

ar - az

- area, on page 3
- area authentication, on page 5
- area default-cost, on page 7
- area filter-list prefix, on page 9
- area nssa, on page 11
- area-password, on page 13
- area range (ipv6 router ospf), on page 17
- area range (router ospf), on page 19
- area stub, on page 21
- area virtual-link (ipv6 router ospf), on page 23
- area virtual-link (router ospf), on page 25
- arp, on page 28
- arp-inspection, on page 30
- arp permit-nonconnected, on page 32
- arp rate-limit, on page 34
- arp timeout, on page 35
- asdm disconnect, on page 36
- asdm disconnect log_session, on page 38
- asdm history enable, on page 40
- asdm image, on page 41
- asdm location, on page 43
- as-path access-list, on page 44
- asp load-balance per-packet, on page 46
- asp rule-engine compile-offload, on page 48
- asp rule-engine transactional-commit, on page 49
- asr-group, on page 51
- assertion-consumer-url (Deprecated), on page 53
- attribute bind, on page 55
- attribute source-group, on page 56
- attribute source-group host, on page 57
- attribute source-group keepalive, on page 59
- attributes, on page 61
- auth-cookie-name, on page 63

- authenticated-session-username, on page 65
- authentication (bfd-template), on page 67
- authentication, on page 69
- authentication eap-proxy, on page 72
- authentication key, on page 73
- authentication key eigrp, on page 77
- authentication mode, on page 79
- authentication ms-chap-v1, on page 83
- authentication ms-chap-v2, on page 84
- authentication pap, on page 85
- authentication send-only, on page 87
- authentication-attr-from-server, on page 91
- authentication-certificate, on page 93
- authentication-exclude, on page 95
- authentication-port, on page 96
- authentication-server-group (imap4s, pop3s, smtps) (Deprecated), on page 98
- authentication-server-group (tunnel-group general-attributes), on page 100
- authorization-required, on page 102
- authorization-server-group (imap4s, pop3s, smtps) (Deprecated), on page 104
- authorization-server-group (tunnel-group general-attributes), on page 106
- authorize-only, on page 108
- auth-prompt, on page 110
- auto-signon, on page 112
- auto-summary, on page 115
- auto-update device-id, on page 117
- auto-update poll-at, on page 119
- auto-update poll-period, on page 121
- auto-update server, on page 123
- auto-update timeout, on page 125
- avc, on page 126

area

To create an OSPF v2 or OSPFv3 area, use the **area** command in router configuration mode. To remove the area, use the **no** form of this command.

area *area_id*
no area *area_id*

Syntax Description

area_id	The ID of the area being created. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

The area that you create does not have any parameters set. Use the related **area** commands to set the area parameters.

Examples

The following example shows how to create an OSPF area with an area ID of 1:

```
ciscoasa(config-router)# area 1
ciscoasa(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area authentication

To enable authentication for an OSPFv2 area, use the **area authentication** command in router configuration mode. To disable area authentication, use the **no** form of this command.

area *area_id* **authentication** [**message-digest**]
no area *area_id* **authentication** [**message-digest**]

Syntax Description

area_id	The identifier of the area for which authentication is to be enabled. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication for the area specified by the *area_id*.

Command Default

Area authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified OSPFv2 area does not exist, it is created when this command is entered. Entering the **area authentication** command without the **message-digest** keyword enables simple password authentication. Including the **message-digest** keyword enables MD5 authentication.

Examples

The following example shows how to enable MD5 authentication for area 1:

```
ciscoasa(config-router)# area 1 authentication message-digest
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.

Command	Description
show running-config router	Displays the commands in the global router configuration.

area default-cost

To specify a cost for the default summary route sent into a stub or NSSA, use the **area default-cost** command in router configuration mode or IPv6 router configuration mode. To restore the default cost value, use the **no** form of this command.

area *area_id* **default-cost** *cost*
no area *area_id* **default-cost** *cost*

Syntax Description

area_id	The identifier of the stub or NSSA whose default cost is being changed. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
cost	Specifies the cost for the default summary route that is used for a stub or NSSA. Valid values range from 0 to 65535

Command Default

The default value of *cost* is 1.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode and OSPFv3 are supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Examples

The following example show how to specify a default cost for summary route sent into a stub or NSSA:

```
ciscoasa(config-router)# area 1 default-cost 5
ciscoasa(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area filter-list prefix

To filter prefixes advertised in Type 3 LSAs between OSPFv2 areas of an ABR, use the **area filter-list prefix** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

area *area_id* **filter-list prefix** *list_name* { **in** | **out** }
no area *area_id* **filter-list prefix** *list_name* { **in** | **out** }

Syntax Description

area_id	Identifies the area for which filtering is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
in	Applies the configured prefix list to prefixes advertised inbound to the specified area.
list_name	Specifies the name of a prefix list.
out	Applies the configured prefix list to prefixes advertised outbound from the specified area.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Only Type 3 LSAs can be filtered. If an ASBR has been configured in the private network, then it sends Type 5 LSAs (describing private networks) that are flooded to the entire AS including the public areas.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
ciscoasa(config-router)# area 1 filter-list prefix-list AREA_1 in
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area nssa

To configure an area as an NSSA, use the **area nssa** command in router configuration mode or IPv6 router configuration mode. To remove the NSSA designation from the area, use the **no** form of this command.

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** { **1** | **2** }] [**metric** *value*]] [**no-summary**]
no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** { **1** | **2** }] [**metric** *value*]] [**no-summary**]

Syntax Description

area_id	Identifies the area being designated as an NSSA. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
default-information-originate	Used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.
metric *metric_value*	(Optional) Specifies the OSPF default metric value. Valid values range from 0 to 16777214.
metric-type {**1** | **2**}	(Optional) the OSPF metric type for default routes. Valid values are the following: • **1**—type 1 • **2**—type 2. The default value is 2.
no-redistribution	(Optional) Used when the router is an NSSA ABR and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area.
no-summary	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Command Default

The defaults are as follows:

- No NSSA area is defined.
- The **metric-type** is 2.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple content mode and OSPFv3 are supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

If you configure one option for an area, and later specify another option, both options are set. For example, entering the following two command separately results in a single command with both options set in the configuration:

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area area_id nssa default-information-originate
```

Examples

The following example shows how setting two options separately results in a single command in the configuration:

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area 1 nssa default-information-originate
ciscoasa(config-rtr)# exit
ciscoasa(config-rtr)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

Related Commands

Command	Description
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area-password

To configure the IS-IS area authentication password, use the **area-password** command in router isis configuration mode. To disable the password, use the **no** form of this command.

area-password *password* [**authenticate snp** { **validate** | **send-only** }]
no area password [*password*]

Syntax Description

password	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into sequence number PDUS (SNPs).
validate	Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	Causes the system to only insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Command Default

No area password is defined and area password authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

Using the **area-password** command on all routers in an area prevents unauthorized routers from injecting false routing information into the link-state database.

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 1 (station router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an area authentication password and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
ciscoasa(config-router)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.

Command	Description
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.

Command	Description
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

area range (ipv6 router ospf)

To consolidate and summarize OSPFv3 routes at an area boundary, use the **area range** command in ipv6 router ospf configuration mode. To disable this function, use the **no** form of this command.

area *area_id ipv6-prefix-/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]
no area *area_id ipv6-prefix-/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

Syntax Description

advertise	(Optional) Sets the range status to advertise and generates Type 3 summary link-state advertisements (LSAs).
area_id	Specifies the identifier of the area for which routes are to be summarized. You can specify the identifier as either a decimal number or an IPv6 prefix.
cost *cost*	(Optional) Specifies the metric or cost for this summary route, which is used during OSPF SPF calculations to detemine the shortest paths to the destination. Valid values range from 0 to 16777215.
ipv6-prefix	Specifies the IPv6 prefix.
not-advertise	(Optional) Sets the range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
prefix-length	Specifies the IPv6 prefix length.

Command Default

The range status is set to advertise by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each IPv6 prefix and prefix

length. This behavior is called *route summarization* . You can configure multiple **area range** commands for an area. In this way, OSPFv3 can summarize routes for many different sets of IPv6 prefixes and prefix lengths.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for IPv6 prefix 2000:0:0:4::2 with the prefix-length 2001::/64:

```
ciscoasa(config-router)# area 1 range
2000:0:0:4::2/2001::/64

ciscoasa(config-router)#
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode for OSPFv3.
show running-config ipv6 router	Displays the IPv6 commands in the global router configuration.

area range (router ospf)

To consolidate and summarize routes at an area boundary, use the **area range** command in router ospf configuration mode. To disable this function, use the **no** form of this command.

area *area_id* **range** *address mask* **advertise** | **not-advertise**]
no area *area_id* **range** *address mask* **advertise** | **not-advertise**]

Syntax Description

address	IP address of the subnet range.
advertise	(Optional) Sets the address range status to advertise and generates Type 3 summary link-state advertisements (LSAs).
area_id	Identifies the area for which the range is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
mask	IP address subnet mask.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Command Default

The address range status is set to advertise.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization* . You can configure multiple **area range** commands for an area. In this way, OSPF can summarize addresses for many different sets of address ranges.

The **no area** *area_id* **range** *ip_address netmask* **not-advertise** command removes only the **not-advertise** optional keyword.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
ciscoasa(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
ciscoasa(config-router)# area 0 range 192.168.110.0 255.255.255.0
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area stub

To define an area as a stub area, use the **area stub** command in router configuration mode or IPv6 router configuration mode. To remove the stub area, use the **no** form of this command.

area *area_id* **stub** [**no-summary**]
no area *area_id* **stub** [**no-summary**]

Syntax Description

area_id	Identifies the stub area. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
no-summary	Prevents an ABR from sending summary link advertisements into the stub area.

Command Default

The default behaviors are as follows:

- No stub areas are defined.
- Summary link advertisements are sent into the stub area.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	We added this command.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

The command is used only on an ABR attached to a stub or NSSA.

There are two stub area router configuration commands: the area stub and area default-cost commands. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost** command only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example configures the specified area as a stub area:

```
ciscoasa(config-rtr)# area 1 stub
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub or NSSA.
area nssa	Defines the area as a not-so-stubby area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area virtual-link (ipv6 router ospf)

To define an OSPFv3 virtual link, use the **area virtual-link** command in ipv6 router ospf configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]
no area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

Syntax Description

area_id	Specifies the area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or valid IPv6 prefix. Valid decimal values range from 0 to 4294967295.
hello-interval *seconds*	(Optional) Specifies the time in seconds between hello packets that the ASA sends on the interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192 seconds.
retransmit-interval *seconds*	(Optional) Specifies the time in seconds between LSA retransmissions for adjacent routers that belong to the interface. The retransmission interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Valid values range from 1 to 8192 seconds.
router_id	Specifies the router ID that is associated with the virtual link neighbor. The router ID appears in the **show ipv6 ospf** or **show ipv6 display** command.
transmit-delay *seconds*	(Optional) Specifies the estimated time in seconds that is required to send a link-state update packet on the interface. The integer value must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. Valid values range from 1 to 8192 seconds.
dead-interval *seconds*	(Optional) Specifies the time in seconds that hello packets are not seen before a neighbor indicates that the router is down. The dead interval in an unsigned integer value. As with the hello interval, this value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192 seconds.
ttl-security hops *hop-count*	(Optional) Configures the time-to-live (TTL) security on a virtual link. Valid values for the hop count range from 1 to 254.

Note Single-digit passwords and passwords starting with a digit followed by a white space are no longer supported.

Command Default

The defaults are as follows:

- *area_id*: No area ID is predefined.

- *router_id*: No router ID is predefined.
- **hello-interval**: 10 seconds.
- **retransmit-interval**: 5 seconds.
- **transmit-delay**: 1 second.
- **dead-interval**: 40 seconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

In OSPFv3, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic occurs.

The setting of the retransmission interval should be conservative, or unnecessary retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be correctly configured. Use the **show ipv6 ospf** command to obtain the router ID.

Examples

The following example establishes a virtual link in OSPFv3:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello interval 5
```

area virtual-link (router ospf)

To define an OSPF virtual link, use the **area virtual-link** command in router ospf configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0|8]** *key*] | [**message-digest-key** *key_id* **md5[0|8]** *key*]]]]
no area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0|8]** *key*] | [**message-digest-key** *key_id* **md5[0|8]** *key*]]]]

Syntax Description

area_id	Area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
authentication	(Optional) Specifies the authentication type.
key-chain *key-chain-name*	(Optional) Specifies a key chain to use for authentication. The key-name argument can be a maximum of 63 alphanumeric characters.
authentication-key [0 | 8]*key*	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
dead-interval *seconds*	(Optional) Specifies the interval before declaring a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
hello-interval *seconds*	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
md5 [0 | 8] *key*	(Optional) Specifies an alphanumeric key up to 16 bytes.
message-digest	(Optional) Specifies that message digest authentication is used.
message-digest-key *key_id*	(Optional) Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
0	Specifies an unencrypted password will follow.
8	Specifies an encrypted password will follow.
null	(Optional) Specifies that no authentication is used. Overrides password or message digest authentication if configured for the OSPF area.
retransmit-interval *seconds*	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
router_id	The router ID associated with the virtual link neighbor. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.

transmit-delay *seconds*	(Optional) Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535. The default is 5 seconds.

Note Single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported.

Command Default

The defaults are as follows:

- *area_id*: No area ID is predefined.
- *router_id*: No router ID is predefined.
- **hello-interval** *seconds*: 10 seconds.
- **retransmit-interval** *seconds*: 5 seconds.
- **transmit-delay** *seconds*: 1 second.
- **dead-interval** *seconds*: 40 seconds.
- **authentication-key [0 | 8]** *key*: No key is predefined.
- **message-digest-key** *key_id* **md5 [0 | 8]** *key*: No key is predefined.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We added this command.
9.12(1)	Key chain feature was added to support rotating keys for OSPF authentication.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic ensues.

The setting of the retransmit interval should be conservative, or needless retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

The specified authentication key is used only when authentication is enabled for the backbone with the **area** *area_id* **authentication** command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key [0 | 8]** *key* or **message-digest-key** *key_id* **md5[0 | 8]** *key* are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

If the authentication type is not specified for an interface, the interface uses the authentication type specified for the area. If no authentication type has been specified for the area, the area default is null authentication.



Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be properly configured. Use the **show ospf** command to see the router ID.

Examples

The following example establishes a virtual link with MD5 authentication:

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 8
sa5721bk47
```

The following example establishes a virtual link with rotating keys authentication:

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 authentication key-chain
CHAIN-RTR-OSPFKEY
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
show running-config router	Displays the commands in the global router configuration.

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
show running-config ipv6 router	Displays the IPv6 commands in the global router configuration.

arp

To add a static ARP entry to the ARP table, use the **arp** command in global configuration mode. To remove the static entry, use the **no** form of this command.

arp *interface_name ip_address mac_address* [**alias**]
no arp *interface_name ip_address mac_address*

Syntax Description

alias	(Optional) Enables proxy ARP for this mapping. If the ASA receives an ARP request for the specified IP address, then it responds with the ASA MAC address. When the ASA receives traffic destined for the host belonging to the IP address, the ASA forwards the traffic to the host MAC address that you specify in this command. This keyword is useful if you have devices that do not perform ARP, for example. In transparent firewall mode, this keyword is ignored; the ASA does not perform proxy ARP.
interface_name	The interface attached to the host network.
ip_address	The host IP address.
mac_address	The host MAC address.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	We added this command.

Usage Guidelines

Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

A static ARP entry maps a MAC address to an IP address and identifies the interface through which the host is reached. Static ARP entries do not time out, and might help you solve a networking problem. In transparent firewall mode, the static ARP table is used with ARP inspection (see the **arp-inspection** command).



Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the ASA, such as management traffic.

Examples

The following example creates a static ARP entry for 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface:

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Related Commands

Command	Description
arp timeout	Sets the time before the ASA rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp-inspection

To enable ARP inspection for transparent firewall mode, use the **arp-inspection** command in global configuration mode. To disable ARP inspection, use the **no** form of this command.

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]
no arp-inspection *interface_name* **enable**

Syntax Description

enable	Enables ARP inspection.
flood	(Default) Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the ASA drops the packet. **Note** The management-specific interface, if present, never floods packets even if this parameter is set to flood.
interface_name	The bridge group member interface on which you want to enable ARP inspection.
no-flood	(Optional) Specifies that packets that do not exactly match a static ARP entry are dropped.

Command Default

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the ASA. When you enable ARP inspection, the default is to flood non-matching ARP packets.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	You can now configure this command in routed mode when using Integrated Routing and Bridging.

Usage Guidelines

Configure static ARP entries using the **arp** command before you enable ARP inspection.

ARP inspection checks all ARP packets against static ARP entries (see the **arp** command) and blocks mismatched packets. This feature prevents ARP spoofing.

When you enable ARP inspection, the ASA compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the ASA drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the ASA to either forward the packet out all interfaces (flood), or to drop the packet.



Note The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can then intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, provided the correct MAC address and the associated IP address are in the static ARP table.



Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the ASA, such as management traffic.

Examples

The following example enables ARP inspection on the outside interface and sets the ASA to drop any ARP packets that do not match the static ARP entry:

```
ciscoasa(config)# arp outside 209.165.200.225 0009.7cbe.2100
ciscoasa(config)# arp-inspection outside enable no-flood
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp permit-nonconnected

To enable the ARP cache to also include non-directly-connected subnets, use the **arp permit-nonconnected** command in global configuration mode. To disable non-connected subnets, use the **no** form of this command.

arp permit-nonconnected
no arp permit-nonconnected

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
8.4(5), 9.0(1)	We added this command.

Usage Guidelines

The ASA ARP cache only contains entries from directly-connected subnets by default. When the **no arp permit-nonconnected** command is there (default behavior), the ASA rejects both incoming ARP requests and ARP responses in case the ARP packet received is in a different subnet than the connected interface.

Note that the first case (default behavior) causes a failure in case PAT is configured on the ASA and the virtual IP address (mapped) for PAT is in a different subnet than the connected interface.

Also, we do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attacks against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.

You may want to use this feature if you use:

- Secondary subnets.
- Proxy ARP on adjacent routes for traffic forwarding.

Examples

The following example enables non-connected subnets:

```
ciscoasa(config)# arp permit non-connected
```

The default behavior can be seen in the output of the **debug arp** command on the ASA as:

For an incoming ARP request:

```
- larp-in: request at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.2.2 0000.0000.0000
having smac 0013.8083.0bb1 dmac ffff.ffff.ffff\narp-in: Arp packet received from 10.10.2.1
 which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

For an incoming ARP response:

The following example enables non-connected subnets:

```
ciscoasa(config)# arp permit non-connected

- arp-in: response at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.1.2 0016.4687.9f43
having smac 0013.8083.0bb1 dmac 0016.4687.9f43\narp-in: Arp packet received from 10.10.2.1
 which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

Related Commands

Command	Description
arp	Adds a static ARP entry.

arp rate-limit

To set the ARP rate limit to control the number of ARP packets per second, use the **arp rate-limit** command in global configuration mode. To restore the default, use the **no** form of this command.

arp rate-limit *seconds*
no arp rate-limit

Syntax Description

seconds	Specifies the number of seconds between 10 and 32768. The default value depends on your ASA model.

Command Default

The default value depends on your ASA model.

Command Modes

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

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

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

You can customize this value to prevent an ARP storm attack.

Examples

The following example sets the ARP rate to 10000 per second:

```
ciscoasa(config)# arp rate-limit 10000
```

Related Commands

Command	Description
show arp rate-limit	Shows the ARP rate limit.

arp timeout

To set the time before the ASA rebuilds the ARP table, use the **arp timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

arp timeout *seconds*
no arp timeout *seconds*

Syntax Description

seconds	The number of seconds between ARP table rebuilds, from 60 to 4294967.

Command Default

The default value is 14,400 seconds (4 hours).

Command Modes

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

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Gloabl configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.

Usage Guidelines

Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently.

Examples

The following example changes the ARP timeout to 5,000 seconds:

```
ciscoasa(config)# arp timeout 5000
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp timeout	Shows the current configuration of the ARP timeout.

asdm disconnect

To terminate an active ASDM session, use the **asdm disconnect** command in privileged EXEC mode.

asdm disconnect *session*

Syntax Description

session	The session ID of the active ASDM session to be terminated.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm disconnect** command to the **asdm disconnect** command.

Usage Guidelines

Use the **show asdm sessions** command to display a list of active ASDM sessions and their associated session IDs. Use the **asdm disconnect** command to terminate a specific session.

When you terminate an ASDM session, any remaining active ASDM sessions keep their associated session ID. For example, if there are three active ASDM sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM sessions keep the session IDs 0 and 2. The next new ASDM session in this example would be assigned a session ID of 1, and any new sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm sessions** commands display the active ASDM sessions before and after the **asdm disconnect** command is entered.

```
ciscoasa# show asdm sessions
0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm sessions
1 192.168.1.2
```

Related Commands

Command	Description
show asdm sessions	Displays a list of active ASDM sessions and their associated session ID.

asdm disconnect log_session

To terminate an active ASDM logging session, use the **asdm disconnect log_session** command in privileged EXEC mode.

asdm disconnect log_session *session*

Syntax Description

session	The session ID of the active ASDM logging session to be terminated.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **show asdm log_sessions** command to display a list of active ASDM logging sessions and their associated session IDs. Use the **asdm disconnect log_session** command to terminate a specific logging session.

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the ASA. Terminating a log session may have an adverse effect on the active ASDM session. To terminate an unwanted ASDM session, use the **asdm disconnect** command.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

When you terminate an ASDM logging session, any remaining active ASDM logging sessions keep their associated session ID. For example, if there are three active ASDM logging sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM logging sessions keep the session IDs 0 and 2. The next new ASDM logging session in this example would be assigned a session ID of 1, and any new logging sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm log_sessions** commands display the active ASDM sessions before and after the **asdm disconnect log_sessions** command is entered.

```
ciscoasa# show asdm log_sessions
0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm log_sessions
1 192.168.1.2
```

Related Commands

Command	Description
show asdm log_sessions	Displays a list of active ASDM logging sessions and their associated session ID.

asdm history enable

To enable ASDM history tracking, use the **asdm history enable** command in global configuration mode. To disable ASDM history tracking, use the **no** form of this command.

asdm history enable
no asdm history enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm history enable** command to the **asdm history enable** command.

Usage Guidelines

The information obtained by enabling ASDM history tracking is stored in the ASDM history buffer. You can view this information using the **show asdm history** command. The history information is used by ASDM for device monitoring.

Examples

The following example enables ASDM history tracking:

```
ciscoasa(config)# asdm history enable
ciscoasa(config)#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

asdm image

To specify the location of the ASDM software image in flash memory, use the **asdm image** command in global configuration mode. To remove the image location, use the **no** form of this command.

asdm image *url*
no asdm image [*url*]

Syntax Description

url Sets the location of the ASDM image in flash memory. See the following URL syntax:

- **disk0:**/[*path*/]*filename*

For the ASA 5500 series, this URL indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased.

- **disk1:**/[*path*/]*filename*

For the ASA 5500 series, this URL indicates the external Flash memory card.

- **flash:**/[*path*/]*filename*

This URL indicates the internal Flash memory.

Command Default

If you do not include this command in your startup configuration, the ASA uses the first ASDM image it finds at startup. It searches the root directory of internal Flash memory and then external flash memory. The ASA then inserts the **asdm image** command into the running configuration if it discovered an image.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can store more than one ASDM software image in flash memory. If you enter the **asdm image** command to specify a new ASDM software image while there are active ASDM sessions, the new command does not disrupt the active sessions; active ASDM sessions continue to use the ASDM software image they started with. New ASDM sessions use the new software image. If you enter the **no asdm image** command, the command is removed from the configuration. However, you can still access ASDM from the ASA using the last-configured image location.

If you do not include this command in your startup configuration, the ASA uses the first ASDM image it finds at startup. It searches the root directory of internal flash memory and then external flash memory. The ASA then inserts the **asdm image** command into the running configuration if it discovered an image. Be sure to save the running configuration to the startup configuration using the **write memory** command. If you do not save the **asdm image** command to the startup configuration, every time you reboot, the ASA searches for an ASDM image and inserts the **asdm image** command into your running configuration. If you are using Auto Update, the automatic addition of this command at startup causes the configuration on the ASA not to match the configuration on the Auto Update Server. This mismatch causes the ASA to download the configuration from the Auto Update Server. To avoid unnecessary Auto Update activity, save the **asdm image** command to the startup configuration.

Examples

The following example sets the ASDM image to asdm.bin:

```
ciscoasa(config)# asdm image flash:/asdm.bin
ciscoasa(config)#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.
boot	Sets the software image and startup configuration files.

asdm location



Caution Do not manually configure this command. ASDM adds **asdm location** commands to the running configuration and uses them for internal communication. This command is included in the documentation for informational purposes only.

asdm location *ip_addr netmask if_name*
asdm location *ipv6_addr/prefix if_name*

Syntax Description

if_name	The name of the highest security interface. If you have multiple interfaces at the highest security, then an arbitrary interface name is chosen. This interface name is not used, but is a required parameter.
ip_addr	The IP address used internally by ASDM to define the network topology.
ipv6_addr/prefix	The IPv6 address and prefix used internally by ASDM to define the network topology.
netmask	The subnet mask for *ip_addr*.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm location** command to the **asdm location** command.

Usage Guidelines

Do not manually configure or remove this command.

as-path access-list

To configure an autonomous system path filter using a regular expression, use the as-path access-list command in global configuration mode. To delete the autonomous system path filter and remove it from the running configuration file, use the no form of this command.

as-path access-list *acl-name* { **permit** | **deny** } *regexp*
no as-path access-list *acl-name*

Syntax Description

acl-name	Name that specifies the AS-path access-list.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions
regexp	Regular expression that defines the AS-path filter. The autonomous system number is expressed in the range from 1 to 65535. For more details about autonomous system number formats, see the router bgp command. **Note** See the "Regular Expressions" appendix in the Cisco IOS Terminal Services Configuration Guide for information about configuring regular expressions.

Command Default

No autonomous system path filter is created.

Command Modes

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

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

Command History

Release	Modification
9.2(1)	We added this command.

Usage Guidelines

Use the as-path access-list command to configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the permit or deny condition applies. The autonomous system path should not contain the local autonomous system number.

The Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described

in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail.

Examples

In the following example, an autonomous system path access list (number 500) is defined to configure the ASA to not advertise any path through or from autonomous system 65535 to the 10.20.2.2 neighbor:

```
ciscoasa(config)# as-path access-list as-path-acl deny _65535_
ciscoasa(config)# as-path access-list as-path-acl deny ^65535$
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-fmaily ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.1 remote-as 65535
ciscoasa(config-router-af)# neighbor 10.20.2.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 10.20.2.2 filter-list as-path-acl out
```

asp load-balance per-packet

For multi-core ASAs, to change the load balancing behavior to be per packet, use the **asp load-balance per-packet** command in global configuration mode. To restore the default load-balancing mechanism, use the **no** form of this command.

asp load-balance per-packet [**auto**]
no asp load-balance per-packet

Syntax Description

auto Automatically enables and disables per-packet load-balancing on each interface receive ring according to network conditions.

Command Default

Per-packet load-balancing is disabled by default.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	We added this command.
9.3(1)	The **auto** option was added.
9.8(1)	The **auto** option is now available for the ASA Virtual.

Usage Guidelines

The job of the load balancer is to distribute packets to CPU cores and to maintain packet order. By default, a connection can only be processed by one core at a time. Due to this behavior, the cores will be under-utilized if there are a small number of interfaces/RX rings in use when compared to the number of cores. For example if there are only two Gigabit Ethernet interfaces in use on an ASA, then only two cores will be used. (A Ten Gigabit Ethernet interface has 4 RX rings and a Gigabit Ethernet interface as 1 RX ring.) You may want to optimize the load balancer by enabling per-packet load balancing so you can use more cores.

The default load-balancing behavior optimizes overall system performance when you have many interfaces in use, while the per-packet load balancer optimizes the overall system performance when you have a smaller number of interfaces that are active.

If you enable per-packet load balancing, when one core processes packets from an interface, another core can receive and process the next packet from the same interface. Therefore, it is possible for all cores to process packets from the same interface simultaneously.

Per-packet load balancing will improve performance if:

- The system drops packets
- The **show cpu** command shows CPU usage far less than 100%—The CPU usage is a good indicator of how many cores are being used. For example, on an 8-core system, if two cores are used, **show cpu** shows 25%; four cores: 50%; six cores: 75%.
- There are a small number of interfaces that are in use



Note Typically if there are less than 64 concurrent flows on the ASA, then enabling per-packet load balancing will incur more overhead than its benefit.

The **auto** option enables the ASA to detect whether or not asymmetric traffic has been added. The one-to-one lock between interface receive rings and cores is released if load balancing is needed. Load balancing per packet is only enabled on the heavily-loaded interface receive rings, not on all the interface receive rings. This adaptive load balance mechanism helps avoid the following issues:

- Overruns caused by sporadic traffic spikes on flows
- Overruns caused by bulk flows oversubscribing specific interface receive rings
- Overruns caused by relatively heavily overloaded interface receive rings, in which a single core cannot sustain the load.

The **auto** option is not available for the ASA Virtual in 9.7 and earlier.

Examples

The following example shows how to change the default load-balancing behavior:

```
ciscoasa(config)# asp load-balance per-packet
```

The following example enables the automatic switching on and off of per-packet load balancing:

```
ciscoasa(config)# asp load-balance per-packet auto
```

Related Commands

Command	Description
clear asp load-balance history	Clears and resets the ASP load balancing per packet history statistics.
show asp load-balance	Displays a histogram of the load balancer queue sizes.
show asp load-balance per-packet	Displays current status, high and low watermarks, and the global threshold.
show asp load-balance per-packet history	Displays current status, high and low watermarks, the global threshold, the times of switching ASP load balancing per packet on and off since the last reset, the history of ASP load balancing per packet with time stamps, and the reasons for switching it on and off.

asp rule-engine compile-offload

Use the **asp rule-engine compile-offload** command to enable or disable the compile offload function for the rule engine.

asp rule-engine compile-offload [**threshold** *rule-threshold*]
no asp rule-engine compile-offload [**threshold** *rule-threshold*]

Syntax Description

threshold*rule-threshold*	Rule update threshold count to offload the compilation, 1 – 1000000. Default is 100.

Command Default

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.20(1)	This command was introduced.

Usage Guidelines

When enabled, tmatch compilation is offloaded to the data path from the control plane if the tmatch object rule update count is greater than the threshold value. This leaves more time for the control plane to perform other tasks. Offloaded compliation is for rule-based policies such as ACLs, NAT, and VPN.

Because there is a fixed overhead to offload the compilation, you can increase the default threshold of 100 to adjust performance. The default threshold should work well in most cases.

Example

The following example increases the threshold to 1000.

```
ciscoasa(config)# asp rule-engine compile-offload threshold 1000
```

Related Commands

Command	Description
show asp rule-engine	Displays the status of the ASP rule engine.

asp rule-engine transactional-commit

Use the **asp rule-engine transactional-commit** command to enable or disable the transactional commit model for the rule engine.

asp rule-engine transactional-commit *option*
no asp rule-engine transactional-commit *option*

Syntax Description

option Enables the transactional commit model for the rule engine for the selected policies. Options include:

- **access-group**—Access rules applied globally or to interfaces.
- **nat**—Network address translation rules.

Command Default

By default, the transactional commit model is disabled.

Command Modes

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

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

Command History

Release	Modification
9.1(5)	We added this command.
9.3(1)	We added the **nat** keyword.

Usage Guidelines

By default, when you change a rule-based policy (such as access rules), the changes become effective immediately. However, this immediacy comes at a slight cost in performance. The performance cost is more noticeable for very large rule lists in a high connections-per-second environment, for example, when you change a policy with 25,000 rules while the ASA is handling 18,000 connections per second.

The performance is affected because the rule engine compiles rules to enable faster rule lookup. By default, the system will also search uncompiled rules when evaluating a connection attempt so that new rules can be applied; since the rules are not compiled, the search takes longer.

You can change this behavior so that the rule engine uses a transactional model when implementing rule changes, continuing to use the old rules until the new rules are compiled and ready for use. Using the transactional model, performance should not drop during the rule compilation. The following table clarifies the behavioral difference.

Model	Before Compilation	During Compilation	After Compilation
Default	Match old rules.	Match new rules. (Connections per second rate will decrease.)	Match new rules.
Transactional	Match old rules.	Match old rules. (Connections per second rate will be unaffected.)	Match new rules.

An additional benefit of the transactional model is that, when replacing an ACL on an interface, there is no gap between deleting the old ACL and applying the new one. This reduces the chances that acceptable connections will be dropped during the operation.



Tip If you enable the transactional model for a rule type, there are syslog messages to mark the beginning and the end of the compilation. These messages are numbered 780001 and following.

Examples

The following example enables the transactional commit model for access groups:

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

Related Commands

Command	Description
clear conf asp rule-engine transactional-commit	Clears the transactional commit configurations for the rule engine.
show asp rule-engine	Displays the status of the ASP rule engine.

asr-group

To specify an asymmetrical routing interface group ID, use the **asr-group** command in interface configuration mode. To remove the ID, use the **no** form of this command.

asr-group *group_id*
no asr-group *group_id*

Syntax Description

group_id	The asymmetric routing group ID. Valid values are from 1 to 32.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When Active/Active failover is enabled, you may encounter situations where load balancing causes the return traffic for outbound connections to be routed through an active context on the peer unit, in which the context for the outbound connection is in the standby group.

The **asr-group** command causes incoming packets to be reclassified with the interface of the same ASR group if a flow with the incoming interface cannot be found. If reclassification finds a flow with another interface, and the associated context is in standby state, then the packet is forwarded to the active unit for processing.

Stateful Failover must be enabled for this command to take effect.

You can view ASR statistics using the **show interface detail** command. These statistics include the number of ASR packets sent, received, and dropped on an interface.



Note No two interfaces in the same context should be configured in the same ASR group.

Examples

The following example assigns the selected interfaces to the asymmetric routing group 1.

Context ctx1 configuration:

```
ciscoasa/ctx1(config)# interface Ethernet2
ciscoasa/ctx1(config-if)# nameif outside
ciscoasa/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
ciscoasa/ctx1(config-if)# asr-group 1
```

Context ctx2 configuration:

```
ciscoasa/ctx2(config)# interface Ethernet3
ciscoasa/ctx2(config-if)# nameif outside
ciscoasa/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
ciscoasa/ctx2(config-if)# asr-group 1
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
show interface	Displays interface statistics.

assertion-consumer-url (Deprecated)

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

To identify the URL that the security device accesses to contact the assertion consumer service, use the **assertion-consumer-url** command in the webvpn configuration mode for that specific SAML-type SSO server. To remove the URL from the assertion, use the **no** form of this command.

assertion-consumer-url *url*
no assertion-consumer-url [*url*]

Syntax Description

url	Specifies the URL of the assertion consumer service used by the SAML-type SSO server. The URL must start with either http:// or https:// and must be less than 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
9.5(2)	This command was deprecated, with the introduction of support for SAML 2.0.

Usage Guidelines

Single sign-on (SSO) support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO servers.

If the URL begins with HTTPS, the requirement is to install the root certificate for the assertion consumer service SSL certificate.

Examples

The following example specifies the assertion consumer URL for a SAML-type SSO server:

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
```

```
ciscoasa(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
ciscoasa(config-webvpn-sso-saml#
```

Related Commands

Command	Description
issuer	Specifies the SAML-type SSO server security device name.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a WebVPN SSO server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

attribute bind

To change the IP-to-attribute binding for an attribute-based network object, use the **attribute bind** command in EXEC mode.

attribute bind *agent-name* **binding** *ip-address* **type** *attribute-type* **value** *attribute-value*

Syntax Description

agent-name	Specifies the name of the VM attribute agent monitoring the attribute.
ip-address	Specifies the IP address of the attribute-based network object being managed.
attribute-type	Specifies the string identifying the attribute type to be updated.
attribute-value	Specifies the string identifying the new value to be assigned to the attribute type.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	This command was added.

Examples

The following example specifies the assertion consumer URL for a SAML-type SSO server:

```
ciscoasa(config)# attribute bind VMAgent binding 10.10.1.19 type custom.location value
global
```

Related Commands

Command	Description
attribute source-group	Configures a VM attribute agent.
object network attribute	Configures an attribute-based network object.
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attribute source-group

To configure a VM attribute agent to communicate with VMware vCenter or a single ESXi host, use the **attribute source-group** command in EXEC mode. To delete an agent, use the **no** form of this command.

attribute source-group *agent-name* **type** *agent-type*
no attribute source-group *agent-name*

Syntax Description

agent-name	Specifies the name of the VM attribute agent name.
agent-type	Specifies the the type of attribute agent. Currently ESXi is the only supported agent type.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	This command was added.

Examples

The following example shows how to configure a VM attribute agent:

```
ciscoasa(config)# attribute source-group VMAgent type esxi
```

Related Commands

Command	Description
object network attribute	Configures an attribute-based network object.
show attribute source-group	Shows information about configured attribute agents.
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attribute source-group host

To configure VMware vCenter host credentials that allow a VM attribute agent to communicate with vCenter or a single ESXi host, use the **attribute source-group host** command in attribute agent configuration mode. To delete host credentials, use the **no** form of this command.

host *ip-address* **username** *ESXi-username* **password** *ESXi-password*
no host *ip-address*

Syntax Description

ip-address	Specifies the name of the VM attribute agent.
ESXi-username	Specifies the vCenter host username.
ESXi-password	Specifies the vCenter host password.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use this command after you configure or modify an attribute agent.

Examples

The following example shows how to configure host credentials for an attribute agent:

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# host 10.122.202.217 user admin password Cisco123
```

Related Commands

Command	Description
attribute source-group	Configures a VM attribute agent.
object network attribute	Configures an attribute-based network object.
show attribute source-group	Shows information about configured attribute agents.

Command	Description
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attribute source-group keepalive

To configure keepalive settings for VMware vCenter communication, use the **attribute source-group keepalive** command in attribute agent configuration mode. To restore the default values, use the **no** form of this command.

keepalive retry-interval *interval* **retry-count** *count*
no keepalive

Syntax Description

interval	Specifies the interval between keepalive messages from the attribute agent to vCenter. Each time a keepalive message receives a response from the source, the agent is considered to be in contact with the source, and the keepalive timer for that agent is restarted. The default is 30 seconds.
count	Specifies the retry count when a keepalive message is not received. Each time the timer expires without receiving a keepalive, the retry count for that agent is incremented. If the retry count reaches the configured threshold value, the agent declares that it has lost contact with the source. The default is 3.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use this command after you configure or modify an attribute agent.

Examples

The following example specifies the assertion consumer URL for a SAML-type SSO server:

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# keepalive retry-timer 100 retry-count 5
```

Related Commands

Command	Description
attribute source-group	Configures a VM attribute agent.
object network attribute	Configures an attribute-based network object.

Command	Description
show attribute source-group	Shows information about configured attribute agents.
show attribute object-map	Shows the object-to-attribute bindings.
show attribute host-map	Shows a map of the host-to-attribute bindings.

attributes

To specify attribute value pairs that the ASA writes to the DAP attribute database, enter the **attributes** command in dap test attributes mode.

attributes *name value*

Syntax Description

name	Specifies a well-known attribute name, or an attribute that incorporates a "label" tag. The label tag corresponds to the endpoint ID that you configure for file, registry, process, antivirus, antispyware, and personal firewall endpoint attributes in the DAP record.
value	The value assigned to the AAA attribute.

Command Default

No default value or behaviors.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use this command multiple times to enter multiple attribute value pairs.

Normally the ASA retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The ASA writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint selection attributes for a DAP record.

Examples

The following example assumes that ASA selects two DAP records if the authenticated user is a member of the SAP group and has antivirus software installed on the endpoint system. The endpoint ID for the antivirus software endpoint rule is *nav*.

The DAP records have the following policy attributes:

DAP Record 1	DAP Record 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2

DAP Record 1	DAP Record 2
—	url-entry = enable

```
ciscoasa
 #
test dynamic-access-policy attributes
ciscoasa
(config-dap-test-attr)#
attributes aaa.ldap.memberof SAP
ciscoasa
(config-dap-test-attr)#
 attributes endpoint.av.nav.exists true
ciscoasa
(config-dap-test-attr)#
exit
ciscoasa
 #
test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable
ciscoasa
 #
```

Related Commands

Command	Description
display	Displays current attribute lists.
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes.
test dynamic-access-policy execute	Executes the logic that generates the DAP and displays the resulting access policies to the console.

auth-cookie-name

To specify the name of an authentication cookie, use the **auth-cookie-name** command in aaa-server host configuration mode. This is an SSO with HTTP Forms command.

auth-cookie-name

Syntax Description

name	The name of the authentication cookie. The maximum name size is 128 characters.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The WebVPN server of the ASA uses an HTTP POST request to submit a single sign-on (SSO) authentication request to an SSO server. If authentication succeeds, the authenticating web server passes back an authentication cookie to the client browser. The client browser then authenticates to other web servers in the SSO domain by presenting the authentication cookie. The **auth-cookie-name** command configuresthe name of the authentication cookie to be used for SSO by the ASA.

A typical authentication cookie format is Set-Cookie: *cookie name =cookie value* [;*cookie attributes*]. In the following authentication cookie example, SMSESSION is the name that would be configured with the **auth-cookie-name** command:

```
Set-Cookie:
```

Examples

The following example specifies the authentication cookie name of SMSESSION for the authentication cookie received from a web server named example.com:

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# auth-cookie-name SMSESSION
ciscoasa(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies that a username parameter must be submitted as part of the HTTP POST request used for SSO authentication.

authenticated-session-username

To specify which authentication username to associate with the session when double authentication is enabled, use the **authenticated-session-username** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

authenticated-session-username { **primary** | **secondary** }
no authenticated-session-username

Syntax Description

primary	Uses the username from the primary authentication server.
secondary	Uses the username from the secondary authentication server.

Command Default

The default value is **primary**.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **authenticated-session-username** command selects the authentication server from which the ASA extracts the username to associate with the session.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies the use of the username from the secondary authentication server for the connection:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authenticated-session-username secondary
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the prefill username feature.

Command	Description
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

authentication (bfd-template)

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

authentication *authentication-type* [**0|8**] *key-string* **key-id** *id*

Syntax Description

authentication-type	Specifies the authentication type. Valid values are **md5**, **meticulous-md5**, **meticulous-sha-1**, and **sha-1**.
0|8	0 specifies that an UNENCRYPTED password will follow. 8 specifies that an ENCRYPTED password will follow.
key-string	Specifies the authentication string that must be sent and received in the packets using the routing protocol being authenticated. The valid range is 1 to 17 uppercase and lowercase alphanumeric characters, except that the first character CANNOT be a number.
id	Specifies the shared key ID that matches the key string.

Command Default

This command has no default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to configure authentication in a BFD single-hop and multi-hop templates. We recommend that you configure authentication to enhance security.

Authentication must be configured on each BFD source-destination pair, and authentication parameters must match on both devices.

Examples

The following example configures authentication in a single-hop BFD template.

```
ciscoasa(config)# bfd single-hop sh-template
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

The following example configures authentication in a multi-hop BFD template.

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# authentication shat-1 0 cisco key-id 10
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

authentication

To configure the authentication method for WebVPN and e-mail proxies, use the **authentication** command in various modes. To restore the default method, use the **no** form of this command. The ASA authenticates users to verify their identity.

authentication [{ [**aaa**] [**certificate**] [**multiple certificate**] [**saml**] [**mailhost**] [**piggyback**] }
no authentication [[**aaa**] [**certificate**] [**multiple certificate**] [**saml**] [**mailhost**] [**piggyback**]

Syntax Description

aaa	Provides a username and password that the ASA checks with a previously configured AAA server.
certificate	Provides a certificate during SSL negotiation.
mailhost	Authenticates via the remote mail server for SMTPS only. For IMAP4S and POP3S, mailhost authentication is mandatory and not displayed as a configurable option.
multiple certificate	Provides a multiple certificate option during SSL negotiation.
piggyback	Requires that an HTTPS WebVPN session already exist. Piggyback authentication is available for e-mail proxies only.
saml	SAML authentication method is mutually exclusive.

Command Default

The following table shows the default authentication methods for WebVPN and e-mail proxies:

Protocol	Default Authentication Method
IMAP4S	Mailhost (required)
POP3S	Mailhost (required)
SMTPS	AAA
WebVPN	AAA

Command Modes

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

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

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

Command History

Release	Modification
8.0(2)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group webvpn-attributes configuration mode for WebVPN.
8.0(2)	This command was modified to reflect changes to certificate authentication requirements.
9.5(2)	This command was modified to reflect support for SAML 2.0
9.7(1)	The existing authenticatioin attribute is modified to include an option for multiple-certificate authentication.

Usage Guidelines

At least one authentication method is required. For WebVPN, for example, you can specify AAA authentication, certificate authentication, or both. You can enter these commands in either order.

WebVPN certificate authentication requires that HTTPS user certificates be required for the respective interfaces. That is, for this selection to be operational, before you can specify certificate authentication, you must have specified the interface in an **authentication-certificate** command.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group webvpn-attributes configuration mode.

For WebVPN, you can require both AAA and certificate authentication. In this case, users must provide both a certificate and a username and password. For e-mail proxy authentication, you can require more than one authentication method. Specifying the command again overwrites the current configuration.

Examples

The following example shows how to require that WebVPN users provide certificates for authentication:

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

Examples

The following example shows how to require that WebVPN users provide certificates for authentication:

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

Related Commands

Command	Description
authentication-certificate	Requests a certificate from a WebVPN client establishing a connection.
show running-config	Displays the current tunnel group configuration.
clear configure aaa	Removes or resets the configured AAA values.
show running-config aaa	Displays the AAA configuration.

authentication eap-proxy

For L2TP over IPsec connections, to enable EAP and permit the ASA to proxy the PPP authentication process to an external RADIUS authentication server, use the **authentication eap-proxy** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication eap-proxy
no authentication eap-proxy

Syntax Description

This command has no keywords or arguments.

Command Default

By default, EAP is not a permitted authentication protocol.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel group type.

Examples

The following example entered in config-ppp configuration mode, permits EAP for PPP connections for the tunnel group named ppremotegrp:

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication eap
ciscoasa(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication key

To enable authentication for IS-IS, use the **authentication key** command in router isis configuration mode. To disable such authentication, use the **no** form of this command

authentication key [**0** | **8**] *password* [**level-1** | **level-2**]
no authentication key [**0** | **8**] *password* [**level-1** | **level-2**]

Syntax Description

password	Enables authentication and specifies the key.
level-1	(Optional) Enables authentication for Level 1 packets only.
level-2	(Optional) Enables authentication for Level 2 packets only.

Command Default

No key authentication is provided for IS-IS packets at the router level.

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If no password is configured with the **key** command, no key authentication is performed.

Key authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the authentication mode command.

Only one authentication key is applied to IS-IS at one time. That is, if you configure a second authentication key command, the first is overridden.

If neither the **level-1** nor **level-2** keyword is configured, the password applies to both levels.

You can specify authentication for an individual IS-IS interface by using the **isis authentication key** command.



Note In IS-IS, the **authentication key-chain** command is used to select live for the globally configured key chain. Due to the absence of the key chain infrastructure in ASA, we supply the key along with the command.

Examples

The following example configures IS-IS to accept and send any key belonging to the key chain named site1:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).

Command	Description
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.

Command	Description
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

authentication key eigrp

To enable authentication of EIGRP packets and specify the authentication key, use the **authentication key eigrp** command in interface configuration mode. To disable EIGRP authentication, use the **no** form of this command.

authentication key eigrp *as-number key* **key-id** *key-id*
no authentication key eigrp *as-number*

Syntax Description

as-number	The autonomous system number of the EIGRP process being authenticated. This must be the same value as configured for the EIGRP routing process.
key	Key to authenticate EIGRP updates. The key can contain up to 16 characters.
key-id *key-id*	Key identification value; valid values range from 1 to 255.

Command Default

EIGRP authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

You must configure both the **authentication mode eigrp** and the **authentication key eigrp** commands on an interface to enable EIGRP message authentication. Use the **show running-config interface** command to view the **authentication** commands configured on an interface.

Examples

The following examples shows EIGRP authentication configured on interface GigabitEthernet0/3:

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# authentication mode eigrp md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

Related Commands

Command	Description
authentication mode eigrp	Specifies the type of authentication used for EIGRP authentication.

authentication mode

To specify the type of authentication used in IS-IS packets for the IS-IS instance, use the **authentication mode** command in router isis configuration mode. To restore clear text authentication, use the **no** form of this command.

authentication mode { **md5** | **text** } [**level-1** | **level-2**]
no authentication mode

Syntax Description

md5	Message Digest 5 (MD5) authentication.
text	Clear text authentication.
level-1	(Optional) Enables the specified authentication for Level 1 packets only.
level-2	(Optional) Enables the specified authentication for Level 2 packets only.

Command Default

No authentication is provided for IS-IS packets at the router level by use of this command, although you can configure clear text (plain text) authentication by other means, such as the **area-password** command or the **domain-password** command.

Command Modes

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

Usage Guidelines

If neither the **level-1** nor **level-2** keyword is configured, the mode applies to both levels.

You can specify the type of authentication and the level to which it applies for a single IS-IS interface, rather than per IS-IS instance, by using the **isis authentication mode** command.

If you had clear text authentication configured by using the **area-password** or **domain-password** command, the authentication mode command overrides both of those commands.

If you configure the authentication mode command and subsequently try to configure the **area-password** or **domain-password** command, you will not be allowed to do so. If you truly want to configure clear text authentication using the **area-password** or **domain-password** command, you must use the **no authentication mode** command first.

Examples

The following example configures MD5 authentication for the IS-IS instance on Level 1 packets:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

authentication ms-chap-v1

For L2TP over IPsec connections, to enable Microsoft CHAP, Version 1 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode.To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command. To disable Microsoft CHAP, Version 1, use the **no** form of this command.

authentication ms-chap-v1
no authentication ms-chap-v1

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel-group type. This protocol is similar to CHAP, but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

authentication ms-chap-v2

For L2TP over IPsec connections, to enable Microsoft CHAP, Version 2 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication ms-chap-v2
no authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ppp-attributes configurationn	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel-group type.

This protocol is similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than clear text passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel group database or just the specified tunnel group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

authentication pap

For L2TP over IPsec connections, to permit PAP authentication for PPP, use the **authentication pap** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication pap
no authentication pap

Syntax Description

This command has no keywords or arguments.

Command Default

By default, PAP is not a permitted authentication protocol.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the L2TP or IPsec tunnel group type.

This protocol passes the clear text username and password during authentication and is not secure.

Examples

The following example entered in config-ppp configuration mode, permits PAP for PPP connections for a tunnel group named ppppremotegrps:

```
ciscoasa(config)# tunnel-group ppppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication pap
ciscoasa(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.

Command	Description
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication send-only

To specify for the IS-IS instance that authentication is performed only on IS-IS packets being sent (not received), use the **authentication send-only** command in router isis configuration mode. To configure authentication to be performed on packets being sent and received, use the **no** form of this command.

authentication send-only [**level-1** | **level-2**]
no authentication send-only

Syntax Description

level-1	(Optional) Authentication is performed only on Level 1 packets that are being sent (not received).
level-2	(Optional) Authentication is performed only on Level 2 packets that are being sent (not received).

Command Default

If authentication is configured at the router level, it applies to IS-IS packets being sent and received.

Command Modes

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

Usage Guidelines

Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. The routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then specify the **no authentication send-only** command to disable the send only feature.

If neither the **level-1** nor **level-2** keyword is configured, the send only feature applies to both levels.

This command can apply to clear text authentication or MD5 authentication. The mode is determined by the **authentication mode** command.

Examples

The following example configures IS-IS Level 1 packets to use clear text authentication on packets being sent (not received):

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication key-chain site1 level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.

Command	Description
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.

Command	Description
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

authentication-attr-from-server

To specify which authentication server authorization attributes to apply to the connection when double authentication is enabled, use the **authentication-attr-from-server** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

authentication-attr-from-server { **primary** | **secondary** }
no authentication-attr-from-server

Syntax Description

primary	Uses the primary authentication server.
secondary	Uses the secondary authentication server.

Command Default

The default value is **primary**.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **authentication-attr-from-server** command selects the authentication server from which the ASA extracts the authorization attributes to be applied to the connection.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies that the authorization attributes to be applied to the connection must come from the secondary authentication server:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-attr-from-server secondary
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the prefill username feature.

Command	Description
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

authentication-certificate

To request a certificate from a WebVPN client establishing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

authentication-certificate *interface-name*
no authentication-certificate [*interface-name*]

Syntax Description

interface-name The name of the interface used to establish the connection. Available interfaces names are:

- **inside** Name of interface GigabitEthernet 0/1
- **outside** Name of interface GigabitEthernet 0/0

Command Default

If you omit the **authentication-certificate** command, client certificate authentication is disabled. If you do not specify an interface name with the **authentication-certificate** command, the default interface name is **inside**.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

For this command to take effect, WebVPN must already be enabled on the corresponding interface. An interface is configured and named with the **interface**, **IP address**, and **nameif** commands.

This command applies only to WebVPN client connections; however, the ability to specify client certificate authentication for management connections with the **http authentication-certificate** command is available on all platforms, including those that do not support WebVPN.

The ASA validates certificates using the PKI trustpoints. If a certificate does not pass validation, then one of the following actions occurs:

If:	Then:
The local CA embedded in the ASA is not enabled.	The ASA closes the SSL connection.

If:	Then:
The local CA is enabled, and AAA authentication is not enabled.	The ASA redirects the client to the certificate enrollment page for the local CA to obtain a certificate.
Both the local CA and AAA authentication are enabled.	The client is redirected to a AAA authentication page. If configured, the client also is presented with a link to the enrollment page for the local CA.

Examples

The following example configures certificate authentication for WebVPN user connections on the outside interface:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
authentication (tunnel-group webvpn configuration mode)	Specifies that the members of a tunnel group must use a digital certificate for authentication.
http authentication-certificate	Specifies authentication by means of certificate for ASDM management connections to the ASA.
interface	Configures the interface used to establish the connection
show running-config ssl	Displays the current set of configured SSL commands.
ssl trust-point	Configures the SSL certificate trustpoint.

authentication-exclude

To enable end users to browse to configured links without logging in to clientless SSL VPN, enter the **authentication-exclude** command in webvpn configuration mode. Use this command multiple times to permit acccess to multiple sites.

authentication-exclude *url-fnmatch*

Syntax Description

url-fnmatch	Identifies the link to exempt from the requirement to log in to a clientless SSL VPN.

Command Default

Disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

This feature is useful when you require some internal resources to be available for public use via SSL VPN.

You need to distribute information about the links to end users in an SSL VPN-mangled form, for example, by browsing to these resources using SSL VPN and copying the resulting URLs into the information about links that you distribute.

Examples

The following example shows how to exempt two sites from authentication requirements:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 authentication-exclude http://www.example.com/public/*
ciscoasa
(config-webvpn)#
authentication-exclude *example.html
ciscoasa
(config-webvpn)#
ciscoasa
 #
```

authentication-port

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

authentication-port *port*
no authentication-port

Syntax Description

port	A port number, in the range 1-65535, for RADIUS authentication.

Command Default

By default, the device listens for RADIUS on port 1645 (in compliance with RFC 2058). If the port is not specified, the RADIUS authentication default port number 1645 is used.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Semantic change to the command to support the specification of server ports on a per-host basis for server groups that contain RADIUS servers.

Usage Guidelines

This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to assign authentication functions. If your RADIUS authentication server uses a port other than 1645, you must configure the ASA for the appropriate port before starting the RADIUS service with the **aaa-server** command.

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

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry interval of 7 seconds, and configures authentication port 1650.

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

```
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication on a server designated by the aaa-server command or by ASDM user authentication.
aaa-server host	Enters aaa-server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

authentication-server-group (imap4s, pop3s, smtps) (Deprecated)

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

To specify the set of authentication servers to use for e-mail proxies, use the **authentication-server-group** command in various modes. To remove authentication servers from the configuration, use the **no** form of this command.

authentication-server-group *group_tag*
no authentication-server-group

Syntax Description

group_tag	Identifies the previously configured authentication server or group of servers.

Command Default

No authentication servers are configured by default.

Command Modes

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

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

Command History

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

Usage Guidelines

The ASA authenticates users to verify their identity.

If you configure AAA authentication, you must configure this attribute as well. Otherwise, authentication always fails.

Use the **aaa-server** command to configure authentication servers.

Examples

The following example shows how to configure an IMAP4S e-mail proxy to use the set of authentication servers named “IMAP4SSVRS”:

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# authentication-server-group IMAP4SSVRS
```

Related Commands

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

authentication-server-group (tunnel-group general-attributes)

To specify the AAA server group to use for user authentication for a tunnel group, use the **authentication-server-group** command in tunnel-group general-attributes configuration mode. To return this attribute to the default, use the **no** form of this command.

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]
authentication-server-group [(*interface_name*)] *server_group*

Syntax Description

interface_name	(Optional) Specifies the interface at which the IPsec tunnel terminates.
LOCAL	(Optional) Requires authentication with the local user database if all of the servers in the server group have been deactivated due to communication failures.
server_group	Identifies the previously configured authentication server or group of servers.

Command Default

The default setting for the server-group in this command is **LOCAL**.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
8.0(2)	This command was enhanced to allow per-interface authentication for IPsec connections.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Use the **aaa-server** command to configure authentication servers and the **aaa-server-host** command to add servers to a previously configured AAA server group.

Examples

The following example entered in config-general configuration mode, configures an authentication server group named aaa-server456 for an IPsec remote access tunnel group named remotegrp:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
```

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server	Creates a AAA server group and configures AAA server parameters that are group-specific and common to all group hosts.
aaa-server host	Adds servers to a previously configured AAA server group and configures host-specific AAA server parameters.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

authorization-required

To require users to authorize successfully prior to connecting, use the **authorization-required** command in various modes. To remove the attribute from the configuration, use the **no** form of this command.

authorization-required
no authorization-required

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
7.2(1)	Replaced the webvpn configuration mode with the imap4s, pop3s, and smtps configuration modes.
9.5(2)	This command was deprecated for the following modes: imap4s, pop3s, and smtps.

Examples

The following example requires authorization based on the complete DN for users connecting through a remote access tunnel group named remotegrp. The first command configures the tunnel-group type as ipsec_ra (IPsec remote access) for the remote group named remotegrp. The second command enters tunnel-group general-attributes configuration mode for the specified tunnel group, and the last command specifies that authorization is required for the named tunnel group.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-required
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
authorization-dn-attributes	Specifies the primary and secondary subject DN fields to use as the username for authorization.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

authorization-server-group (imap4s, pop3s, smtps) (Deprecated)

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

To specify the set of authorization servers to use for a tunnel group for all remote access VPNs, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command.

authorization-server-group *group_tag*
no authorization-server-group

Syntax Description

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

Command Default

No authorization servers are configured by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
9.5(2)	This command was deprecated.

Usage Guidelines

The ASA uses authorization to verify the level of access to network resources that users are permitted. Use the server configurations for authorization that you used with the **aaa-server** command.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group general-attributes mode.

When VPN authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example shows how to configure POP3S e-mail proxy to use the set of authorization servers named “POP3Spermit”:

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)# authorization-server-group POP3Spermit
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

authorization-server-group (tunnel-group general-attributes)

To specify the set of authorization servers to use for a tunnel group for all remote access VPNs, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command.

authorization-server-group [(*if_name*)] *group_tag*
no authorization-server-group

Syntax Description

group_tag	Identifies the previously configured authorization server or group of servers. Use the **aaa-server** command to configure authorization servers.
(*if_name*)	(Optional) The name of the interface on which the tunnel terminates. You must include the parentheses.

Command Default

No authorization servers are configured by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.

Usage Guidelines

The ASA uses authorization to verify the level of access to network resources that users are permitted. Use the server configurations for authorization that you used with the aaa-server command.

If you enter this command in webvpn configuration mode, it is transformed into the same command in tunnel-group general-attributes mode.

When VPN authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example entered in tunnel-general configuration mode, configures an authorization server group named “aaa-server78” for an IPsec remote-access tunnel group named “remotegrp”:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

authorize-only

To enable authorize-only mode for a RADIUS AAA server group, use the **authorize-only** command in aaa-server group configuration mode. To disable authorize-only mode, use the **no** form of this command.

authorize-only
no authorize-only

Syntax Description

This command has no arguments or keywords.

Command Default

Authorize-only mode is not enabled.

Command Modes

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

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

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to configure a RADIUS server group in authorize-only mode for ISE Change of Authorization (CoA). If you use authorize-only mode, any RADIUS common password configured for a RADIUS host are ignored.

The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is no longer required to apply access control lists (ACLs) for each VPN session established with the ASA.

When an end user requests a VPN connection, the ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network. An accounting start message is sent to the ISE to register the session. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA. The ISE sends a policy update to the ASA via a CoA "policy push." This identifies a new user ACL that provides increased network access privileges. Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates.

Examples

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE. Include the **authorize-only** command in the server group configuration, because the server group will not be used for authentication.

```
ciscoasa(config)# aaa-server ise protocol radius
```

```
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Related Commands

Command	Description
dynamic-authorization	Enables dynamic authorization for the RADIUS server group.
interim-accounting-update	Enables the generation of RADIUS interim-accounting-update messages.
without-csd	Switches off hostscan processing for connections that are made to a specific tunnel-group.

auth-prompt

To specify or change the AAA challenge text for through-the-ASA user sessions, use the **auth-prompt** command in global configuration mode. To remove the authentication challenge text, use the **no** form of this command.

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*
no auth-prompt prompt [**prompt** | **accept** | **reject**]

Syntax Description

accept	If a user authentication via Telnet is accepted, displays the prompt string.
prompt	The AAA challenge prompt string follows this keyword.
reject	If a user authentication via Telnet is rejected, displays the prompt string.
string	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters, spaces, and punctuation characters are permitted. Entering a question mark or pressing the Enter key ends the string. (The question mark appears in the string.)

Command Default

If you do not specify an authentication prompt:

- FTP users see FTP authentication .
- HTTP users see HTTP Authentication.
- Telnet users see no challenge text.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Minor semantic changes.

Usage Guidelines

The auth-prompt command lets you specify the AAA challenge text for HTTP, FTP, and Telnet access through the ASA when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users see when logging in.

If user authentication occurs from Telnet, you can use the accept and reject options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the ASA displays the auth-prompt accept text, if specified, to the user; otherwise, it displays the reject text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The accept and reject text do not appear.



Note Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example sets the authentication prompt to the string "Please enter your username and password.":

```
ciscoasa(config)# auth
-prompt prompt Please enter your username and password
```

After this string is added to the configuration, users see the following:

```
Please enter your username and password
User Name:
Password:
```

For Telnet users, you can also provide separate messages to display when the ASA accepts or rejects the authentication attempt; for example:

```
ciscoasa(config)# auth-prompt reject Authentication failed. Try again.
ciscoasa(config)# auth-prompt accept Authentication succeeded.
```

The following example sets the authentication prompt for a successful authentication to the string, "You're OK."

```
ciscoasa(config)# auth-prompt accept You're OK.
```

After successfully authenticating, the user sees the following message:

```
You're OK.
```

Related Commands

Command	Description
clear configure auth-prompt	Removes the previously specified authentication prompt challenge text and reverts to the default value, if any.
show running-config auth-prompt	Displays the current authentication prompt challenge text.

auto-signon

To configure the ASA to automatically pass user login credentials for clientless SSL VPN connections on to internal servers, use the **auto-signon** command in any of three modes: webvpn configuration, webvpn group configuration, or webvpn username configuration mode. To disable auto-signon to a particular server, use the **no** form of this command with the original **ip**, **uri**, and **auth-type** arguments. To disable auto-signon to all servers, use the **no** form of this command without arguments.

auto-signon allow { **ip** *ip-address ip-mask* | **uri** *resource-mask* } **auth-type** { **basic** | **ftp** | **ntlm** | **all** }
no auto-signon [**allow** { **ip** *ip-address ip-mask* | **uri** *resource-mask* } **auth-type** { **basic** | **ftp** | **ntlm** | **all** }]

Syntax Description

all	Specifies both the NTLM and HTTP Basic authentication methods.
allow	Enables authentication to a particular server.
auth-type	Enables selection of an authentication method.
basic	Specifies the HTTP Basic authentication method.
ftp	Ftp and cifs authentication type.
ip	Specifies that an IP address and mask identifies the servers to be authenticated to.
ip-address	In conjunction with *ip-mask* , identifies the IP address range of the servers to be authenticated to.
ip-mask	In conjunction with *ip-address* , identifies the IP address range of the servers to be authenticated to.
ntlm	Specifies the NTLMv1 authentication method.
resource-mask	Identifies the URI mask of the servers to be authenticated to.
uri	Specifies that a URI mask identifies the servers to be authenticated to.

Command Default

By default, this feature is disabled for all servers.

Command Modes

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

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

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

Command History

Release	Modification
7.1(1)	This command was added.
8.0(1)	NTLMv2 support was added. The **ntlm** keyword includes both NTLMv1 and NTLMv2.

Usage Guidelines

The **auto-signon** command is a single sign-on method for clientless SSL VPN users. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, HTTP Basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).

You can use the auto-signon feature in three modes: webvpn configuration group-policy, webvpn configuration, or webvpn username configuration mode. The typical precedence behavior applies, where username supersedes group, and group supersedes global. The mode you choose depends on the desired scope of authentication:

Mode	Scope
Webvpn configuration	All WebVPN users globally
Webvpn group configuration	A subset of WebVPN users defined by a group policy
Webvpn username configuration	An individual WebVPN user

Examples

The following example configures auto-signon for all clientless users, using NTLM authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow ip 10.1.1.0
 255.255.255.0
 auth-type ntlm
```

The following example configures auto-signon for all clientless users, using HTTP Basic authentication, to servers defined by the URI mask https://*.example.com/*:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
The following example configures auto-signon for clientless users ExamplePolicy group policy,
 using either HTTP Basic or NTLM authentication, to servers defined by the URI mask
https://*.example.com/*:
```

```
ciscoasa(config)# group-policy ExamplePolicy attributes

ciscoasa(config-group-policy)# webvpn

ciscoasa(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

The following example configures auto-signon for a user named Anyuser, using HTTP Basic authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# auto-signon allow ip 10.1.1.0
 255.255.255.0
 auth-type basic
```

Related Commands

Command	Description
show running-config webvpn auto-signon	Displays auto-signon assignments of the running configuration.

auto-summary

To enable the automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable route summarization, use the **no** form of this command.

auto-summary
no auto-summary

Syntax Description

This command has no arguments or keywords.

Command Default

Route summarization is enabled for RIP Version 1, RIP Version 2, and EIGRP.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	Support for EIGRP was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

RIP Version 1 always uses automatic summarization. You cannot disable automatic summarization for RIP Version 1.

If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised.

EIGRP summary routes are given an administrative distance value of 5. You cannot configure this value.

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables RIP route summarization:

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
ciscoasa(config-router)# no auto-summary
```

The following example disables automatic EIGRP route summarization:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# no auto-summary
```

Related Commands

Command	Description
clear configure router	Clears all **router** commands and router configuration mode commands from the running configuration.
router eigrp	Enables the EIGRP routing process and enters EIGRP router configuration mode.
router rip	Enables the RIP routing process and enters RIP router configuration mode.
show running-config router	Displays the **router** commands and router configuration mode commands in the running configuration.

auto-update device-id

To configure the ASA device ID for use with an Auto Update Server, use the **auto-update device-id** command in global configuration mode. To remove the device ID, use the **no** form of this command.

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** | [*if_name*] | **mac-address** [*if_name*] | **string** *text*]
no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** | [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

Syntax Description

hardware-serial	Uses the hardware serial number of the ASA to uniquely identify the device.
hostname	Uses the hostname of the ASA to uniquely identify the device.
ipaddress [*if_name*]	Uses the IP address of the ASA to uniquely identify the ASA. By default, the ASA uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the *if_name* option.
mac-address [*if_name*]	Uses the MAC address of the ASA to uniquely identify the ASA. By default, the ASA uses the MAC address of the interface used to communicate with the Auto Update Server. If you want to use a different MAC address, specify the *if_name* option.
string *text*	Specifies the text string to uniquely identify the device to the Auto Update Server.

Command Default

The default ID is the hostname.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example sets the device ID to the serial number:

```
ciscoasa(config)# auto-update device-id hardware-serial
```

Related Commands

auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.

auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-at

To schedule a specific time for the ASA to poll the Auto Update Server, use the **auto-update poll-at** command in global configuration mode. To remove all specified scheduling times for the ASA to poll the Auto Update Server, use the **no** form of this command.

auto-update poll-at *days-of-the-week time* [**randomize** *minutes* [*retry_count* [*retry_period*]]]
no auto-update poll-at *days-of-the-week time* [**randomize** *minutes* [*retry_count* [*retry_period*]]]

Syntax Description

days-of-the-week	Any single day or combination of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday. Other possible values are daily (Monday through Sunday), weekdays (Monday through Friday) and weekend (Saturday and Sunday).
randomize >*minutes*	Specifies the period to randomize the poll time following the specified start time. from from 1 to 1439 minutes.
>*retry_count*	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
>*retry_period*	Specifies how long to wait between connection attempts. The default is 5 minutes. The range is from 1 and 35791 minutes.
>*time*	Specifies the time in the format HH:MM at which to start the poll. For example, 8:00 is 8:00 AM and 20:00 is 8:00 PM.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **auto-update poll-at** command specifies a time at which to poll for updates. If you enable the **randomize** option, the polling occurs at a random time within the range of the first >*time* option and the specified number of minutes. The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

In the following example, the ASA polls the Auto Update Server every Friday and Saturday night at a random time between 10:00 p.m. and 11:00 p.m. If the ASA is unable to contact the server, it tries two more times every 10 minutes.

```
ciscoasa(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
ciscoasa(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the ASA.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-period

To configure how often the ASA checks for updates from an Auto Update Server, use the **auto-update poll-period** command in global configuration mode. To reset the parameters to the defaults, use the **no** form of this command.

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]
no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

Syntax Description

poll_period	Specifies how often, in minutes, to poll an Auto Update Server, between 1 and 35791. The default is 720 minutes (12 hours).
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait, in minutes, between connection attempts, between 1 and 35791. The default is 5 minutes.

Command Default

The default poll period is 720 minutes (12 hours).

The default number of times to try reconnecting to the Auto Update Server if the first attempt fails is 0.

The default period to wait between connection attempts is 5 minutes.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

The following example sets the poll period to 360 minutes, the retries to 1, and the retry period to 3 minutes:

```
ciscoasa(config)# auto-update poll-period 360 1 3
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update server

To identify the Auto Update Server, use the **auto-update server** command in global configuration mode. To remove the server, use the **no** form of this command.

auto-update server *url* [**source** *interface*] { **verify-certificate** | **no-verification** }
no auto-update server *url* [**source** *interface*] { **verify-certificate** | **no-verification** }

Syntax Description

no-verification	Does not verify the Auto Update Server certificate.
source *interface*	Specifies which interface to use when sending requests to the Auto Update Server. If you specify the same interface specified by the **management-access** command, the Auto Update requests travel over the same IPsec VPN tunnel used for management access.
url	Specifies the location of the Auto Update Server using the following syntax: **https:**[[*user:password@location* [*:port*]] */pathname*
verify-certificate	For HTTPS, verifies the certificate returned by the Auto Update Server. This setting is the default.

Command Default

9.1 and earlier: Certificate verification is disabled.

9.2(1) and later: The **verify-certificate** option is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The command was modified to add support for multiple servers.
9.2(1)	The Auto Update server certificate verification is now enabled by default. The **no-verification** keyword was added.

Usage Guidelines

The ASA periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

You can configure multiple servers to work with auto-update. When checking for updates, a connection is made to the first server, but if that fails, then the next server is contacted. This process continues until all the

servers have been tried. If all of them fail to connect, then a retry starting with the first server is attempted if the auto-update poll period has been configured to retry the connection.

For auto-update functionality to work correctly, you must use the **boot system configuration** command and ensure that it specifies a valid boot image. In addition, you must use the **asdm image** command with auto-update to update the ASDM software image.

If the interface specified in the **source** *interface* argument is the same interface specified with the **management-access** command, requests to the Auto Update Server are sent over the VPN tunnel.

9.2(1) and later: The Auto Update server certificate verification is now enabled by default; for new configurations, you must explicitly disable certificate verification. If you are upgrading from an earlier release, and you did not enable certificate verification, then certificate verification is not enabled, and you see the following warning:

```
WARNING: The certificate provided by the auto-update servers will not be verified. In order
 to verify this certificate please use the verify-certificate option.
```

The configuration will be migrated to explicitly configure no verification:

auto-update server no-verification

Examples

The following example sets the Auto Update Server URL and specifies the interface as outside:

```
ciscoasa(config)# auto-update server http://10.1.1.1:1741/ source outside verify-certificate
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the ASA.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update timeout

To set a timeout period in which to contact the Auto Update Server, use the **auto-update timeout** command in global configuration mode. To remove the timeout, use the **no** form of this command.

auto-update timeout [*period*]
no auto-update timeout [*period*]

Syntax Description

period Specifies the timeout period in minutes between 1 and 35791. The default is 0, which means there is no timeout. You cannot set the timeout to 0; use the **no** form of the command to reset it to 0.

Command Default

The default timeout is 0, which sets the ASA to never time out.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

A timeout condition is reported with syslog message 201008.

If the Auto Update Server has not been contacted for the timeout period, the ASA stops all traffic going through it. Set a timeout to ensure that the ASA has the most recent image and configuration.

Examples

The following example sets the timeout to 24 hours:

```
ciscoasa(config)# auto-update timeout 1440
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

avc

To enable Application Visibility Control (AVC) and download the Vulnerability Database (VDB), use the **avc** command in global configuration mode. To disable AVC and remove all AVC network-service objects, groups, and other data structures, use the **no** form of the command.

When downloading the VDB manually, the command is for Privileged EXEC mode.

avc
no avc
avc download vdb

Syntax Description

download vdb	Manually download the Vulnerability Database (VDB). Use this command if a VDB automatic download fails.

Command Default

No defaults.

Command Modes

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

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

Command History

Release	Modification
9.24(1)	This command was added.

Usage Guidelines

You must enable Application Visibility and Control (AVC) to download the Vulnerability Database (VDB) and create the network-service objects and groups that you can use in access control rules or other policies that use extended ACLs. If you subsequently disable AVC, all downloaded and extracted files, and the AVC network-service objects and groups, are deleted.

When you view the running configuration, the **avc** command shows the version of the VDB currently installed on the **vdb-version** parameter. A 0 indicates the VDB is not installed. This parameter is not configurable.

VDB Download Guidelines

- You must configure DNS and DNS lookup on an interface through which support.sourcefire.com can be contacted, so that the Vulnerability Database (VDB) can be downloaded. A route to that server must also be available.

- In a high-availability group, the VDB download must be possible over the management interface, because the standby unit cannot pass traffic over data interfaces. The standby unit downloads VDB updates itself.
- In a cluster, each unit downloads the VDB separately.
- In multiple context mode, only one user context downloads the VDB, and shares it with contexts where AVC is enabled.
- VDB download uses HTTPS, so it requires that a trusted CA certificate from third-party Certificate Authority is installed on the device, to ensure a secure connection.
- When downloading a VDB update, after the download is complete, the system clears the existing AVC network-service objects and groups, and other AVC files, and rebuilds them. Your AVC-based policies will stop working until the update is complete.
- The VDB download file is about 70 MB. An extracted VDB requires at least 450 MB of disk space. Ensure there is adequate free space on the device to download and extract the VDB.

.

Example

The following example enables AVC and starts the VDB download. After giving the download time to complete, use the **show avc status** command to verify when the download is complete and the AVC feature is ENABLED and READY to be used.

```
ciscoasa(config)# avc
...
ciscoasa(config)# show avc status
AVC (Application Visibility and Control): ENABLED : READY
VDB (containing app definition) download status: UP-TO-DATE
VDB version: current 397, last 0
VDB last update at 15:29:57 UTC Apr 29 2025; last update attempt at 15:27:36 UTC Apr 29
2025; next update at 15:30:55 UTC May 6 2025.
VDB download link:
https://50.19.123.95/auto-update/auto-dl.cgi/Download/files/Cisco_VDB_Fingerprint_Database-4.5.0-399.sh.REL.tar
```

The following example manually downloads the VDB. This action is necessary only if a VDB download fails.

```
ciscoasa# avc download vdb
```

Related Commands

show avc	Shows the status and associated information about the AVC system.