CHAPTER 3

acl-netmask-convert through auto-update timeout Commands

acl-netmask-convert

Use the **acl-netmask-convert** command in aaa-server host configuration mode to specify how the security appliance treats netmasks received in a downloadable ACL from a RADIUS server which is accessed by using the **aaa-server host** command. Use the **no** form of this command to remove the speciied behavior for the security appliance.

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

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

The **auto-detect** keyword is helpful when you are uncertain how the RADIUS server is configured; however, wildcard netmask expressions with "holes" in them cannot be unambiguously detected and converted. For example, the wildcard netmask 0.0.255.0 permits anything in the third octet and can be used validly on Cisco VPN 3000 series concentrators, but the security appliance may not detect this expression as a wildcard netmask.

Examples

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

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

Related Commands

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

action

To either apply access policies to a session or teminate the session, use the **action** command in dynamic-access-policy-record configuration mode.

To reset the session to apply an access policy to a session, use the **no** form of the command.

action {continue | terminate}

no action {continue | terminate}

Syntax Description

continue	Applies the access policies to the session.
terminate	Terminates the connection.

Defaults

The default value is continue.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Dynamic-access-policy- record configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **continue** keyword to apply the access policies to the session in all of the selected DAP records. Use the **terminate** keyword to terminate the connection in any of the selected DAP records.

Examples

The following example shows how to terminate a session for the DAP policy Finance:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# action terminate
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

action-uri

To specify a web server URI to receive a username and password for single sign-on authentication, use the **action-uri** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command. Use the **no** form of the command to reset the URI parameter value, .

action-uri *string*

no action-uri

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The URI for an authentication program. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for the complete URI is 2048 characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

A URI or Uniform Resource Identifier is a compact string of characters that identifies a point of content on the Internet, whether it be a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the web page address, which is a particular form or subset of URI called a URL.

The WebVPN server of the security appliance can use a POST request to submit a single sign-on authentication request to an authenticating web server. To accomplish this, configure the security appliance to pass a username and a password to an action URI on an authenticating web server using an HTTP POST request. The **action-uri** command specifies the location and name of the authentication program on the web server to which the security appliance sends the POST request.

You can discover the action URI on the authenticating web server by connecting to the web server login page directly with a browser. The URL of the login web page displayed in your browser is the action URI for the authenticating web server.

For ease of entry, you can enter URIs on multiple, sequential lines. The security appliance then concatenates the lines into the URI as you enter them. While the maximum characters per action-uri line is 255 characters, you can enter fewer characters on each line.

Note Any question mark in the string must be preceded by a CTRL-v escape sequence.

Examples

The following example specifies the URI on www.example.com:

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
hostname(config)# aaa-server testgrp1 host www.example.com
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```

Note You must include the hostname and protocol in the action URI. In the preceding example, these are included in http://www.example.com at the start of the URI.

Related Commands

Command	Description
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the SSO server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

activation-key

To change the activation key on the security appliance and check the activation key running on the security appliance against the activation key that is stored as a hidden file in the Flash partition of the security appliance, use the **activation-key** command in global configuration mode. Use the **no** form of this command to deactivate the specified activation key running on the security appliance.

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

no activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

Syntax Description

activation-key-four-tuple	Activation key; see the "Usage Guidelines" section for formatting guidelines.
activation-key-five-tuple	Activation key; see the "Usage Guidelines" section for formatting guidelines.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Enter the *activation-key-four-tuple* as a four-element hexadecimal string with one space between each element, or *activation-key-five-tuple* as a five-element hexidecimal string withe one space between each element as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal.

The key is not stored in the configuration file. The key is tied to the serial number.

Examples

The following example shows how to change the activation key on the security appliance:

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

Related Commands

Command	Description
show activation-key	Displays the activation key.

activex-relay

To enable or disable ActiveX controls on WebVPN sessions, use the **activex-relay** command in group-policy webvpn configuration mode or username webvpn configuration mode. Use the **no** form of this command to inherit the **activex-relay** command from the default group policy.

activex-relay {**enable | disable**}

no activex-relay

Syntax Description

enable	Enables ActiveX on WebVPN sessions.
disable	Disables ActiveX on WebVPN sessions.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Group-policy webvpn configuration	•	—	•	—	—
Username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **activex-relay enable** command to let users launch ActiveX controls from the WebVPN browser. These applications use the WebVPN session to download and upload ActiveX controls. The ActiveX relay remains in force until the WebVPN session closes.

Examples

The following commands enable ActiveX controls on WebVPN sessions associated with a given group policy:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

The following commands disable ActiveX controls on WebVPN sessions associated with a given username:

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay disable
```

```
hostname(config-username-webvpn)
```

address-pool (tunnel-group general attributes mode)

To specify a list of address pools for allocating addresses to remote clients, use the **address-pool** command in tunnel-group general-attributes configuration mode. To eliminate address pools, use the **no** form of this command.

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

Syntax Description

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
interface name	(Optional) Specifies the interface to be used for the address pool.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

The address-pools settings in the group-policy **address-pools** command override the local pool settings in the tunnel group **address-pool** command.

The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

Examples

The following example entered in config-tunnel-general configuration mode, specifies a list of address pools for allocating addresses to remote clients for an IPSec remote-access tunnel group test:

```
hostname(config)# tunnel-group test type remote-access
hostname(config)# tunnel-group test general
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN remote-access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

address-pools (group-policy attributes configuration mode)

To specify a list of address pools for allocating addresses to remote clients, use the **address-pools** command in group-policy attributes configuration mode. To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command.

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

Syntax Description

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
none	Specifies that no address pools are configured and disables inheritance from other sources of group policy.
value	Specifies a list of up to 6 address pools from which to assign addresses.

Defaults

By default, the address pool attribute allows inheritance.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The address-pools settings in this command override the local pool settings in the group. You can specify a list of up to six local address pools to use for local address allocation.

The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

The command **address-pools none** disables this attribute from being inherited from other sources of policy, such as the DefaultGrpPolicy. The command **no address pools none** removes the **address-pools none** command from the configuration, restoring the default value, which is to allow inheritance.

Examples

The following example entered in config-general configuration mode, configures pool_1 and pool_20 as lists of address pools to use for allocating addresses to remote clients for GroupPolicy1:

```
hostname(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
hostname(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# address-pools value pool_1 pool_20
hostname(config-group-policy)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN group policies.
clear configure group-policy	Clears all configured group policies.
show running-config group-policy	Shows the configuration for all group-policies or for a particular group-policy.

admin-context

To set the admin context for the system configuration, use the **admin-context** command in global configuration mode. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the security appliance software or allowing remote management for an administrator), it uses one of the contexts that is designated as the admin context.

admin-context *name*

Syntax Description

name	Sets the name as a string up to 32 characters long. If you have not defined any contexts yet, then first specify the admin context name with this command. Then, the first context you add using the **context** command must be the specified admin context name. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. "System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.

Defaults

For a new security appliance in multiple context mode, the admin context is called "admin."

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can set any context to be the admin context, as long as the context configuration resides on the internal Flash memory.

You cannot remove the current admin context, unless you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to be "administrator":

```
hostname(config)# admin-context administrator
```

Related Commands

Command	Description
clear configure context	Removes all contexts from the system configuration.
context	Configures a context in the system configuration and enters context configuration mode.
show admin-context	shows the current admin context name.

alias

To manually translate an address and perform DNS reply modification, use the **alias** command in global configuration mode. To remove an **alias** command, use the **no** form of this command.

alias (*interface_name*) *real_ip mapped_ip* [*netmask*]

no alias (*interface_name*) *real_ip mapped_ip* [*netmask*]

Syntax Description

(*interface_name*)	Specifies the ingress interface name for traffic destined for the mapped IP address (or the egress interface name for traffic from the mapped IP address). Be sure to include the parentheses in the command.
mapped_ip	Specifies the IP address to which you want to translate the real IP address.
netmask	(Optional) Specifies the subnet mask for both IP addresses. Enter **255.255.255.255** for a host mask.
real_ip	Specifies the real IP address.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command functionality has been replaced by outside NAT commands, including the **nat** and **static** commands with the **dns** keyword. We recommend that you use outside NAT instead of the **alias** command.

Use this command to perform address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, use the **alias** command to redirect traffic to another address, such as 209.165.201.30.

Note If the **alias** command is used for DNS rewrite and not for other address translation, disable **proxy-arp** on the alias-enabled interface. Use the **sysopt noproxyarp** command to prevent the security appliance from pulling traffic toward itself via **proxy-arp** for generic NAT processing.

After changing or removing an **alias** command, use the **clear xlate** command.

An A (address) record must exist in the DNS zone file for the "dnat" address in the **alias** command.

The **alias** command has two uses that can be summarized in the following ways:

- If the security appliance gets a packet that is destined for the *mapped_ip*, you can configure the **alias** command to send it to the *real_ip*.
- If the security appliance gets a DNS packet that is returned to the security appliance destined for *real_ip*, you can configure the **alias** command to alter the DNS packet to change the destination network address to *mapped_ip*.

The **alias** command automatically interacts with the DNS servers on your network to ensure that domain name access to the aliased IP address is handled transparently.

Specify a net alias by using network addresses for the *real_ip* and *mapped_ip* IP addresses. For example, the **alias 192.168.201.0 209.165.201.0 255.255.255.224** command creates aliases for each IP address between 209.165.201.1 and 209.165.201.30.

To access an **alias** *mapped_ip* address with **static** and **access-list** commands, specify the *mapped_ip* address in the **access-list** command as the address from which traffic is permitted as follows:

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq
ftp-data
hostname(config)# access-group acl_out in interface outside
```

An alias is specified with the inside address 192.168.201.1 mapping to the destination address 209.165.201.1.

When the inside network client 209.165.201.2 connects to example.com, the DNS response from an external DNS server to the internal client's query would be altered by the security appliance to be 192.168.201.29. If the security appliance uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the security appliance with SRC=209.165.201.2 and DST=192.168.201.29. The security appliance translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

Examples

The following example shows that the inside network contains the IP address 209.165.201.29, which on the Internet belongs to example.com. When inside clients try to access example.com, the packets do not go to the security appliance because the client assumes that the 209.165.201.29 is on the local inside network. To correct this behavior, use the **alias** command as follows:

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

This example shows a web server that is on the inside at 10.1.1.11 and the **static** command that was created at 209.165.201.11. The source host is on the outside with address 209.165.201.7. A DNS server on the outside has a record for www.example.com as follows:

```
dns-server# www.example.com. IN A 209.165.201.11
```

You must include the period at the end of the www.example.com. domain name.

This example shows how to use the **alias** command:

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

The security appliance changes the name server replies to 10.1.1.11 for inside clients to directly connect to the web server.

To provide access you also need the following commands:

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host 209.165.201.7
```

Related Commands

Command	Description
access-list extended	Creates an access list.
clear configure alias	Removes all **alias** commands from the configuration.
show running-config alias	Displays the overlapping addresses with dual NAT commands in the configuration.
static	Configures a one-to-one address translation rule by mapping a local IP address to a global IP address, or a local port to a global port.

allocate-interface

To allocate interfaces to a security context, use the **allocate-interface** command in context configuration mode. To remove an interface from a context, use the **no** form of this command.

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

Syntax Description

invisible	(Default) Allows context users to only see the mapped name (if configured) in the **show interface** command.

map_name	(Optional) Sets a mapped name.
	The *map_name* is an alphanumeric alias for the interface that can be used within the context instead of the interface ID. If you do not specify a mapped name, the interface ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces are being used by the context.
	A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names:
	`int0`
	`inta`
	`int_0`
	For subinterfaces, you can specify a range of mapped names.
	See the "Usage Guidelines" section for more information about ranges.

physical_interface	Sets the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values. Do not include a space between the interface type and the port number.
subinterface	Sets the subinterface number. You can identify a range of subinterfaces.
visible	(Optional) Allows context users to see physical interface properties in the **show interface** command even if you set a mapped name.

Defaults

The interface ID is invisible in the **show interface** command output by default if you set a mapped name.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can enter this command multiple times to specify different ranges. To change the mapped name or visible setting, reenter the command for a given interface ID, and set the new values; you do not need to enter the **no allocate-interface** command and start over. If you remove the **allocate-interface** command, the security appliance removes any interface-related configuration in the context.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA adaptive security appliance, you can use the dedicated management interface, Management 0/0, (either the physical interface or a subinterface) as a third interface for management traffic.

Note The management interface for transparent mode does not flood a packet out the interface when that packet is not in the MAC address table.

You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.

If you specify a range of subinterfaces, you can specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range:

  ```
  int0-int10
  ```

  If you enter **gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5**, for example, the command fails.

- The numeric portion of the mapped name must include the same quantity of numbers as the subinterface range. For example, both ranges include 100 interfaces:

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  If you enter **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15**, for example, the command fails.

Examples

The following example shows gigabitethernet0/1.100, gigabitethernet0/1.200, and gigabitethernet0/2.300 through gigabitethernet0/1.305 assigned to the context. The mapped names are int1 through int8.

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
```

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.
show interface	Displays the runtime status and statistics of interfaces.
vlan	Assigns a VLAN ID to a subinterface.

allocate-ips

To allocate an IPS virtual sensor to a security context if you have the AIP SSM installed, use the **allocate-ips** command in context configuration mode. To remove a virtual sensor from a context, use the **no** form of this command.

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

Syntax Description

default	(Optional) Sets one sensor per context as the default sensor; if the context configuration does not specify a sensor name, the context uses this default sensor. You can only configure one default sensor per context. If you want to change the default sensor, enter the **no allocate-ips** *sensor_name* command to remove the current default sensor before you allocate a new default sensor. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor on the AIP SSM.
mapped_name	(Optional) Sets a mapped name as an alias for the sensor name that can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called “sensor1” and “sensor2,” then you can map the “highsec” and “lowsec” senors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.
sensor_name	Sets the sensor name configured on the AIP SSM. To view the sensors that are configured on the AIP SSM, enter **allocate-ips ?**. All available sensors are listed. You can also enter the **show ips** command. In the system execution space, the **show ips** command lists all available sensors; if you enter it in the context, it shows the sensors you already assigned to the context. If you specify a sensor name that does not yet exist on the AIP SSM, you get an error, but the **allocate-ips** command is entered as is. Until you create a sensor of that name on the AIP SSM, the context assumes the sensor is down.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the AIP SSM using the **ips** command, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the AIP SSM is used. You can assign the same sensor to multiple contexts.

Note You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

Examples

The following example assigns sensor1 and sensor2 to context A, and sensor1 and sensor3 to context B. Both contexts map the sensor names to "ips1" and "ips2." In context A, sensor1 is set as the default sensor, but in context B, no default is set so the default that is configured on the AIP SSM is used.

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
ips	Diverts traffic to the AIP SSM for inspection.
show context	Shows a list of contexts (system execution space) or information about the current context.
show ips	Shows the virtual sensors configured on the AIP SSM.

apcf

To enable an Application Profile Customization Framework profile, use the **apcf** command in webvpn configuration mode. To disable a particular APCF script, use the **no** version of the command. To disable all APCF scripts, use the **no** version of the command without arguments.

apcf URL/filename.ext

no apcf [URL/filename.ext]

Syntax Description

filename.extension	Specifies the name of the APCF customization script. These scripts are always in XML format. The extension might be .xml, .txt, .doc or one of many others
URL	Specifies the location of the APCF profile to load and use on the security appliance. Use one of the following URLs: http://, https://, tftp://, ftp://; flash:/, disk#:/' The URL might include a server, port, and path. If you provide only the filename, the default URL is flash:/. You can use the **copy** command to copy an APCF profile to flash memory.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **apcf** command enables the security appliance to handle non-standard web applications and web resources so that they render correctly over a WebVPN connection. An APCF profile contains a script that specifies when (pre, post), where (header, body, request, response), and what data to transform for a particular application.

You can use multiple APCF profiles on the security appliance. When you do, the security appliance applies each one of them in the order of oldest to newest.

We recommend that you use the apcf command only with the support of the Cisco TAC.

Examples

The following example shows how to enable an APCF named apcf1, located on flash memory at /apcf:

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

This example shows how to enable an APCF named apcf2.xml, located on an https server called myserver, port 1440 with the path being /apcf:

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

Related Commands

Command	Description
proxy-bypass	Configures minimal content rewriting for a particular application.
rewrite	Determines whether traffic travels through the security appliance.
show running config webvpn apcf	Displays the APCF configuration.

appl-acl

To identify a previously configured web-type ACL to apply to a session, use the **appl-acl** command in dap webvpn configuration mode. To remove the attribute from the configuration, use the **no** version of the command; to remove all web-type ACLs, use the **no** version of the command without arguments.

appl-acl *identifier*

no appl-acl [*identifier*]

Syntax Description

identifier	The name of the previously configured web-type ACL Maximum 240 characters.

Defaults

No default value or behaviors.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dap webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To configure web-type ACLs, use the **access-list_webtype** command in global configuration mode.

Use the **appl-acl** command multiple times to apply more than one web-type ACL to the DAP policy.

Examples

The following example shows how to apply the previously configured web-type ACL called newacl to the dynamic access policy:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dynamic-access-policy-record)# appl-acl newacl
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
access-list_webtype	Create web-type ACLs.

application-access

To customize the Application Access fiels of the WebVPN Home page that is displayed to authenticated WebVPN users, and the Application Access window that is launched when the user selects an application, use the **application-access** command from customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

Syntax Description

message	Changes the message displayed under the title of the Application Access field.
style	Changes the style of the Application Access field.
text	Changes the text of the Application Access field.
title	Changes the title of the Application Access field.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).
window	Changes the Application Access window.

Defaults

The default title text of the Application Access field is “Application Access”.

The default title style of the Application Access field is:

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text of the Application Access field is “Start Application Client”.

The default message style of the Application Access field is:

background-color:#99CCCC;color:maroon;font-size:smaller.

The default window text of the Application Access window is:

“Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.”.

The default window style of the Application Access window is:

background-color:#99CCCC;color:black;font-weight:bold.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

This command is accessed by using the **webvpn** command or the **tunnel-group webvpn-attributes** command.

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

The following tips can help you make the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the background color of the Application Access field to the RGB hex value 66FFFF, a shade of green:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

Related Commands

Command	Description
application-access hide-details	Enable or disables the display of the application details in the Application Access window.
browse-networks	Customizes the Browse Networks field of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application field of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.

application-access hide-details

To hide application details that are displayed in the WebVPN Applications Access window, use the **application-access hide-details** command from customization configuration mode, which is accessed by using the **webvpn** command or the **tunnel-group webvpn-attributes** command. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

application-access hide-details {**enable | disable**}

no application-access [**hide-details** {**enable | disable**}]

Syntax Description

disable	Does not hide application details in the Application Access window.
enable	Hides application details in the Application Access window.

Defaults

The default is disabled. Application details appear in the Application Access window.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example disables the appearance of the application details:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# application-access hide-details disable
```

Related Commands

Command	Description
application-access	Customizes the Application Access field of the WebVPN Home page.
browse-networks	Customizes the Browse Networks field of the WebVPN Home page.
web-applications	Customizes the Web Application field of the WebVPN Home page.

area

To create an OSPF 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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:

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

Related Commands

Command	Description
area authentication	Enables authentication for the OSPF area.
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 OSPF 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 on 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 on the area specified by the *area_id*.

Defaults

Area authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified OSPF 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:

```
hostname(config-router)# area 1 authentication message-digest
hostname(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 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. 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**

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

Defaults

The default value of *cost* is 1.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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:

```
hostname(config-router)# area 1 default-cost 5
hostname(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 filter-list prefix

To filter prefixes advertised in Type 3 LSAs between OSPF 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	Identifier of 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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 is configured in the private network, then it will send Type 5 LSAs (describing private networks) which 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:

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(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. 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	Identifier of 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.

Defaults

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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:

```
area 1 nssa no-redistribution
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:

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# 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 range

To consolidate and summarize routes at an area boundary, use the **area range** command in router 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	Identifier of 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.

Defaults

The address range status is set to advertise.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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 address range. This behavior is called *route summarization*. You can configure multiple **area range** commands for an area. Thus, 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:

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(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. To remove the stub area function, use the **no** form of this command.

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

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

Syntax Description

area_id	Identifier for 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.

Defaults

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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:

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

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

To define an OSPF virtual link, use the **area virtual-link** command in router 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** [**message-digest | null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest | null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *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.
authentication-key *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 *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.
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.

Defaults

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** *key*: No key is predefined.
- **message-digest-key** *key_id* **md5** *key*: No key is predefined.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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** *key* or **message-digest-key** *key_id* **md5** *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.

To remove an option from a virtual link, use the **no** form of the command with the option that you want removed. To remove the virtual link, use the **no area** *area_id* **virtual-link** command.

Examples

The following example establishes a virtual link with MD5 authentication:

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
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.

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. 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).

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 security appliance receives an ARP request for the specified IP address, then it responds with the security appliance MAC address. When the security appliance receives traffic destined for the host belonging to the IP address, the security appliance 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 security appliance 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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.

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the security appliance, 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:

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

Related Commands

Command	Description
arp timeout	Sets the time before the security appliance 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 timeout

To set the time before the security appliance 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. 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.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

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

```
hostname(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.

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

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 security appliance drops the packet. **Note** The management-specific interface, if present, never floods packets even if this parameter is set to flood.
interface_name	The 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.

Defaults

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the security appliance. 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

When you enable ARP inspection, the security appliance 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 security appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the security appliance 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 now 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, so long as 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 security appliance, such as management traffic.

Examples

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

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(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.

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. You can display the session IDs of all active ASDM sessions using the **show asdm sessions** command.

Defaults

No default behavior or values.

Command Modes

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

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

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.

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# 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. You can display the session IDs of all active ASDM sessions using the **show asdm log_sessions** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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 security appliance. 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.

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# 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.

Defaults

No default behavior or values.

Command Modes

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

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

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:

```
hostname(config)# asdm history enable
hostname(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 adaptive security appliance, 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 adaptive security appliance, this URL indicates the external Flash memory card. • **flash:/**[*path*/]*filename* This URL indicates the internal Flash memory.

Defaults

If you do not include this command in your startup configuration, the security appliance uses the first ASDM image it finds at startup. It searches the root directory of internal Flash memory and then external Flash memory. The security appliance 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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 security appliance using the last-configured image location.

If you do not include this command in your startup configuration, the security appliance uses the first ASDM image it finds at startup. It searches the root directory of internal Flash memory and then external Flash memory. The security appliance 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 security appliance 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 security appliance not to match the configuration on the Auto Update Server. This mismatch causes the security appliance 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:

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

ip_addr	IP address used internally by ASDM to define the network topology.
netmask	The subnet mask for *ip_addr.*
if_name	The name of the interface through which ASDM is accessed.
ipv6_addr/prefix	The IPv6 address and prefix used internally by ASDM to define the network topology.

Defaults

No default behavior or values.

Command Modes

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

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

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.

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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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, where the context for the outbound connection is in the standby group.

The **asr-group** command causes incoming packets to be re-classified with the interface of the same asr-group if a flow with the incoming interface cannot be found. If re-classification 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.

Examples

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

Context ctx1 configuration:

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

Context ctx2 configuration:

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

Related Commands

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

assertion-consumer-url

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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance 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's SSL certificate.

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

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
hostname(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 Single Sign-On server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

attribute

To specify attribute value pairs that the security appliance writes to the DAP attribute database, enter the **attribute** command in dap test attributes mode. Use this command multiple times to enter multiple attribute value pairs.

attribute *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, anti-virus, anti-spyware, 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:

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Normally the security appliance 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 security appliance writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record.

Examples

The following example assumes that security appliance selects two DAP records if the authenticated user is a member of the SAP group and has anti-virus software installed on the endpoint system. The Endpoint ID for the anti-virus 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
	url-entry = enable

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)# attribute aaa.ldap.memberof SAP
hostname(config-dap-test-attr)# attribute endpoint.av.nav.exists true
hostname(config-dap-test-attr)# exit

hostname # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

hostname #
```

Related Commandsl

Command	Description
display	Displays current attribute list.s
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes submode.
test dynamic-access-policy execute	Executes the logic that generates 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on 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 configures name of the authentication cookie to be used for SSO by the security appliance.

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:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49X1Kc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5d
c/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Pa
th=/
```

Examples

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

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

authentication-certificate

To request a certificate from a WebVPN client establing 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 GigabitEthernet0/1 • **outside** Name of interface GigabitEthernet0/0

Defaults

- 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:

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

Command History

Release	Modification
8.0(2)	This command was introduced.

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 the platforms that do not support WebVPN.

The security appliance validates certificates against 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 security appliance is not enabled.	The security appliance closes the SSL connection.
The local CA is enabled, and AAA authentication is not enabled.	The security appliance 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:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(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 security appliance.
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 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 clientless SSL VPN.

Command Default

Disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This feature is useful when you require that some internal resources 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:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-exclude http://www.site.com/public/*
hostname(config-webvpn)#authentication-exclude *announcement.html
hostname(config-webvpn)# hostname #
```

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 security appliance authenticates users to verify their identity.

authentication {[**aaa**] [**certificate**] [**mailhost**] [**piggyback**]}

no authentication [**aaa**] [**certificate**] [**mailhost**] [**piggyback**]

Syntax Description

aaa	Provides a username and password that the security appliance checks against a previously configured AAA server.
certificate	Provides a certificate during SSL negotiation.
mailhost	Authenticates via the remote mail server. For SMTPS only. For the IMAP4S and POP3S, mailhost authentication is mandatory and not displayed as a configurable option.
piggyback	Requires that an HTTPS WebVPN session already exists. Piggyback authentication is available for e-mail proxies only.

Defaults

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
SMTPS configuration	•	—	•	—	—
Webvpn configuration	•		•		

Command History

Release	Modification
8.0(2)	This command was introduced.

Release	Modification
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.

Usage Guidelines

At least one authentication method is required. For WebVPN, for example, you can specify AAA authentication, certificate authentication, or both. You can specify these 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 to the same command in tunnel-group webvpn-attributes configuration mode.

For WebVPN, you can require both AAA and certificate authentication, in which 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:

```
hostname(config)# webvpn
hostname(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	Remove/reset the configured AAA values.
show running-config aaa	Display the AAA configuration.

authentication eap-proxy

For L2TP over IPSec connections, to enable EAP and permit the security appliance 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.

Defaults

By default, EAP is not a permitted authentication protocol.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

Examples

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

```
hostname(config)# tunnel-group pppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group pppremotegrp ppp-attributes
hostname(config-ppp)# authentication eap
hostname(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
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 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 values 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.

Defaults

EIGRP authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

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:

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# authentication mode eigrp md5
hostname(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 eigrp

To specify the type of authentication used for EIGRP authentication, use the **authentication mode eigrp** command in interface configuration mode. To restore the default authentication method, use the **no** form of this command.

authentication mode eigrp *as-num* **md5**

no authentication mode eigrp *as-num* **md5**

Syntax Description

as-num	The autonomous system number of the EIGRP routing process.
md5	Uses MD5 for EIGRP message authentication.

Defaults

No authentication is provided by default.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

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:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# authentication mode eigrp 100 md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

Related Commands

Command	Description
authentication key eigrp	Enables authentication of EIGRP packets and specifies the authentication key.

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. 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.

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-v2

no authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

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. 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.

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 2, 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

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 authentiation for PPP, use the **authentication pap** command in tunnel-group ppp-attributes configuration mode. This protocol passes cleartext username and password during authentication and is not secure.

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.

Defaults

By default, PAP is not a permitted authentication protocol.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

Examples

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

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication pap
hostname(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
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-certificate

To request a certificate from a WebVPN client establing 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 GigabitEthernet0/1 • **outside** Name of interface GigabitEthernet0/0

Defaults

- 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:

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

Command History

Release	Modification
8.0(2)	This command was introduced.

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 the platforms that do not support WebVPN.

The security appliance validates certificates against 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 security appliance is not enabled.	The security appliance closes the SSL connection.
The local CA is enabled, and AAA authentication is not enabled.	The security appliance 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:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(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 security appliance.
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-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. This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to assign authentication functions:

authentication-port *port*

no authentication-port

Syntax Description

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

Defaults

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:

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

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

If your RADIUS authentication server uses a port other than 1645, you must configure the security appliance for the appropriate port prior to 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.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

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

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

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. The security appliance authenticates users to verify their identity.

authentication-server-group *group_tag*

no authentication-server-group

Syntax Description

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

Defaults

No authentication servers are configured by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config)# imap4s
hostname(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**]

no authentication-server-group [(*interface_name*)] *server_group*

Syntax Description

interface_name	(Optional) Specifies the interface where the IPSec tunnel terminates.
LOCAL	(Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either **LOCAL** or **NONE,** do not use the **LOCAL** keyword here.
server_group	Identifies the previously configured authentication server or group of servers.

Defaults

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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.
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:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(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-dn-attributes

Note As of Release 8.0(4) this command has been deprecated. Use the **username-from-certificate** command in place of this command.

To specify the primary and secondary subject DN fields to use as the username for authorization, use the **authorization-dn-attributes** command in various configuration modes. To remove the attribute from the configuration and restore default values, use the **no** form of this command.

authorization-dn-attributes {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no authorization-dn-attributes

Syntax Description

primary-attr	Specifies the attribute to use to derive a name for an authorization query from a certificate.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a name for an authorization query from a digital certificate.
use-entire-name	Specifies that the security appliance must use the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.

Defaults

The default value for the primary attribute is CN (Common Name).

The default value for the secondary attribute is OU (Organization Unit).

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
7.2(1)	Added imap4s, pop3, and smtps configuration modes.

Usage Guidelines

Possible values for primary and secondary attributes include the following:

Attribute	Definition
CN	Common Name: the name of a person, system, or other entity
OU	Organizational Unit: the subgroup within the organization (O)
O	Organization: the name of the company, institution, agency, association or other entity
L	Locality: the city or town where the organization is located
SP	State/Province: the state or province where the organization is located
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
EA	E-mail address
T	Title
N	Name
GN	Given Name
SN	Surname
I	Initials
GENQ	Generational Qualifier
DNQ	Domain Name Qualifier
UID	User Identifier
UPN	User Principal Name
SER	Serial Number
use-entire-name	Use entire DN name

Examples

The following example, entered in global configuration mode, creates an IPSec remote access tunnel group named remotegrp and specifies the use of CN (Common Name) as the primary attribute to use to derive a name for an authorization query from a digital certificate:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

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 general-attributes	Specifies the general attributes for the named 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** version of this command.

authorization-required

no authorization-required

Syntax Description

This command has no arguments or keywords.

Defaults

Authorization-required is disabled by default.

Command Modes

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

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

Command History

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

Examples

The following example, entered in global configuration mode, 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:

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

To specify the set of authorization servers to use with WebVPN and e-mail proxies, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command. The security appliance uses authorization to verify the level of access to network resources that users are permitted.

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.

Defaults

No authorization servers are configured by default.

Command Modes

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

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

Command History

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

Usage Guidelines

If you enter this command in webvpn configuration mode, it is transformed to 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”:

```
hostname(config)# pop3s
```

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

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

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

auth-prompt

To specify or change the AAA challenge text for through-the-security appliance 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, display the prompt *string*.
prompt	The AAA challenge prompt string follows this keyword.
reject	If a user authentication via Telnet is rejected, display the prompt *string*.
string	A string of up to 235 alphanumeric characters or 30 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.)

Defaults

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:

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

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 security appliance 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 view when logging in.

If the 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 security appliance 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 are not displayed.

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.":

```
hostname(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 security appliance accepts or rejects the authentication attempt; for example:

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

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

```
hostname(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 security appliance 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. The authentication method can be NTLM (includes NTLMv1 and NTLMv2), HTTP Basic authentication, or both. 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	Specifies an 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.

Defaults

By default, this feature is disabled for all servers.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Webvpn configuration (global)	•	—	•	—	—
Webvpn group policy configuration	•	—	•	—	—
Webvpn username configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.
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 upon 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 commands configure 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:

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

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

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

The following example commands configure 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/*:

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

The following example commands configure 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:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(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.

Defaults

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:

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

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Support for EIGRP 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:

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

The following example disables automatic EIGRP route summarization:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(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 security appliance 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 security appliance to uniquely identify the device.
hostname	Uses the hostname of the security appliance to uniquely identify the device.
ipaddress [*if_name*]	Uses the IP address of the security appliance to uniquely identify the security appliance. By default, the security appliance uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the *if_name*.
mac-address [*if_name*]	Uses the MAC address of the security appliance to uniquely identify the security appliance. By default, the security appliance 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*.
string *text*	Specifies the text string to uniquely identify the device to the Auto Update Server.

Defaults

The default ID is the hostname.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

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

Related Commands

auto-update poll-period	Sets how often the security appliance 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 security appliance 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 security appliance to poll the Auto Update Server, use the **auto-update poll-at** command from global configuration mode. To remove all specified scheduling times for the security appliance 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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **auto-update poll-at** command specifys 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* 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 security appliance 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 security appliance is unable to contact the server, it tries two more times every 10 minutes.

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

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance 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 security appliance.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-period

To configure how often the security appliance 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.

Defaults

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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

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

Related Commands

auto-update device-id	Sets the security appliance 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 security appliance 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. The security appliance periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

Syntax Description

interface	Specifies which interface to use when sending requests to the auto-update server.
url	Specifies the location of the Auto Update Server using the following syntax: **http**[**s**]**:**[[*user:password@*]*location* [:*port*]] **/** *pathname*
verify_certificate	Verifies the certificate returned by the Auto Update Server.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The command was modified to add support for multiple servers.

Usage Guidelines

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 will be contacted. This will continue 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 is configured to retry the connection.

For auto update functionality to work properly, you must use the **boot system configuration** command and ensure it specifies a valid boot image. Likewise, the **asdm image** command must be used 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 will be sent over the VPN tunnel.

Examples

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

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

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance 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 security appliance.
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. If the Auto Update Server has not been contacted for the timeout period, the security appliance stops all traffic through the security appliance. Set a timeout to ensure that the security appliance has the most recent image and configuration. 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.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A timeout condition is reported with system log message 201008.

Examples

The following example sets the timeout to 24 hours:

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

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance 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.