gateway through hw-module module shutdown Commands

gateway

To specify which group of call agents are managing a particular gateway, use the **gateway** command in mgcp map configuration mode. To remove the configuration, use the **no** form of this command.

gateway *ip_address* [*group_id*]

Syntax Description

gateway	The group of call agents that are managing a particular gateway.
group_id	The ID of the call agent group, from 0 to 2147483647.
ip_address	The IP address of the gateway.

Defaults

This command 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**
Mgcp map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **gateway** command to specify which group of call agents are managing a particular gateway. The IP address of the gateway is specified with the *ip_address* option. The *group_id* option is a number from 0 to 4294967295 that must correspond with the *group_id* of the call agents that are managing the gateway. A gateway may only belong to one group.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debugging information for MGCP.
mgcp-map	Defines an MGCP map and enables mgcp map configuration mode.
show mgcp	Displays MGCP configuration and session information.

gateway-fqdn

To configure the FQDN of the ASA. use the **gateway-fqdn** command. To remove the configuration, use the **no** form of this command.

gateway-fqdn value {**FQDN_Name** | **none**}

no gateway-fqdn

Syntax Description

fqdn-name	Defines the ASA FQDN to push down to the AnyConnect client.
none	Defines the FQDN as null value where the FQDN is not specified. The global FQDN configurd using hostname and domain-name commands will be used if available.

Defaults

The default FQDN name is not set in the default group policy. New group policies are set to inherit this value.

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 configuration	•		•		

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

If you have configured Load Balancing between your ASAs, specify the FQDN of the ASA in order to resolve the ASA IP address used for re-establishing the VPN session. This setting is critical to support client roaming between networks of different IP protocols (such as IPv4 to IPv6).

You cannot use the ASA FQDN present in the AnyConnect profile to derive the ASA IP address after roaming. The addresses may not match the correct device (the one the tunnel was established to) in the load balancing scenario.

If the ASA's FQDN is not pushed to the client, the client will try to reconnect to whatever IP address the tunnel had previously established. In order to support roaming between networks of different IP protocols (from IPv4 to IPv6), AnyConnect must perform name resolution of the device FQDN after roaming, so that it can determine which ASA address to use for re-establishing the tunnel. The client uses the ASA FQDN present in its profile during the initial connection. During subsequent session reconnects, it always uses the device FQDN pushed by ASA (and configured by the administrator in the group policy), when available. If the FQDN is not configured, the ASA derives the device FQDN (and sends it to the client) from whatever is set under Device Setup > Device Name/Password and Domain Name in ASDM.

If the device FQDN is not pushed by the ASA, the client cannot reestablish the VPN session after roaming between networks of different IP protocols.

Examples

The following example defines the FQDN of the ASA as ASAName.example.cisco.com

```
hostname(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy)#
```

The following example removes the FQDN of the ASA from the group policy. The group policy then inherits this value from the Default Group Policy.

```
hostname(config-group-policy)# no gateway-fqdn
hostname(config-group-policy)#
```

The following example defines the FQDN as having no value. The global FQDN configurd using hostname and domain-name commands will be used if available.

```
hostname(config-group-policy)# gateway-fqdn none
hostname(config-group-policy)#
```

group

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

group {**1** | **2** | **5** | **14** | **19** | **20** | **21** | **24**}

no group {**1** | **2** | **5** | **14** | **19** | **20** | **21** | **24**}

Syntax Description

1	Specifies the 768-bit Diffie-Hellman group 1 (not supported in FIPS mode).
2	Specifies the 1024-bit Diffie-Hellman group 2.
5	Specifies the 1536-bit Diffie-Hellman group 5.
14	Choose ECDH group as the IKEv2 DH key exchange group.
19	Choose ECDH groups as the IKEv2 DH key exchange group.
20	Choose ECDH groups as the IKEv2 DH key exchange group.
21	Choose ECDH groups as the IKEv2 DH key exchange group.
24	Choose ECDH groups as the IKEv2 DH key exchange group.

Defaults

The default Diffie-Hellman group is group 2.

Usage Guidelines

An IKEv2 SA is a key used in Phase 1 to enable IKEv2 peers to communicate securely in Phase 2. After entering the **crypto ikev2 policy** command, you can use the **group** command to set the SA Diffie-Hellman group. The ASA and the AnyConnect client use the group identifier to derive a shared secret without transmitting it to each other. The lower the Diffie-Hellman group number, the less CPU time it requires to execute. The higher the Diffie-Hellman group number, the greater the security.

When the AnyConnect client is operating in non-FIPS mode, the ASA supports Diffie-Hellman groups 1, 2 and 5. In FIPS mode, it supports groups 2 and 5. Therefore, if you configure the ASA to use *only* group 1, the AnyConnect client in FIPS mode will fail to connect.

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
Ikev2 policy configuration	•	—	•	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Added the ability to choose an ECDH group as the IKEv2 DH key exchange group.

Examples

The following example enters ikev2 policy configuration mode and sets the Diffie-Hellman group to group 5:

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 5
```

Related Commands

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

group-alias

To create one or more alternate names by which the user can refer to a tunnel group, use the **group-alias** command in tunnel-group webvpn configuration mode. To remove an alias from the list, use the **no** form of this command.

group-alias *name* [**enable** | **disable**]

no group-alias *name*

Syntax Description

disable	Disables the group alias.
enable	Enables a previously disabled group alias.
name	Specifies the name of a tunnel group alias. This can be any string you choose, except that the string cannot contain spaces.

Defaults

There is no default group alias, but if you do specify a group alias, that alias is enabled 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
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The group alias that you specify appears in the drop-down list on the login page. Each group can have multiple aliases or no alias. This command is useful when the same group is known by several common names, such as “Devtest” and “QA”.

Examples

The following example shows the commands for configuring the tunnel group named “devtest” and establishing the aliases “QA” and “Fra-QA” for the group:

```
hostname(config)# tunnel-group devtest type webvpn
hostname(config)# tunnel-group devtest webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias QA
hostname(config-tunnel-webvpn)# group-alias Fra-QA
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel group database or the named tunnel group configuration.
show webvpn group-alias	Displays the aliases for the specified tunnel group or for all tunnel groups.
tunnel-group webvpn-attributes	Enters the tunnel-group webvpn configuration mode for configuring WebVPN tunnel group attributes.

group-delimiter

To enable group name parsing and specify the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated, use the **group-delimiter** command in global configuration mode. To disable this group name parsing, use the **no** form of this command.

group-delimiter *delimiter*

no group-delimiter

Syntax Description

delimiter	Specifies the character to use as the group name delimiter. Valid values are: **@**, **#**, and **!**.

Defaults

By default, no delimiter is specified, disabling group-name parsing.

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 delimiter is used to parse tunnel group names from user names when tunnels are negotiated. By default, no delimiter is specified, disabling group name parsing.

Examples

This example shows the **group-delimiter** command to change the group delimiter to the hash mark (#):

```
hostname(config)# group-delimiter #
```

Related Commands

Command	Description
clear configure group-delimiter	Clears the configured group delimiter.
show running-config group-delimiter	Displays the current group delimiter value.
strip-group	Enables or disables strip group processing.

group-lock

To restrict remote users to access through the tunnel group only, issue the **group-lock** command in group-policy configuration mode or username configuration mode. To remove the **group-lock** attribute from the running configuration, use the **no** form of this command.

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

Syntax Description

none	Sets group-lock to a null value, thereby allowing no group lock restriction. Prevents inheriting a group lock value from a default or specified group policy.
value *tunnel-grp-name*	Specifies the name of an existing tunnel group that the ASA requires for the user to connect.

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 configuration	•	—	•	—	—
Username configuration	•	—	•	—	—

Usage Guidelines

To disable group lock, use the **group-lock none** command. The **no group-lock** command allows inheritance of a value from another group policy.

Group lock restricts users by checking if the group configured in the VPN client is the same as the tunnel group to which the user is assigned. If it is not, the ASA prevents the user from connecting. If you do not configure group lock, the ASA authenticates users without regard to the assigned group.

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set group lock for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# group-lock value tunnel group name
```

group-object

To add object groups, use the **group-object** command in protocol, network, service, and icmp-type, and object-group user configuration modes. To remove network object groups, use the **no** form of this command.

group-object *obj_grp_name*

no group-object *obj_grp_name*

Syntax Description

obj_grp_name	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." 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
Protocol, network, service, icmp-type, and object-group user configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(2)	Add support for adding object groups in the object-group user configuration mode for use with the Identity Firewall feature.

Usage Guidelines

The **group-object** command is used with the **object-group** command to define an object that itself is an object group. It is used in protocol, network, service, and icmp-type, object-group user configuration modes. This sub-command allows logical grouping of the same type of objects and construction of hierarchical object groups for structured configuration.

Duplicate objects are allowed in an object group if they are group objects. For example, if object 1 is in both group A and group B, it is allowed to define a group C which includes both A and B. It is not allowed, however, to include a group object which causes the group hierarchy to become circular. For example, it is not allowed to have group A include group B and then also have group B include group A.

The maximum allowed levels of a hierarchical object group is 10.

See the **user-group object** command for information about using the **group-object** command with the Identity Firewall feature.

Note The security appliance does not support IPv6 nested object groups, so you cannot use the **group-object** command for an object with IPv6 entities in it under another IPv6 object-group.

Examples

The following example shows how to use the **group-object** command in network configuration mode eliminate the need to duplicate hosts:

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)# access-list all permit tcp object-group all-hosts any eq w
```

The following example shows how to use the **group-object** command with the **object-group user** command to add a locally defined object group for use with the Identity Firewall feature:

```
hostname(config)# object-group user sampleuser1-group
hostname(config-object-group user)# description group members of sampleuser1-group
hostname(config-object-group user)# user-group CSCO\\group.sampleusers-all
hostname(config-object-group user)# user CSCO\user2
hostname(config-object-group user)# exit
hostname(config)# object-group user sampleuser2-group
hostname(config-object-group user)# description group members of sampleuser2-group
hostname(config-object-group user)# group-object sampleuser1-group
hostname(config-object-group user)# user-group CSCO\\group.sampleusers-marketing
hostname(config-object-group user)# user CSCO\user3
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
object-group user	Creates a user group object for the Identity Firewall feature.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

Syntax Description

external server-group *server_group*	Specifies the group policy as external and identifies the AAA server group for the ASA to query for attributes.
from *group-policy_name*	Initializes the attributes of this internal group policy to the values of a preexisting group policy.
internal	Identifies the group policy as internal.
name	Specifies the name of the group policy. The name can be up to 64 characters long and can contain spaces. Group names with spaces must be enclosed in double quotes, for example, “Sales Group”.
password *server_password*	Provides the password to use when retrieving attributes from the external AAA server group. The password can be up to 128 characters long and cannot contain spaces.

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.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A default group policy, named “DefaultGroupPolicy,” always exists on the ASA. However, this default group policy does not take effect unless you configure the ASA to use it. For configuration instructions, see the CLI configuration guide.

Use the **group-policy attributes** command to enter group-policy configuration mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
backup-servers	keep-client-config
banner	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

In addition, you can configure webvpn configuration mode attributes for the group policy, either by entering the **webvpn** command in group policy configuration mode or by entering the **group-policy attributes** command and then entering the **webvpn** command in group-webvpn configuration mode. See the description of the **group-policy attributes** command for details.

Examples

The following example shows how to create an internal group policy with the name "FirstGroup":

```
hostname(config)# group-policy FirstGroup internal
```

The following example shows how to create an external group policy with the name "ExternalGroup," the AAA server group "BostonAAA," and the password "12345678":

```
hostname(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

Related Commands

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

group-policy attributes

To enter the group-policy configuration mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, user the **no** form of this command.

group-policy *name* **attributes**

no group-policy *name* **attributes**

Syntax Description

name	Specifies the name of the group policy.

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.

Usage Guidelines

In group-policy configuration mode, you can configure Attribute-Value Pairs for a specified group policy or enter group-policy webvpn configuration mode to configure WebVPN attributes for the group.

The syntax of the commands in attributes mode have the following characteristics in common:

- The **no** form removes the attribute from the running configuration, and enables inheritance of a value from another group policy.
- The **none** keyword sets the attribute in the running configuration to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

A default group policy, named DefaultGroupPolicy, always exists on the ASA. However, this default group policy does not take effect unless you configure the ASA to use it. For configuration instructions, see the CLI configuration guide.

The **group-policy attributes** command enters group-policy configuration mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
backup-servers	keep-client-config
banner	none
client-access-rule	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

In addition, you can configure webvpn-mode attributes for the group policy, by entering the **group-policy attributes** command and then entering the **webvpn** command in group-policy configuration mode. See the description of the **webvpn** command (group-policy attributes and username attributes modes) for details.

Examples

The following example shows how to enter group-policy attributes mode for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy	Creates, edits, or removes a group policy.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn	Enters group-webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

group-prompt

To customize the group prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the ASA, use the **group-prompt** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

group-prompt {**text** | **style**} *value*

no group-prompt {**text** | **style**} *value*

Syntax Description

text	Specifies a change to the text.
style	Specifies a change the style.
value	The actual text to display or Cascading Style Sheet (CSS) parameters (the maximum bunber is 256 characters).

Defaults

The default text of the group prompt is “GROUP:”.

The default style of the group prompt is color:black;font-weight:bold;text-align:right.

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 customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

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

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

Examples

In the following example, the text is changed to “Corporate Group:”, and the default style is changed with the font weight increased to bolder:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# group-prompt text Corporate Group:
F1-asa1(config-webvpn-custom)# group-prompt style font-weight:bolder
```

Related Commands

Command	Description
password-prompt	Customizes the password prompt of the WebVPN page.
username-prompt	Customizes the username prompt of the WebVPN page.

group-search-timeout

To specify the maximum time to wait for a response from an Active Directory server queried using the **show ad-groups** command, use the **group-search-timeout** command in aaa-server host configuration mode. To remove the command from the configuration, use the **no** form of the command:

group-search-timeout *seconds*

no group-search-timeout *seconds*

Syntax Description

seconds	The time to wait for a response from the Active Directory server, from 1 to 300 seconds.

Defaults

The default is 10 seconds.

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
8.0(4)	This command is introduced.

Usage Guidelines

The **show ad-groups** command applies only to Active Directory servers using LDAP, and displays groups that are listed on an Active Directory server. Use the **group-search-timeout** command to adjust the time to wait for a response from the server.

Examples

The following example sets the timeout to 20 seconds:

```
hostname(config-aaa-server-host)#group-search-timeout 20
```

Related Commands

Command	Description
ldap-group-base-dn	Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.
show ad-groups	Displays groups that are listed on an Active Directory server.

group-url

To specify incoming URLs or IP addresses for the group, use the **group-url** command in tunnel-group webvpn configuration mode. To remove a URL from the list, use the **no** form of this command.

group-url *url* [**enable** | **disable**]

no group-url *url*

Syntax Description

disable	Disables the URL, but does not remove it from the list.
enable	Enables the URL.
url	Specifies a URL or IP address for this tunnel group.

Defaults

There is no default URL or IP address, but if you do specify a URL or IP address, it is enabled 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
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Specifying a group URL or IP address eliminates the need for the user to select a group at login. When a user logs in, the ASA looks for the user's incoming URL/address in the tunnel group policy table. If it finds the URL/address and if this command is enabled in the tunnel group, then the ASA automatically selects the associated tunnel group and presents the user with only the username and password fields in the login window. This simplifies the user interface and has the added advantage of never exposing the list of groups to the user. The login window that the user sees uses the customizations configured for that tunnel group.

If the URL/address is disabled and the **group-alias** command is configured, then the drop-down list of groups is also displayed, and the user must make a selection.

You can configure multiple URLs/addresses (or none) for a group. Each URL/address can be enabled or disabled individually. You must use a separate **group-url** command for each URL/address specified. You must specify the entire URL/address, including either the HTTP or HTTPS protocol.

You cannot associate the same URL/address with multiple groups. The ASA verifies the uniqueness of the URL/address before accepting it for a tunnel group.

Examples

The following example shows the commands for configuring the WebVPN tunnel group named “test” and establishing two group URLs, “http://www.cisco.com” and “https://supplier.example.com” for the group:

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com
hostname(config-tunnel-webvpn)# group-url https://supplier.example.com
hostname(config-tunnel-webvpn)#
```

The following example enables the group URLs http://www.cisco.com and http://192.168.10.10 for the tunnel group named RadiusServer:

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias “Cisco Remote Access” enable
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel group database or the named tunnel group configuration.
show webvpn group-url	Displays the URLs for the specified tunnel group or for all tunnel groups.
tunnel-group webvpn-attributes	Enters the webvpn configuration mode for configuring WebVPN tunnel group attributes.

h245-tunnel-block

To block H.245 tunneling in H.323, use the **h245-tunnel-block** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

h245-tunnel-block action [**drop-connection** | **log**]

no h245-tunnel-block action [**drop-connection** | **log**]

Syntax Description

drop-connection	Drops the call setup connection when an H.245 tunnel is detected.
log	Issues a log when an H.245 tunnel is detected.

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
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to block H.245 tunneling on an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# h245-tunnel-block action drop-connection
```

Related Commands

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

health-check

To enab;e the cluster health check feature, use the **health-check** command in cluster group configuration mode. To the health check, use the **no** form of this command.

health-check [**holdtime** *timeout*] [**vss-enabled**]

no health-check [**holdtime** *timeout*] [**vss-enabled**]

Syntax Description

holdtime *timeout*	(Optional) Determines the amount of time between keepalive or interface status messages, between .8 and 45 seconds. The default is 3 seconds.
vss-enabled	If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, then you might need to enable the **vss-enabled** option. For some switches, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable **vss-enabled**, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them.

Command Default

Health check is enabled by default, with a holdtime of 3 seconds.

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
Cluster group configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.
9.1(4)	We added the **vss-enabled** keyword.

Usage Guidelines

We recommend that you temporarily disable the health check with the **no health-check** command when any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the ASA or the switch, or adding an additional switch to form a VSS or vPC). After the cluster topology is stable, you must re-enable the cluster health check feature.

Keepalive messages between members determine member health. If a unit does not receive any keepalive messages from a peer unit within the holdtime period, the peer unit is considered unresponsive or dead. Interface status messages detect link failure. If an interface fails on a particular unit, but the same interface is active on other units, then the unit is removed from the cluster.

If a unit does not receive interface status messages within the holdtime, then the amount of time before the ASA removes a member from the cluster depends on the type of interface and whether the unit is an established member or is joining the cluster. For EtherChannels (spanned or not), if the interface is down on an established member, then the ASA removes the member after 9 seconds. If the unit is joining the cluster as a new member, the ASA waits 45 seconds before rejecting the new unit. For non-EtherChannels, the unit is removed after 500 ms, regardless of the member state.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units.

Examples

The following example disables the health check:

```
hostname(config)# cluster group cluster1
hostname(cfg-cluster)# no health-check
```

Related Commands

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

hello-interval

To specify the interval between EIGRP hello packets sent on an interface, use the **hello-interval** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

hello-interval eigrp *as-number seconds*

no hello-interval eigrp *as-number seconds*

Syntax Description

as-number	Specifies the autonomous system number of the EIGRP routing process.
seconds	Specifies the interval between hello packets that are sent on the interface. Valid values are from 1 to 65535 seconds.

Defaults

The default is 5 seconds.

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.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will occur. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

```
hostname(config-if)# hello-interval eigrp 100 10
hostname(config-if)# hold-time eigrp 100 30
```

Related Commands

Command	Description
hold-time	Configures the EIGRP hold time advertised in hello packets.

help

To display help information for the command specified, use the **help** command in user EXEC mode.

help {*command* | **?**}

Syntax Description

?	Displays all commands that are available in the current privilege level and mode.
command	Specifies the command for which to display the CLI help.

Defaults

No default behaviors 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
User EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **help** command displays help information about all commands. You can see help for an individual command by entering the **help** command followed by the command name. If you do not specify a command name and enter **?** instead, all commands that are available in the current privilege level and mode display.

If you enable the **pager** command and after 24 lines display, the listing pauses, and the following prompt appears:

```
<--- More --->
```

The More prompt uses syntax similar to the UNIX **more** command as follows:

- To see another screen of text, press the **Space** bar.
- To see the next line, press the **Enter** key.
- To return to the command line, press the **q** key.

Examples

The following example shows how to display help for the **rename** command:

```
hostname# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
```

```
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

hostname#
```

The following examples shows how to display help by entering the command name and a question mark:

```
hostname(config)# enable ?
usage: enable password <pwd> [encrypted]
```

Help is available for the core commands (not the **show**, **no**, or **clear** commands) by entering **?** at the command prompt:

```
hostname(config)# ?
aaa            Enable, disable, or view TACACS+ or RADIUS
               user authentication, authorization and accounting
…
```

Related Commands

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

hidden-parameter

To specify hidden parameters in the HTTP POST request that the ASA submits to the authenticating web server for SSO authentication, use the **hidden-parameter** command in aaa-server-host configuration mode. To remove all hidden parameters from the running configuration, use the **no** form of this command.

hidden-parameter *string*

no hidden-parameter

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	A hidden parameter embedded in the form and sent to the SSO server. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for all lines together—the complete hidden parameter—is 2048.

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

This is an SSO with HTTP Forms command.

The WebVPN server of the ASA uses an HTTP POST request to submit an SSO authentication request to an authenticating web server. That request may require specific hidden parameters from the SSO HTML form—other then username and password—that are not visible to the user. You can discover hidden parameters that the web server expects in the POST request by using a HTTP header analyzer on a form received from the web server.

The **hidden-parameter** command lets you specify a hidden parameter that the web server requires in the authentication POST request. If you use a header analyzer, you can copy and paste the entire hidden parameter string, including any encoded URL parameters.

For ease of entry, you can enter a hidden parameter on multiple, sequential lines. The ASA then concatenates the lines into a single hidden parameter. While the maximum characters per hidden-parameter 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 shows a hidden parameter comprised of four form entries and their values, separated by &. Excerpted from the POST request, the four entries and their values are:

- SMENC with a value of ISO-8859-1
- SMLOCALE with a value of US-EN
- target with a value of https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do %3FEMCOPageCode%3DENG
- smauthreason with a value of 0

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for SSO authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
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 prelogin cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

hidden-shares

To control the visibility of hidden shares for CIFS files, use the **hidden-shares** command in group-webvpn configuration mode. To remove the hidden shares option from the configuration, use the **no** form of this command.

hidden-shares {**none** | **visible**}

[**no**] **hidden-shares** {**none** | **visible**}

Syntax Description

none	Specifies that no configured hidden shares are visible or accessible to users.
visible	Reveals hidden shares, making them accessible to users.

Defaults

The default behavior for this command is none.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A hidden share is identified by a dollar sign ($) at the end of the share name. For example, drive C is shared as C$. With hidden shares, a shared folder is not displayed, and users are restricted from browsing or accessing these hidden resources.

The **no** form of the **hidden-shares** command removes the option from the configuration and disables hidden shares as a group policy attribute.

Examples

The following example makes visible WebVPN CIFS hidden-shares related to GroupPolicy2:

```
hostname(config)# webvpn
hostname(config-group-policy)# group-policy GroupPolicy2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# hidden-shares visible
hostname(config-group-webvpn)#
```

Related Commands

Command	Description
debug webvpn cifs	Displays debugging messages about the CIFS.
group-policy attributes	Enters group-policy configuration mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn configuration mode to configure WebVPN attributes for the group.
url-list	Configures a set of URLs for WebVPN users to access.
url-list	Applies a list of WebVPN servers and URLs to a particular user or group policy.

hold-time

To specify the hold time advertised by the ASA in EIGRP hello packets, use the **hold-time** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

hold-time eigrp *as-number seconds*

no hold-time eigrp *as-number seconds*

Syntax Description

as-number	The autonomous system number of the EIGRP routing process.
seconds	Specifies the hold time, in seconds. Valid values are from 1 to 65535 seconds.

Defaults

The default is 15 seconds.

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.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

This value is advertised in the EIGRP hello packets sent by the ASA. The EIGRP neighbors on that interface use this value to determine the availability of the ASA. If they do not receive a hello packet from the ASA during the advertised hold time, the EIGRP neighbors will consider the ASA to be unavailable.

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If the ASA does not receive a hello packet within the specified hold time, routes through this neighbor are considered unavailable.

Increasing the hold time delays route convergence across the network.

Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

```
hostname(config-if)# hello-interval eigrp 100 10
hostname(config-if)# hold-time eigrp 100 30
```

Related Commands

Command	Description
hello-interval	Specifies the interval between EIGRP hello packets sent on an interface.

homepage

To specify a URL for the web page that displays upon login for this WebVPN user or group policy, use the **homepage** command in webvpn configuration mode. To remove a configured home page, including a null value created by issuing the **homepage none** command, use the **no** form of this command.

homepage {**value** *url-string* | **none**}

no homepage

Syntax Description

none	Indicates that there is no WebVPN home page. Sets a null value, thereby disallowing a home page. Prevents inheriting a home page.
value *url-string*	Provides a URL for the home page. The string must begin with either http:// or https://.

Defaults

There is no default home page.

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
7.0(1)	This command was introduced.

Usage Guidelines

To specify a home page URL for users associated with the group policy, enter a value for the URL string in this command. To inherit a home page from the default group policy, use the **no** form of the comand. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a home page, use the **homepage none** command.

Clientless users are immediately brought to this page after successful authentication. AnyConnect launches the default web browser to this URL upon successful establishment of the VPN connection. On Linux platforms, AnyConnect does not currently support this command and ignores it.

Examples

The following example shows how to specify www.example.com as the home page for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# homepage value http://www.example.com
```

Related Commands

Command	Description
webvpn	Lets you enter webvpn configuration mode to configure parameters that apply to group policies or usernames.

homepage use-smart-tunnel

To allow the group policy home page to use the smart tunnel feature when clientless SSL VPN is used, use the **homepage use-smart-tunnel** command in the group-policy webvpn configuration mode.

homepage {**value** *url-string* | **none**}

homepage use-smart-tunnel

Syntax Description

none	Indicates that there is no WebVPN home page. Sets a null value, thereby disallowing a home page. Prevents inheriting a home page.
value *url-string*	Provides a URL for the home page. The string must begin with either http:// or https://.

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	•	—	•	—	—

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

You can use the HTTP capture tool to monitor the browser session and verify that the smart tunnel was initiated during the WebVPN connection. What you see in the browser capture determines whether the request is forwarded to the web page without degradation and whether the smart tunnel is used. If you see something like https://172.16.16.23/+CSCOE+portal.html, the *+CSCO** indicates that the content is degraded by the ASA. When the smart tunnel is initiated, you see an **http get** command to a specific URL without the +CSCO* (such as GET 200 html http://mypage.example.com).

Examples

If you consider a case where Vendor V wants to provide Partner P with clientless access to their interal inventory server pages, Vendor V's administrator must decide the following:

- Will users have access to the inventory pages after they log into a clientless SSL VPN, whether or not they go through the clientless portal?
- Will the smart tunnel be a good choice for access because the page includes a Microsoft Silverlight component?
- Is a tunnel-all policy suitable because once the browser has been tunneled, all tunnel policy forces all browser traffic to go through Vendor V's ASA, leaving Partner P's users with no access to internal resources?

With the assumption that inventory pages are hosted at inv.example.com (10.0.0.0), the following example creates a tunnel policy that contains only one host:

```
hostname(config-webvpn)# smart-tunnel network inventory ip 10.0.0.0
hostname(config-webvpn)# smart-tunnel network inventory host inv.example.com
```

The following example applies a tunnel-specified tunnel policy to the partner's group policy:

```
hostname(config-group-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory
```

The following example specifies the group policy home page and enables a smart tunnel on it:

```
hostname(config-group-webvpn)# homepage value http://inv.example.com
hostname(config-group-webvpn)# homepage use-smart-tunnel
```

host (network object)

To configure a host for a network object, use the **host** command in object network configuration mode. To remove the host from the object, use the **no** form of this command.

host *ip_address*

no host *ip_address*

Syntax Description

ip_address	Identifies the host IP address for the object, either IPv4 or IPv6.

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
Object configuration	•	•	•	•	—

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

If you configure an existing network object with a different IP address, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a host network object:

```
hostname (config)# object network OBJECT1
hostname (config-network-object)# host 10.1.1.1
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.
fqdn	Specifies a fully qualified domain name network object.
nat	Enables NAT for the network object.
object network	Creates a network object.
object-group network	Creates a network object group.

Command	Description
range	Specifies a range of addresses for the network object.
show running-config object network	Shows the network object configuration.
subnet	Specifies a subnet network object.

host (parameters)

To specify a host to interact with using RADIUS accounting, use the **host** command in radius-accounting parameter configuration mode, which is accessed by using the **parameters** command in the policy-map type inspect radius-accounting submode. To disable the specified host, use the **no** form of this command.

host *address* [**key** *secret*]

no host *address* [**key** *secret*]

Syntax Description

host	Specifies a single endpoint sending the RADIUS accounting messages.
address	The IP address of the client or server sending the RADIUS accounting messages.
key	Optional keyword to specify the secret of the endpoint sending the gratuitous copy of the accounting messages.
secret	The shared secret key of the endpoint sending the accounting messages used to validate the messages. This can be up to 128 alphanumeric characters.

Defaults

The **no** option 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
Radius-accounting parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Multiple instances of this command are allowed.

Examples

The following example shows how to specify a host with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# host 209.165.202.128 key cisco123
```

Related Commands

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

hostname

To set the ASA hostname, use the **hostname** command in global configuration mode. To restore the default hostname, use the **no** form of this command.

hostname *name*

no hostname [*name*]

Syntax Description

name	Specifies a hostname up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.

Defaults

The default hostname depends on your platform.

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)	You can no longer use non-alphanumeric characters (other than a hyphen).

Usage Guidelines

The hostname appears as the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts.

The hostname that you optionally set within a context does not appear in the command line, but can be used for the **banner** command **$(hostname)** token.

Examples

The following example sets the hostname to firewall1:

```
hostname(config)# hostname firewall1
firewall1(config)#
```

Related Commands

Command	Description
banner	Sets a login, message of the day, or enable banner.
domain-name	Sets the default domain name.

hpm topn enable

To enable real-time reports in ASDM of the top hosts connecting through the ASA, use the **hpm topn enable** command in global configuration mode. To disable the hosts reporting, use the **no** form of this command.

hpm topn enable

no hpm topn enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

You might want to disable this command to maximize system performance. This command populates the ASDM Home > Firewall Dashboard > Top 200 Hosts pane.

Examples

The following example enables the top hosts reporting:

```
hostname(config)# hpm topn enable
```

Related Commands

Command	Description
clear configure hpm	Clears the HPM configuration.
show running-config hpm	Shows the HPM configuration.

hsi

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

hsi *ip_address*

no hsi *ip_address*

Syntax Description

ip_address	IP address of the host to add. A maximum of five HSIs per HSI group is allowed.

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
Hsi group configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

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

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

Related Commands

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

hsi-group

To define an HSI group for H.323 protocol inspection and to enter hsi group configuration mode, use the **hsi-group** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

hsi-group *group_id*

no hsi-group *group_id*

Syntax Description

group_id	HSI group ID number, from 0 to 2147483647.

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**
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

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

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

Related Commands

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

html-content-filter

To filter Java, ActiveX, images, scripts, and cookies for WebVPN sessions for this user or group policy, use the **html-content-filter** command in webvpn configuration mode. To remove a content filter, use the **no** form of this command.

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

Syntax Description

cookies	Removes cookies from images, providing limited ad filtering and privacy.
images	Removes references to images (removes <IMG> tags).
java	Removes references to Java and ActiveX (removes the <EMBED>, <APPLET>, and <OBJECT> tags.
none	Indicates that there is no filtering. Sets a null value, thereby disallowing filtering. Prevents inheriting filtering values.
scripts	Removes references to scripting (removes <SCRIPT> tags).

Defaults

No filtering occurs.

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
7.0(1)	This command was introduced.

Usage Guidelines

To remove all content filters, including a null value created by issuing the **html-content-filter none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting an HTML content filter, use the **html-content-filter none** command.

Using the command a second time overrides the previous setting.

Examples

The following example shows how to set filtering of Java and ActiveX, cookies, and images for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
```

Related Commands

Command	Description
webvpn	Lets you enter webvpn configuration mode to configure parameters that apply to group policies or usernames. Lets you enter global configuration mode to configure global settings for WebVPN.

http

To specify hosts that can access the HTTP server internal to the ASA, use the **http** command in global configuration mode. To remove one or more hosts, use the **no** form of this command. To remove the attribute from the configuration, use the **no** form of this command without arguments.

http *ip_address subnet_mask interface_name*

no http

Syntax Description

interface_name	Provides the name of the ASA interface through which the host can access the HTTP server.
ip_address	Provides the IP address of a host that can access the HTTP server.
subnet_mask	Provides the subnet mask of a host that can access the HTTP server.

Defaults

No hosts can access the HTTP server.

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 shows how to allow the host with the IP address of 10.10.99.1 and the subnet mask of 255.255.255.255 access to the HTTP server via the outside interface:

```
hostname(config)# http 10.10.99.1 255.255.255.255 outside
```

The next example shows how to allow any host access to the HTTP server via the outside interface:

```
hostname(config)# http 0.0.0.0 0.0.0.0 outside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.

Command	Description
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http authentication-certificate

To require a certficate for authentication with ASDM HTTPS connections, use the **http authentication-certificate** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all **http authentication-certificate** commands from the configuration, use the **no** version without arguments.

The ASA validates certificates against the PKI trust points. If a certificate does not pass validation, the ASA closes the SSL connection.

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

Syntax Description

interface	Specifies the interface on the ASA that requires certificate authentication.

Defaults

HTTP certificate 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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0.3	This command was deprecated in favor of the **ssl certificate-authentication** command.
8.2.1	This command was re-added; the global **ssl certificate-authentication** command was kept for backwards compatibility.
8.4.7, 9.1.3	Certificate-only authentication was enabled. Previously, this command only added certificate authentication to user authentication when you enabled the **aaa authentication http console** command.

Usage Guidelines

You configure certificate authentication for each interface, so that connections on a trusted/inside interface do not have to provide a certificate. You can use the command multiple times to enable certificate authentication on multiple interfaces.

Examples

The following example shows how to require certificate authentication for clients connecting to the interfaces named outside and external:

```
hostname(config)# http authentication-certificate inside
hostname(config)# http authentication-certificate external
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the ASA interface through which the host accesses the HTTP server.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.
ssl authentication-certificate	To require a certificate for SSL connections.

http[s] (parameters)

To specify the service type for the scansafe inspection policy map, use the **http**[**s**] command in parameters configuration mode. To remove the service type, use the **no** form of this command. You can access the parameters configuration mode by first entering the the **policy-map type inspect scansafe** command.

{**http** | **https**}

no {**http** | **https**}

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

You can only specify one service type for a scansafe inspection policy map, either **http** or **https**. There is no default; you must specify a type.

Examples

The following example creates an inspection policy map, and sets the service type to HTTP:

```
hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.

Command	Description
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

http-comp

To enable compression of HTTP data over a WebVPN connection for a specific group or user, use the **http-comp** command in the group-policy webvpn and username webvpn configuration modes. To remove the command from the configuration and have the value be inherited, use the **no** form of this command.

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

Syntax Description

gzip	Specifies compression is enabled for the group or user.
none	Specifies compression is disabled for the group or user.

Defaults

By default, compression is set to enabled.

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
7.1(1)	This command was introduced.

Usage Guidelines

For WebVPN connections, the **compression** command configured in global configuration mode overrides the **http-comp** command configured in group policy and username webvpn configuration modes.

Examples

The following example disables compression for the group-policy sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
```

Related Commands

Command	Description
compression	Enables compression for all SVC, WebVPN, and IPsec VPN connections.

http-proxy

To configure the ASA to use an external proxy server to handle HTTP requests, use the **http-proxy** command in webvpn configuration mode. To remove the HTTP proxy server from the configuration, use the **no** form of this command.

http-proxy {*host* [*port*] [**exclude** *url*] | **pac** *pacfile*} [**username** *username* {**password** *password*}]

no http-proxy

Syntax Description

host	Hostname or IP address for the external HTTP proxy server.
pac *pacfile*	Identifies the PAC file that contains a JavaScript function that specifies one or more proxies.
password	(Optional, and available only if you specify a username) Enter this keyword to accompany each HTTP proxy request with a password to provide basic, proxy authentication.
password	Password to send to the proxy server with each HTTP request.
port	(Optional) Port number used by the HTTP proxy server. The default port is 80, which is the port that the ASA uses if you do not supply a value. The range is 1-65535.
url	Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards: • * to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string. • **?** to match any single character, including slashes and periods. • [*x*-*y*] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set. • [**!***x*-*y*] to match any single character that is not in the range.
username	(Optional) Enter this keyword to accompany each HTTP proxy request with a username to provide basic, proxy authentication.
username	Username to send to the proxy server with each HTTP request.

Defaults

By default, no HTTP proxy server is configured.

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
7.0(1)	This command was introduced.
8.0(2)	Added the **exclude**, **username**, and **password** keywords.

Usage Guidelines

Requiring Internet access via a server that the organization controls provides another opportunity for filtering to assure secure Internet access and administrative control.

The ASA supports only one instance of the **http-proxy** command. If one instance of this command is already present in the running configuration and you enter another instance, the CLI overwrites the previous instance. The CLI lists any **http-proxy** commands in the running configuration if you enter the **show running-config webvpn** command. If the response does not list an **http -proxy** command, then none is present.

Note Proxy NTLM authentication is not supported in **http-proxy**. Only proxy without authentication and basic authentication are supported.

Examples

The following example shows how to configure use of an HTTP proxy server with an IP address of 209.165. 201.2 using the default port, 443:

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 209.165.201.2
hostname(config-webvpn)
```

The following example shows how to configure use of the same proxy server, and send a username and password with each HTTP request:

```
hostname(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

The following example shows the same command, except when the ASA receives the specific URL www.example.com in an HTTP request, it resolves the request instead of passing it on to the proxy server:

```
hostname(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)
```

The followiing example shows how to use the **exclude** option:

```
hostname(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
12345678
hostname(config-webvpn)
```

The followiing example shows how to use the **pac** option:

```
hostname(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

Related Commands

Command	Description
https-proxy	Configures the use of an external proxy server to handle HTTPS requests.
show running-config webvpn	Displays the running configuration for SSL VPN, including any HTTP and HTTPS proxy servers.

http-proxy (dap)

To enable or disable HTTP proxy port forwarding, use the **http-proxy** command in dap-webvpn configuration mode.To remove the attribute from the configuration, use the **no** form of this command.

http-proxy {**enable** | **disable** | **auto-start**}

no http-proxy

Syntax Description

auto-start	Enables and automatically starts HTTP proxy port forwarding for the DAP record.
enable/disable	Enables or disables HTTP proxy port forwarding for the DAP record.

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

The ASA can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the tunnel group
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or tunnel group.

When you enable or disable an attribute for a DAP record, the ASA applies that value and enforces it. For example, when you disable HTTP proxy in dap-webvpn configuration mode, the ASA looks no further for a value. When you instead use the **no** value for the **http-proxy** command, the attribute is not present in the DAP record, so the ASA moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable HTTP proxy port forwarding for the DAP record named Finance.

```
hostname (config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# http-proxy enable
hostname(config-dap-webvpn)#
```

Related Commands

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

http redirect

To specify that the ASA redirect HTTP connections to HTTPS, use the **http redirect** command in global configuration mode. To remove a specified **http redirect** command from the configuration, use the **no** form of this command. To remove all **http redirect** commands from the configuration, use the **no** form of this command without arguments.

http redirect *interface* [*port*]

no http redirect [*interface*]

Syntax Description

interface	Identifies the interface for which the ASA should redirect HTTP requests to HTTPS.
port	Identifies the port that the ASA listens on for HTTP requests, which it then redirects to HTTPS. By default, it listens on port 80,

Defaults

HTTP redirect 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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The interface requires an access list that permits HTTP. Otherwise the ASA does not listen to port 80, or to any other port that you configure for HTTP.

If the **http redirect** command fails, the following message appears:

```
"TCP port <port_number> on interface <interface_name> is in use by another feature. Please
choose a different port for the HTTP redirect service"
```

Use a different port for the HTTP redirect service.

Examples

The following example shows how to configure HTTP redirect for the inside interface, keeping the default port 80:

```
hostname(config)# http redirect inside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the ASA interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server enable

To enable the ASA HTTP server, use the **http server enable** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

http server enable [*port*]

Syntax Description

port	The port to use for HTTP connections. The range is 1-65535. The default port is 443.

Defaults

The HTTP server 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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to enable the HTTP server.

```
hostname(config)# http server enable
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the ASA interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server idle-timeout

To set an idle timeout for ASDM connections to the ASA, use the **http server idle-timeout** command in global configuration mode. To disable the timeout, use the **no** form of this command.

http server idle-timeout [*minutes*]

no http server idle-timeout [*minutes*]

Syntax Description

minutes	The idle timeout, from 1-1440 minutes.

Defaults

The default setting is 20 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
8.2(1)	This command was introduced.

Examples

The following example sets the idle timeout for ASDM sessions to 500 minutes:

```
hostname(config)# http server idle-timeout 500
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration, disables the HTTP server, and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask and the interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http server enable	Enables the HTTP server for ASDM sessions.
http server session-timeout	Limits the session time of ASDM sessions to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server session-timeout

To set a session timeout for ASDM connections to the ASA, use the **http server session-timeout** command in global configuration mode. To disable the timeout, use the **no** form of this command.

http server session-timeout [*minutes*]

no http server session-timeout [*minutes*]

Syntax Description

minutes	The session timeout, from 1-1440 minutes.

Defaults

The session timeout is disabled. ASDM connections have no session time limit.

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
8.2(1)	This command was introduced.

Examples

The following example sets a session timeout for ASDM connections to 1000 minutes:

```
hostname(config)# http server session-timeout 1000
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask and the interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the ASA.
http server enable	Enables the HTTP server for ASDM sessions.
http server idle-timeout	Limits the idle time of ASDM sessions to the ASA.
http redirect	Specifies that the ASA redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

https-proxy

To configure the ASA to use an external proxy server to handle HTTPS requests, use the **https-proxy** command in webvpn configuration mode. To remove the HTTPS proxy server from the configuration, use the **no** form of this command.

https-proxy {*host* [*port*] [**exclude** *url*] | [**username** *username* {**password** *password*}]

no https-proxy

Syntax Description

host	Hostname or IP address for the external HTTPS proxy server.
password	(Optional, and available only if you specify a username) Enter this keyword to accompany each HTTPS proxy request with a password to provide basic, proxy authentication.
password	Password to send to the proxy server with each HTTPS request.
port	(Optional) Port number used by the HTTPS proxy server. The default port is 443, which is the port the ASA uses if you do not supply a value. The range is 1-65535.
url	Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards: • ***** to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string. • **?** to match any single character, including slashes and periods. • [*x*-*y*] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set. • [**!***x*-*y*] to match any single character that is not in the range.
username	(Optional) Enter this keyword to accompany each HTTPS proxy request with a username to provide basic, proxy authentication.
username	Username to send to the proxy server with each HTTPS request.

Defaults

By default, no HTTPS proxy server is configured.

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
7.0(1)	This command was introduced.
8.0(2)	Added the **exclude**, **username**, and **password** keywords.

Usage Guidelines

Requiring Internet access via a server that the organization controls provides another opportunity for filtering to assure secure Internet access and administrative control.

The ASA supports only one instance of the **https-proxy** command. If one instance of this command is already present in the running configuration and you enter another instance, the CLI overwrites the previous instance. The CLI lists any **https-proxy** commands in the running configuration if you enter the **show running-config webvpn** command. If the response does not list an **https-proxy** command, then none is present.

Examples

The following example shows how to configure use of an HTTPS proxy server with an IP address of 209.165. 201.2 using the default port, 443:

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 209.165.201.2
hostname(config-webvpn)
```

The following example shows how to configure use of the same proxy server, and send a username and password with each HTTPS request:

```
hostname(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

The following example shows the same command, except that when the ASA receives the specific URL www.example.com in an HTTPS request, it resolves the request instead of passing it on to the proxy server:

```
hostname(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)
```

The followiing example shows how to use the **exclude** option:

```
hostname(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
hostname(config-webvpn)
```

The followiing example shows how to use the **pac** option:

```
hostname(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

Related Commands

Command	Description
http-proxy	Configures the use of an external proxy server to handle HTTP requests.
show running-config webvpn	Displays the running configuration for SSL VPN, including any HTTP and HTTPS proxy servers.

hw-module module allow-ip

For the AIP SSC on the ASA 5505, to set the hosts that are allowed to access the management IP address, use the **hw-module module allow-ip** command in privileged EXEC mode.

hw-module module 1 allow-ip *ip_address netmask*

Syntax Description

1	Specifies the slot number, which is always 1.
ip_ address	Specifies the host IP address(es).
netmask	Specifies the subnet mask.

Defaults

In the factory default configuration, the following hosts are allowed to manage the IPS module: 192.168.1.5 through 192.168.1.254.

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
8.2(1)	This command was introduced.

Usage Guidelines

This command is only valid when the SSC status is Up.

These settings are written to the IPS application configuration, not the ASA configuration. You can view these settings from the ASA using the **show module details** command.

You can alternatively use the IPS application **setup** command to configure this setting from the IPS CLI.

Examples

The following example shows how to configure host parameters on the SSC:

```
hostname# hw-module module 1 allow-ip 209.165.201.29 255.255.255.0
```

Related Commands

Command	Description
hw-module module ip	Configures the AIP SSC management address.
show module	Shows module status information.

hw-module module ip

For the AIP SSC on the ASA 5505, to configure the management IP address, use the **hw-module module ip** command in privileged EXEC mode.

hw-module module 1 ip *ip_address netmask gateway*

Syntax Description

1	Specifies the slot number, which is always 1.
gateway	Specifies the gateway IP address.
ip_address	Specifies the management IP address.
netmask	Specifies the subnet mask.

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
8.2(1)	This command was introduced.

Usage Guidelines

Make sure this address is on the same subnet as the ASA VLAN IP address. For example, if you assigned 10.1.1.1 to the VLAN for the ASA, then assign another address on that network, such as 10.1.1.2, for the IPS management address.

If the management station is on a directly connected ASA network, then set the gateway to be the ASA IP address assigned to the IPS management VLAN. In the example decribed, set the gateway to 10.1.1.1. If the management station is on a remote network, then set the gateway to be the address of an upstream router on the IPS management VLAN.

Note These settings are written to the IPS application configuration, not the ASA configuration. You can view these settings from the ASA using the **show module details** command.

You can alternatively use the IPS application **setup** command to configure this setting from the IPS CLI.

Examples

The following example shows how to configure a management address for the IPS module:

```
hostname# hw-module module 1 ip 209.165.200.254 255.255.255.224 209.165.200.225
```

Related Commands

Command	Description
hw-module module allow-ip	Configures the AIP SSC management host addresses.
show module	Shows module status information.

hw-module module password-reset

To reset the password for the default admin user on the hardware module to the default value, use the **hw-module module password-reset** command in privileged EXEC mode.

hw-module module 1 password-reset

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

The default username and password depends on your module:

- IPS module—username: **cisco**; password: **cisco**
- CSC module—username: **cisco**; password: **cisco**
- ASA CX module—username: **admin**; password: **Admin123**

Command Modes

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

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

Command History

Release	Modification
7.2(2)	This command was introduced.
8.4(4.1)	We added support for the ASA CX module.

Usage Guidelines

This command is only valid when the hardware module is in the Up state and supports password reset. For IPS, password reset is supported if the module is running IPS Version 6.0 or later. After resetting the password, you should change it to a unique value using the module application. Resetting the module password causes the module to reboot. Services are not available while the module is rebooting, which may take several minutes. You can run the **show module** command to monitor the module state.

The command always prompts for confirmation. If the command succeeds, no other output appears. If the command fails, an error message appears that explains why the failure occurred. The possible error messages are as follows:

```
Unable to reset the password on the module in slot 1

Unable to reset the password on the module in slot 1 - unknown module state

Unable to reset the password on the module in slot 1 - no module installed

Failed to reset the password on the module in slot 1 - module not in Up state

Unable to reset the password on the module in slot 1 - unknown module type

The module in slot 1 does not support password reset

Unable to reset the password on the module in slot 1 - no application found

The SSM application version does not support password reset

Failed to reset the password on the module in slot 1
```

Examples

The following example resets a password on a hardware module in slot 1:

```
hostname(config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

Related Commands

Command	Description
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the module software.
hw-module module reset	Shuts down and resets the module hardware.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module recover

To load a recovery software image from a TFTP server to an installed module, or to configure network settings to access the TFTP server, use the **hw-module module recover** command in privileged EXEC mode. You might need to recover a module using this command if, for example, the module is unable to load a local image.

hw-module module 1 recover {**boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *module_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*]}

Syntax Description

1	Specifies the slot number, which is always 1.
boot	Initiates recovery of this module and downloads a recovery image according to the **configure** keyword settings. The module then reboots from the new image.
configure	Configures the network parameters to download a recovery image. If you do not enter a network parameter after the **configure** keyword, you are prompted for all parameters. This command prompts you for the URL for the TFTP server, the management interface IP address and netmask, gateway address, and VLAN ID. These network parameters are configured in ROMMON; the network parameters you configured in the module application configuration are not available to ROMMON, so you must set them separately here.
gateway *gateway_ip_address*	(Optional) The gateway IP address for access to the TFTP server through the SSM management interface.
ip *module_address*	(Optional) The IP address of the module management interface.
stop	Stops the recovery action, and stops downloading the recovery image. The module boots from the original image. You must enter this command within 30 to 45 seconds after starting recovery using the **hw-module module recover boot** command. If you issue the **stop** command after this period, it might cause unexpected results, such as the module becoming unresponsive.
url *tfp_url*	(Optional) The URL for the image on a TFTP server, in the following format: **tftp://***server*/[*path*/]*filename*
vlan *vlan_id*	(Optional) Specifies the VLAN ID for the management interface.

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

If the module suffers a failure, and the module application image cannot run, you can reinstall a new image on the module from a TFTP server.

Note Do not use the **upgrade** command within the module software to install the image.

Be sure the TFTP server that you specify can transfer files up to 60 MB in size. This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

This command is only available when the module is in the Up, Down, Unresponsive, or Recovery state. See the **show module** command for state information.

You can view the recovery configuration using the **show module 1 recover** command.

Note This command is not supported on the ASA CX module.

Examples

The following example sets the module to download an image from a TFTP server:

```
hostname# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

The following example recovers the module:

```
hostname# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
hw-module module reset	Shuts down a module and performs a hardware reset.
hw-module module reload	Reloads the module software.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module reload

To reload module software for a physical module, use the **hw-module module reload** command in privileged EXEC mode.

hw-module module 1 reload

Syntax Description

1	Specifies the slot number, which is always 1.

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.
8.4(4.1)	We added support for the ASA CX module.

Usage Guidelines

This command differs from the **hw-module module reset** command, which also performs a hardware reset before reloading the module.

This command is only valid when the module status is Up. See the **show module** command for state information.

Examples

The following example reloads the module in slot 1:

```
hostname# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down a module and performs a hardware reset.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module reset

To reset the module hardware and then reload the module software, use the **hw-module module reset** command in privileged EXEC mode.

hw-module module 1 reset

Syntax Description

1	Specifies the slot number, which is always 1.

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.
8.4(4.1)	We added support for the ASA CX module.

Usage Guidelines

When the module is in an Up state, the **hw-module module reset** command prompts you to shut down the software before resetting.

You can recover a module (if supported) using the **hw-module module recover** command. If you enter the **hw-module module reset** command while the module is in a Recover state, the module does not interrupt the recovery process. The **hw-module module reset** command performs a hardware reset of the module, and the module recovery continues after the hardware reset. You might want to reset the module during recovery if the module hangs; a hardware reset might resolve the issue.

This command differs from the **hw-module module reload** command, which only reloads the software and does not perform a hardware reset.

This command is only valid when the module status is Up, Down, Unresponsive, or Recover. See the **show module** command for state information.

Examples

The following example resets an module in slot 1 that is in the Up state:

```
hostname# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
```

```
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the module software.
hw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

hw-module module shutdown

To shut down the module software, use the **hw-module module shutdown** command in privileged EXEC mode.

hw-module module 1 shutdown

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(4.1)	We added support for the ASA CX module.

Usage Guidelines

Shutting down the module software prepares the module to be safely powered off without losing configuration data.

This command is only valid when the module status is Up or Unresponsive. See the **show module** command for state information.

Examples

The following example shuts down a module in slot 1:

```
hostname# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
hostname#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
hw-module module recover	Recovers a module by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the module software.
hw-module module reset	Shuts down a module and performs a hardware reset.
show module	Shows module information.