitto and permitfrom keywords. Using the established command without these keywords is a security risk because when connections are made to external systems, those system can make unrestricted connections to the internal host involved in the connection. This situation can be exploited for an attack of your internal systems.

Examples

The following set of examples shows potential security violations could occur if you do not use the established command correctly.

This example shows that if an internal system makes a TCP connection to an external host on port 4000, then the external host could come back in on any port using any protocol:

```
ciscoasa(config)# established tcp 4000 0
```

You can specify the source and destination ports as **0** if the protocol does not specify which ports are used. Use wildcard ports (0) only when necessary.

```
ciscoasa(config)# established tcp 0 0
```

Note To allow the established command to work correctly, the client must listen on the port that is specified with the permitto keyword.

You can use the established command with the nat 0 command (where there are no global commands).

Note You cannot use the established command with PAT.

The ASA supports XDMCP with assistance from the **established** command.

Caution Using XWindows system applications through the ASA may cause security risks.

XDMCP is on by default, but it does not complete the session unless you enter the established command as follows:

```
ciscoasa(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

Entering the **established** command enables the internal XDMCP-equipped (UNIX or ReflectionX) hosts to access external XDMCP-equipped XWindows servers. UDP/177-based XDMCP negotiates a TCP-based XWindows session, and subsequent TCP back connections are permitted. Because the source port(s) of the return traffic is unknown, specify the *source_port* field as 0 (wildcard). The *dest_port* should be 6000 + *n*, where *n* represents the local display number. Use this UNIX command to change this value:

```
ciscoasa(config)# setenv DISPLAY
 hostname:displaynumber.screennumber
```

The **established** command is needed because many TCP connections are generated (based on user interaction) and the source port for these connections is unknown. Only the destination port is static. The ASA performs XDMCP fixups transparently. No configuration is required, but you must enter the **established** command to accommodate the TCP session.

The following example shows a connection between two hosts using protocol A destined for port B from source port C. To permit return connections through the ASA and protocol D (protocol D can be different from protocol A), the source port(s) must correspond to port F and the destination port(s) must correspond to port E.

```
ciscoasa(config)# established A B C permitto D E permitfrom D F
```

The following example shows how a connection is started by an internal host to an external host using TCP destination port 6060 and any source port. The ASA permits return traffic between the hosts through TCP destination port 6061 and any TCP source port.

```
ciscoasa(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

The following example shows how a connection is started by an internal host to an external host using UDP destination port 6060 and any source port. The ASA permits return traffic between the hosts through TCP destination port 6061 and TCP source port 1024-65535.

```
ciscoasa(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

The following example shows how a local host starts a TCP connection on port 9999 to a foreign host. The example allows packets from the foreign host on port 4242 back to local host on port 5454.

```
ciscoasa(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

Related Commands

Command	Description
clear configure established	Removes all established commands.
show running-config established	Displays the allowed inbound connections that are based on established connections.

event crashinfo

To trigger an event manager applet when a crash occurs on the ASA, use the **event crashinfo** command in event manager applet configuration mode. To remove the crash event, use the **no** form of this command.

event crashinfo
no event crashinfo

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Regardless of the value of the **output** command, the **action** commands are directed to the crash information file. The output is generated before the **show tech** command.

Note The state of the ASA is generally unknown when it crashes. Some CLI commands may not be safe to run during this condition.

Examples

The following example triggers an applet when the ASA crashes:

```
ciscoasa(config-applet)# event crashinfo
```

Related Commands

Command	Description
event none	Invokes an event manager applet manually.
event syslog id	Adds a syslog event to an event manager applet.
event timer absolute time	Configures an absolute event timer.

Command	Description
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

event manager applet

To create or edit an event manager applet that links events with actions and output, use the event manager applet command in global configuration mode. To remove an event manager applet, use the **no** form of this command.

event manager applet *name*
no event manager applet *name*

Syntax Description

name	Specifies the name of the event manager applet. The name can be up to 32 characters long.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use the **event manager applet** command to enter event manager applet configuration mode.

Examples

The following example creates an event manager applet and enters event manager applet configuration mode:

```
ciscoasa(config)# event manager applet appletexample1
ciscoasa(config-applet)#
```

Related Commands

Command	Description
description	Describes an applet.
event manager run	Runs an event manager applet.
show event manager	Shows statistical information for each configured event manager applet.
debug event manager	Manages debugging traces for the event manager.

event memory-logging-wrap

To configure a memory logging wrap event trigger, use the **event memory-logging-wrap** command in event manager applet configuration mode.

event memory-logging-wrap

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuratio	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

When wrap is enabled for memory logging, the memory logger sends an event to the event manager to trigger configured applets.

Examples

The following example shows an applet that records all memory allocations:

```
ciscoasa(config-applet)# event manager applet memlog
ciscoasa(config-applet)# event memory-logging-wrap
ciscoasa(config-applet)# action 0 cli command "show memory logging wrap"
ciscoasa(config-applet)# output file append disk0:/memlog.log
```

Related Commands

Command	Description
memory logging	Enables memory logging.
show memory logging	Shows the results of memory logging.

event none

To invoke an event manager applet manually, use the **event none** command in event manager applet configuration mode. To remove a manual invocation, use the **no** form of this command.

event none
no event none

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

You can configure any other event with the **event none** command.

Examples

The following example invokes an event manager applet manually:

```
ciscoasa(config-applet)# event none
```

Related Commands

Command	Description
event crashinfo	Triggers an event manager applet when a crash occurs on the ASA.
event syslog id	Adds a syslog event tor an event manager applet.
event timer absolute time	Configures an absolute event timer.
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

event syslog id

To add a syslog event to an event manager applet, use the **event syslog id** command in event manager applet configuration mode. To remove a syslog event from an event manager applet, use the **no** form of this command.

event syslog id *nnnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]
no event syslog id *nnnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

Syntax Description

nnnnnn	Identifies the syslog message ID.
occurs *n*	Indicates the number of times that the syslog message must occur for the applet to be invoked. The default is 1. Valid values are from 1 - 4294967295.
period *seconds*	Indicates the number of seconds in which the event must occur, and limits how frequently the applet is invoked to at most once in the configured period. Valid values are from 0 - 604800. A value of 0 means that no period is defined.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use the **event syslog id** command to identify a single syslog message or a range of syslog messages that trigger an applet.

Examples

The following example indicates that syslog message 106201 triggers an applet:

```
ciscoasa(config-applet)# event syslog id 106201
```

Related Commands

Command	Description
event crashinfo	Triggers an event manager applet when a crash occurs on the ASA.
event none	Invokes an event manager applet manually.

Command	Description
event timer absolute time	Configures an absolute event timer.
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

event timer

To configure timer events, use the **event timer** command in event manager applet configuration mode. To remove timer events, use the **no** form of this command.

event timer { **watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss* }
no event timer { **watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss* }

Syntax Description

absolute time	Specifies that an event occurs once a day at a specified time and restarts automatically.
countdown time	Specifies that an event occurs once and does not restart unless it is removed, then re-added.
hh:mm:ss	Specifies the time-of-day format. The time range is from 00:00:00 (midnight) to 23:59:59.
seconds	Specifies the number of seconds. Valid values range from 0 - 604800. A value of 0 disables the timer.
watchdog time	Specifies that an event occurs once per configured period and restarts automatically.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use the **event timer absolute time** command to cause an event to occur once a day at a specified time and restart automatically.

Use the **event timer countdown time** command to cause an event to occur once and not restart unless it is removed, then re-added.

Use the **event timer watchdog time** command to cause an event to occur once per configured period and restart automatically.

Examples

The following example causes an event to occur once a day at the specified time shown:

```
ciscoasa(config-applet)# event timer absolute time 10:30:20
```

The following example causes an event to occur once a day at the specified time shown:

```
ciscoasa(config-applet)# event timer countdown time 10:30:20
```

The following example causes an event to occur once a day and restart automatically:

```
ciscoasa(config-applet)# event timer watchdog time 30
```

Related Commands

Command	Description
event crashinfo	Triggers an event manager applet when a crash occurs on the ASA.
event none	Invokes an event manager applet manually.
event syslog id	Adds a syslog event to an event manager applet.
event timer countdown time	Configures a countdown timer event.
event timer watchdog time	Configures a watchdog timer event.

exceed-mss

To allow or drop packets whose data length exceeds the TCP maximum segment size (MSS) set by the peer during a three-way handshake, use the **exceed-mss** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

exceed-mss { **allow** | **drop** }
no exceed-mss { **allow** | **drop** }

Syntax Description

allow	Allows packets that exceed the MSS. This setting is the default.
drop	Drops packets that exceed the MSS.

Command Default

Packets are allowed by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)/8.0(4)	The default was changed from **drop** to **allow**.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **exceed-mss** command in tcp-map configuration mode to drop TCP packets whose data length exceed the TCP maximum segment size set by the peer during a three-way handshake.

Examples

The following example drops flows on port 21 if they are in excess of MSS:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# exceed-mss drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
```

```
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection advanced-options	Configures advanced connection features, including TCP normalization.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

exempt-list

To add an entry to the list of remote computer types that are exempt from posture validation, use the **exempt-list** command in nac-policy-nac-framework configuration mode. To remove an entry from the exemption list, use the **no** form of this command and name the operating system and ACL in the entry to be removed.

exempt-list os " *os-name* **"** [**disable** | **filter** *acl-name* [**disable**]]
no exempt-list os " *os-name* **"** [**disable** | **filter** *acl-name* [**disable**]]

Syntax Description

acl-name	Name of the ACL present in the ASA configuration. When specified, it must follow the **filter** keyword.
disable	Performs one of two functions, as follows: • If you enter it after the "os-name," the ASA ignores the exemption, and applies NAC posture validation to the remote hosts that are running that operating system. • If you enter it after the *acl-name* , ASA exempts the operating system, but does not assign the ACL to the associated traffic.
filter	Applies an ACL to filter the traffic if the computer's operating system matches the *os name* . The filter/*acl-name* pair is optional.
os	Exempts an operating system from posture validation.
os name	Operating system name. Quotation marks are required only if the name includes a space (for example, "Windows XP").

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nac-policy-nac-framework configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The command name was changed from **vpn-nac-exempt** to **exempt-list**. The command was moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.

Usage Guidelines

When the command specifies an operating system, it does not overwrite the previously added entry to the exception list; enter the command once for each operating system and ACL that you want to exempt.

The **no exempt-list** command removes all exemptions from the NAC Framework policy. Specifying an entry when issuing the **no** form of the command removes the entry from the exemption list.

To remove all entries from the exemption list associated with this NAC policy, use the **no** form of this command without specifying additional keywords.

Examples

The following example adds all hosts running Windows XP to the list of computers that are exempt from posture validation:

```
ciscoasa(config-group-policy)# exempt-list os "Windows XP"
ciscoasa(config-group-policy)
```

The following example exempts all hosts running Windows XP and applies the ACL acl-1 to traffic from those hosts:

```
ciscoasa(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

The following example removes the same entry from the exemption list:

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

The following example removes all entries from the exemption list:

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list
ciscoasa(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
debug nac	Enables logging of NAC Framework events.
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
nac-settings	Assigns a NAC policy to a group policy.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
show vpn-session_summary.db	Displays the number of IPsec, Cisco Secure Client, and NAC sessions.

exit

To exit the current configuration mode, or to logout from privileged or user EXEC modes, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can also use the key sequence **Ctrl+Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **exit** command in privileged or user EXEC modes, you log out from the ASA. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Examples

The following example shows how to use the **exit** command to exit global configuration mode, then log out from the session:

```
ciscoasa(config)# exit
ciscoasa# exit
Logoff
```

The following example shows how to use the **exit** command to exit global configuration mode, then use the **disable** command to exit privileged EXEC mode:

```
ciscoasa(config)# exit
ciscoasa# disable
ciscoasa#
```

Related Commands

Command	Description
quit	Exits a configuration mode or logs out of the privileged or user EXEC modes.

exp-flow-control

To define an action when the Experimental Flow Control (FINN) option occurs in a packet header with IP Options inspection, use the **exp-flow-control** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

exp-flow-control action { **allow** | **clear** }
no exp-flow-control action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Experimental Flow Control IP option.
clear	Remove the Experimental Flow Control option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Experimental Flow Control IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-flow-control action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

expire-entry-timer

To set the expiration timer for fully-qualified domain names (FQDN) specified in network objects, use the **expire-entry-timer** command in dns server-group configuration mode. To remove the timer, use the **no** form of this command.

expire-entry-timer minutes *minutes*
no expire-entry-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer time in minutes. Valid values range from 1 to 65535 minutes.

Command Default

By default, the DNS expire-entry-timer value is 1 minute.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	This command was added.
9.17(1)	The behavior of the command was changed to set a minimum TTL, rather than extend the TTL, of DNS resolutions.

Usage Guidelines

This command is supported for the DefaultDNS server group, or the active server group, only. It sets the expiration timer for fully-qualified domain names (FQDN) specified in network objects. It applies only to these FQDN, and does not apply to any FQDN resolved for other purposes.

Up to version 9.16, the command specifies the time to remove the IP address of a resolved FQDN after its TTL expires. When the IP address is removed, the ASA recompiles the tmatch lookup table. The default DNS expire-entry-timer value is 1 minute, which means that IP addresses are removed 1 minute after the TTL (time to live) of the DNS entry expires.

Starting with 9.17, the command specifies a minimum TTL for the DNS entry. If the expiration timer is longer than the entry's TTL, the TTL is increased to the expire entry time value. If the TTL is longer than the expiration timer, the expire entry time value is ignored: no additional time is added to the TTL in this case.

Note The default setting might result in frequent recompilation of the tmatch lookup table when the resolved TTL of common FQDN hosts, such as www.example.com, is a short time period. You can specify a long DNS expire-entry timer value to reduce the frequency of recompilation of the tmatch lookup table while maintaining security.

Examples

The following example removes resolved entries after 240 minutes:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# expire-entry-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

expiry-time

To configure an expiration time for caching objects without revalidating them, use the **expiry-time** command in cache configuration mode. To remove the expiration time from the configuration and reset it to the default value, use the **no** form of this command.

expiry-time*time*
no expiry-time

Syntax Description

time	The amount of time in minutes that the ASA caches objects without revalidating them.

Command Default

The default is 1 minute.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cache configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The expiration time is the amount of time in minutes that the ASA caches an object without revalidating it. Revalidation consists of rechecking the content.

Examples

The following example shows how to set an expiration time with a value of 13 minutes:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)#expiry-time 13
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters webvpn cache configuration mode.
cache-compressed	Configures WebVPN cache compression.

Command	Description
disable	Disables caching.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum size of an object to cache.

exp-measure

To define an action when the Experimental Measurement (ZSU) option occurs in a packet header with IP Options inspection, use the **exp-measure** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

exp-measure action { **allow** | **clear** }
no exp-measure action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Experimental Measurement IP option.
clear	Remove the Experimental Measurement option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Experimental Measurement IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-measure action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

export

To specify the certificate to be exported to the client, use the export command in ctl-provider configuration mode. To remove the configuration, use the **no** form of this command.

export certificate *trustpoint_name*
no export certificate [*trustpoint_name*]

Syntax Description

certificate *trustpoint_name*	Specifies the certificate to be exported to the client.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl-provider configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the export command in ctl-provider configuration mode to specify the certificate to be exported to the client. The trustpoint name is defined by the crypto ca trustpoint command. The certificate will be added to the CTL file composed by the CTL client.

Examples

The following example shows how to create a CTL provider instance:

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in ctl-provider configuration mode.

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and the username and password for client authentication.
service	Specifies the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

export webvpn AnyConnect-customization

To export a customization object *that customizes the AnyConnect client GUI*, use the **export webvpn AnyConnect-customization** command in privileged EXEC mode:

export webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
type	The type of customization: • binary—An executable that replaces the Secure Client GUI. • transform—A transform that customizes the MSI.
url	Remote path and filename to export the XML customization object, in the form *URL/filename* (the maximum number is 255 characters).

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An Secure Client customization object is an XML file that resides in cache memory, and customizes the GUI screens for Secure Client users. When you export a customization object, an XML file containing XML tags is created at the URL you specify.

The XML file created by the customization object named *Template* contains empty XML tags, and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory, but can be exported, edited, and imported back into the ASA as a new customization object.

The content of *Template* is the same as the initial DfltCustomization object state.

For a complete list of resource files used the Secure Client GUI and their filenames, see the AnyConnect VPN Client Administrator Guide.

Examples

The following example exports the Cisco logo used on the Secure Client GUI:

```
ciscoasa# export webvpn AnyConnect-customization type resource company_logo.bmp
tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn customization

To export a customization object *that customizes screens visible to Clientless SSL VPN users*, use the **export webvpn customization** command in privileged EXEC mode.

export webvpn customization *name url*

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
url	Remote path and filename to export the XML customization object, in the form *URL/filename* (the maximum number is 255 characters).

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A customization object is an XML file that resides in cache memory, and customizes the screens visible to Clientless SSL VPN users, including login and logout screens, the portal page, and available languages. When you export a customization object, an XML file containing XML tags is created at the URL that you specify.

The XML file created by the customization object named *Template* contains empty XML tags, and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory, but can be exported, edited, and imported back into the ASA as a new customization object.

The content of *Template* is the same as the initial DfltCustomization object state.

You can export a customization object using the **export webvpn customization** command, make changes to the XML tags, and import the file as a new object using the **import webvpn customization** command.

Examples

The following example exports the default customization object (DfltCustomization) and creates the resulting XML file named dflt_custom:

```
ciscoasa# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
```

```
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn plug-in

To export a plug-in from the flash device of the ASA, enter the **export webvpn plug-in** command in privileged EXEC mode.

import webvpn plug-in protocol *protocol URL*

Syntax Description

protocol

- **citrix**

The Citrix plugin lets the remote user connect to a computer running Citrix Metaframe services.

- **rdp**

The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes. The web site containing the original is http://properjavardp.sourceforge.net/ .

- **ssh,telnet**

The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer. Cisco redistributes this plug-in without any changes. The web site containing the original is http://javassh.org/ .

Caution The **export webvpn plug-in protocol ssh,telnet** *URL* command exports *both* the SSH and Telnet plug-ins. Do *not* enter this command once for SSH and once for Telnet. When typing the **ssh,telnet** string, do *not* insert a space.

- **vnc**

The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes. The web site containing the original is http://www.tightvnc.com/ .

URL — Path to the remote device.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Exporting a plug-in does not remove it from flash. Exporting creates a copy of the plug-in at the specified URL.

Examples

The following command adds WebVPN support for Citrix:

```
ciscoasa# import webvpn plug-in protocol citrix tftp://209.165.201.22/plugins/ica-plugin.zip
Accessing
tftp://209.165.201.22/plugins/ica-plugin.zip...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/citrix...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
554543 bytes copied in 13.270 secs (42657 bytes/sec)
```

The following command exports the RDP plugin:

```
ciscoasa# export webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
```

Related Commands

Command	Description
import webvpn plugin	Imports a specified plug-in from a local device to the ASA flash.
revert webvpn plug-in protocol	Removes the specified plug-in from the flash device of the ASA.
show import webvpn plug-in	Lists the plug-ins present on the flash device of the ASA.

export webvpn mst-translation

To export a Microsoft transform (MST) *that translates the AnyConnect installer program,* use the **export webvpn mst-translation** command in privileged EXEC mode:

export webvpn mst-translation *component* **language** *language* **URL**

Syntax Description

component	The component to which this MST applies. The only valid choice is Secure Client.
language	The language code of the MST exported. Use the code in the same format that the browser requires.
URL	The remote path and filename to export the transform to, in the form *URL/filename* (the maximum number is 255 characters).

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

As with the Secure Client GUI, you can translate messages displayed by the client installer program. The ASA uses transforms to translate the messages displayed by the installer. The transform alters the installation, but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.

Each language has its own transform. You can edit a transform with a transform editor such as Orca, and make changes to the message strings. Then you import the transform to the ASA. When the user downloads the client, the client detects the preferred language of the computer (the locale specified during installation of the operating system) and applies the appropriate transform.

We currently offer transforms for 30 languages. These transforms are available in the following .zip file on the Secure Client software download page at cisco.com:

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

In this file, <VERSION> is the version of Secure Client release (for exmaple, 2.2.103).

Examples

The following example exports the English language transform as AnyConnect_Installer_English:

```
ciscoasa# export webvpn mst-translation AnyConnect language es tftp://209.165.200.225/
AnyConnect_Installer_English
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn translation-table

To export a translation table used to translate terms displayed to remote users establishing SSL VPN connections, use the **export webvpn translation-table** command in privileged EXEC mode.

export webvpn webvpn *translation_domain* { **language** *language* | **template** } *url*

Syntax Description

language	Specifies the name of a previously imported translation table. Enter the value in the manner expressed by your browser language options.
translation_domain	The functional area and associated messages. Table 14-1 lists available translation domains.
url	Specifies the URL of the object.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The ASA provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

Each functional area and its messages that are visible to remote users has its own translation domain, which are specified by the *translation_domain argument*. Table 14-1 shows the translation domains and the functional areas translated.

Table 1: Translation Domains and Functional Areas Affected

Translation Domain	Functional Areas Translated
AnyConnect	*Messages displayed on the user interface of the Cisco AnyConnect VPN Client.*
banners	Banners displayed to remote users and messages when VPN access is denied.

Translation Domain	Functional Areas Translated
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	*Messages on the login and logout pages, portal page, and all the messages customizable by the user.*
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA, and portal messages that are not customizable.

Usage Guidelines

A translation template is an XML file in the same format as the translation table, but has all the translations empty. The software image package for the ASA includes a template for each domain that is part of the standard functionality. Templates for plug-ins are included with the plug-ins and define their own translation domains. Because you can customize the *login and logout pages, portal page, and URL bookmarks for clientless users,* the ASA **generates the** customization and url-list translation domain templates dynamically, and the template automatically reflects your changes to these functional areas.

Exporting a previously-imported translation table creates an XML file of the table at the URL location. You can view a list of available templates and previously-imported tables using the **show import webvpn translation-table** command.

Download a template or translation table using the **export webvpn translation-table** command, make changes to the messages, and import the translation table using the **import webvpn translation-table** command.

Examples

The following example exports a template for the translation domain *customization* , which is used to translate the *login and logout pages, portal page, and all the messages customizable and visible to remote users establishing clientless SSL VPN connections. The* ASA *creates the XML file with the name >Sales:*

```
ciscoasa# export webvpn translation-table customization template tftp://209.165.200.225/Sales
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The following example exports a previously imported translation table for the Chinese language named >*zh* , an abbreviation compatible with the abbreviation specified for Chinese in the Internet Options of the Microsoft Internet Explorer browser. The ASA *creates the XML file with the name >Chinese* :

```
ciscoasa# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Related Commands

Command	Description
import webvpn translation-table	Imports a translation table.
revert	Removes translation tables from cache memory.
show import webvpn translation-table	Displays information about imported translation tables.

export webvpn url-list

To export a URL list to a remote location, use the **export webvpn url-list** command in privileged EXEC mode.

export webvpn url-list *name url*

Syntax Description

name	The name that identifies the URL list. The maximum number is 64 characters.
url	The remote path to the source of the URL list. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

No URL lists are present in WebVPN by default.

An object, Template, is available for downloading with the **export webvpn url-list** command. The Template object cannot be changed or deleted. The contents of the Template object can be edited and saved as a custom URL list, and imported with the **import webvpn url-list** command to add a custom URL list.

Exporting a previously imported URL list creates an XML file of the list at the URL location. You can view a list of available templates and previously imported tables using the **show import webvpn url-list** command.

Examples

The following example exports a URL list, *servers:*

```
ciscoasa# export webvpn url-list servers2 tftp://209.165.200.225
ciscoasa#
```

Related Commands

Command	Description
import webvpn url-list	Imports a URL list.

Command	Description
revert webvpn url-list	Removes URL lists from cache memory.
show import webvpn url-list	Displays information about imported URL lists.

export webvpn webcontent

To export previously imported content in flash memory that is visible to remote Clientless SSL VPN users, use the **export webvpn webcontent** command in privileged EXEC mode.

export webvpn webcontent *source url destination url*

Syntax Description

destination url	**The URL to export to**. The maximum number is 255 characters.
source url	The URL in the ASA flash memory in which the content resides. The maximum number is 64 characters.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Content exported with the **webcontent** option is content visible to remote clientless users. This includes previously imported help content visible on the clientless portal and logos used by customization objects.

You can see a list of content available for export by entering a question mark (**?**) after the **export webvpn webcontent** command. For example:

```
ciscoasa# export webvpn webcontent ?
Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

Examples

The following example exports the file *logo.gif* , using TFTP, to 209.165.200.225, as the filename *logo_copy.gif* :

```
ciscoasa# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

Related Commands

Command	Description
import webvpn webcontent	Imports content visible to Clientless SSL VPN users.
revert webvpn webcontent	Removes content from flash memory.
show import webvpn webcontent	Displays information about imported content.

extended-security

To define an action when the Extended Security (E-SEC) option occurs in a packet header with IP Options inspection, use the **extended-security** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

extended-security action { **allow** | **clear** }
no extended-security action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Extended Security IP option.
clear	Remove the Extended Security option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Extended Security IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# extended-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

external-browser

To configure Secure Client single sign-on authentication using an external browser (default operating system browser) instead of a browser embedded in Secure Client, use the **external-browser** command in the config-tunnel-webvpn mode. Use the **no** form of the command to disable external browser for single sign-on authentication.

external-browser enable

no external-browser enable

Syntax Description

enable	Configures the default OS browser for single sing-on authentication.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
config-tunnel-webvpn	• Yes	• Yes	• Yes	• No	• No

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

The **external-browser** command allows you to configure the default operating system browser for SAML single sign-on authentication.

The following example shows how to use the**external-browser enable** command to use the default operating system browser for SAML single sign-on authentication.

```
ciscoasa
#
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
anyconnect external-browser-pkg	Configures the Secure Client external browser package file path.
tunnel-group	Creates a VPN connection profile or accesses the database of VPN connection profiles.

Command	Description
show webvpnanyconnect external-browser-pkg	Displays information about the specified single sing-on package file.

external-port

To specify the VXLAN external port for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **external-port** command in interface configuration mode. To remove the port, use the **no** form of this command.

external-port *port*
no external-port *port*

Syntax Description

port	Sets the port between 1024 and 65535.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-segment-id	Specifies the VXLAN external segment ID for a VNI interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-port	Sets the internal VXLAN port.
internal-segment-id	Specifies the VXLAN internal segment ID for a VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
proxy paired	Sets the interface to paired proxy mode.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

external-segment-id

To specify the VXLAN external segment ID for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **external-segment-id** command in interface configuration mode. To remove the ID, use the **no** form of this command.

external-segment-id *id*
no external-segment-id *id*

Syntax Description

id	Sets the ID between 1 and 16777215.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-port	Sets the external VXLAN port.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-port	Sets the internal VXLAN port.
internal-segment-id	Specifies the VXLAN internal segment ID for a VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
proxy paired	Sets the interface to paired proxy mode.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.