



urgent-flag through zonelabs integrity ssl-client-authentication Commands

urgent-flag

To allow or clear the URG pointer through the TCP normalizer, use the **urgent-flag** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

urgent-flag { allow | clear }

no urgent-flag { allow | clear }

Syntax Description

allow	Allows the URG pointer through the TCP normalizer.
clear	Clears the URG pointer through the TCP normalizer.

Defaults

The urgent flag and urgent offset are clear by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **urgent-flag** command in tcp-map configuration mode to allow the urgent flag.

The URG flag is used to indicate that the packet contains information that is of higher priority than other data within the stream. The TCP RFC is vague about the exact interpretation of the URG flag, therefore, end systems handle urgent offsets in different ways, which may make the end system vulnerable to attacks. The default behavior is to clear the URG flag and offset.

Examples

The following example shows how to allow the urgent flag:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 513
hostname(config)# policy-map pmap
```

```
hostname(config-pmap)# class cmap  
hostname(config-pmap)# set connection advanced-options tmap  
hostname(config)# service-policy pmap global
```

Related Commands

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

uri-non-sip

To identify the non-SIP URIs present in the Alert-Info and Call-Info header fields, use the **uri-non-sip** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

uri-non-sip action {mask | log} [log]

no uri-non-sip action {mask | log} [log]

Syntax Description

mask	Masks the non-SIP URIs.
log	Specifies standalone or additional log in case of violation.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to identify the non-SIP URIs present in the Alert-Info and Call-Info header fields in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# uri-non-sip action log
```

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.

url

To maintain the list of static URLs for retrieving CRLs, use the **url** command in **crl configure** configuration mode. The **crl configure** configuration mode is accessible from the **crypto ca trustpoint** configuration mode. To delete an existing URL, use the **no** form of this command.

url *index url*

no url *index url*

Syntax Description

<i>index</i>	Specifies a value from 1 to 5 that determines the rank of each URL in the list. The security appliance tries the URL at index 1 first.
<i>url</i>	Specifies the URL from which to retrieve the CRL.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You cannot overwrite existing URLs. To replace an existing URL, first delete it using the **no** form of this command.

Examples

The following example enters **ca-crl** configuration mode, and sets up an index 3 for creating and maintaining a list of URLs for CRL retrieval and configures the URL **https://foobin.com** from which to retrieve CRLs:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://foobin.com
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
policy	Specifies the source for retrieving CRLs.

url-block

The **url-block** commands can be used to manage the URL buffers used for web server responses while waiting for a filtering decision from the filtering server. The **url-block** commands are also used to manage filtering of long URLs. To remove the configuration, use the **no** form of this command.

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

The numeric parameters for the **url-block** command are lower in multi-context mode than in single-context mode. For example:

Single-context:



url-block block *block_buffer_limit*—max is 128

url-block url-mempool *memory_pool_size*—max is 10240

Multi-context:

url-block block *block_buffer_limit*—max is 16

url-block url-mempool *memory_pool_size*—max is 512

Syntax Description		
block <i>block_buffer</i>		Creates an HTTP response buffer to store web server responses while waiting for a filtering decision from the filtering server. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks.
mempool-size <i>memory_pool_size</i>		Configures the maximum size of the URL buffer memory pool in Kilobytes (KB). The permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB.
		
	Note	This is not supported on the UDP transport servers.
url-size <i>long_url_size</i>		Configures the maximum allowed URL size in KB for each long URL being buffered. The permitted values, which specifies a maximum URL size, for Websense are 2, 3, or 4, representing 2 KB, 3 KB, or 4KB; or for Secure Computing, 2 or 3, representing 2 KB or 3 KB.
		
	Note	This is not supported on the UDP transport servers.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For Websense filtering servers, the **url-block url-size** command allows filtering of long URLs, up to 4 KB. For Secure Computing, the **url-block url-size** command allows filtering of long URLs, up to 3 KB. For both Websense and N2H2 filtering servers, the **url-block block** command causes the security appliance to buffer packets received from a web server in response to a web client request while waiting for a response from the URL filtering server. This improves performance for the web client compared to the default security appliance behavior, which is to drop the packets and to require the web server to retransmit the packets if the connection is permitted.

If you use the **url-block block** command and the filtering server permits the connection, the security appliance sends the blocks to the web client from the HTTP response buffer and removes the blocks from the buffer. If the filtering server denies the connection, the security appliance sends a deny message to the web client and removes the blocks from the HTTP response buffer.

Use the **url-block block** command to specify the number of blocks to use for buffering web server responses while waiting for a filtering decision from the filtering server.

Use the **url-block url-size** command with the **url-block mempool-size** command to specify the maximum length of a URL to be filtered and the maximum memory to assign to the URL buffer. Use these commands to pass URLs longer than 1159 bytes, up to a maximum of 4096 bytes, to the Websense or Secure-Computing server. The **url-block url-size** command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense or Secure-Computing server (through a TCP packet stream) so that the Websense or Secure-Computing server can grant or deny access to that URL.

Examples

The following example assigns 56 1550-byte blocks for buffering responses from the URL filtering server:

```
hostname#(config)# url-block block 56
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.

url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

url-cache

To enable URL caching for URL responses received from a Websense server and to set the size of the cache, use the **url-cache** command in global configuration mode. To remove the configuration, use the **no** form of this command.

url-cache {**dst** | **src_dst**} *kbytes* [**kb**]

no url-cache {**dst** | **src_dst**} *kbytes* [**kb**]

Syntax Description

dst	Cache entries based on the URL destination address. Select this mode if all users share the same URL filtering policy on the Websense server.
size <i>kbytes</i>	Specifies a value for the cache size within the range 1 to 128 KB.
src_dst	Cache entries based on the both the source address initiating the URL request as well as the URL destination address. Select this mode if users do not share the same URL filtering policy on the Websense server.
statistics	Use the statistics option to display additional URL cache statistics, including the number of cache lookups and hit rate.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **url-cache** command provides a configuration option to cache responses from the URL server.

Use the **url-cache** command to enable URL caching, set the size of the cache, and display cache statistics.

Caching stores URL access privileges in memory on the security appliance. When a host requests a connection, the security appliance first looks in the URL cache for matching access privileges instead of forwarding the request to the Websense server. Disable caching with the **no url-cache** command.



Note

If you change settings on the Websense server, disable the cache with the **no url-cache** command and then re-enable the cache with the **url-cache** command.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enable **url-cache** to increase throughput. Accounting logs are updated for Websense protocol Version 4 URL filtering while using the **url-cache** command.

Examples

The following example caches all outbound HTTP connections based on the source and destination addresses:

```
hostname(config)# url-cache src_dst 128
```

Related Commands

Commands	Description
clear url-cache statistics	Removes url-cache command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for URL responses received from a Websense filtering server.
url-server	Identifies a Websense server for use with the filter command.

url-list

To configure a set of URLs for WebVPN users to access, use the **url-list** command in global configuration mode. To configure a list with multiple URLs, use this command with the same listname multiple times, once for each URL. To remove an entire configured list, use the **no url-list listname** command. To remove a configured URL, use the **no url-list listname url** command.

To configure multiple lists, use this command multiple times, assigning a unique *listname* to each list.

url-list {*listname displayname url*}

no url-list *listname*

no url-list *listname url*

Syntax Description

<i>displayname</i>	Provides the text that displays on the WebVPN end user interface to identify the URL. Maximum 64 characters. The <i>displayname</i> must be unique for a given list. Spaces are allowed.
<i>listname</i>	Groups the set of URLs that WebVPN users can access. Maximum 64 characters. Maximum 64 characters. Semi-colons (;) ampersands (&), and less-than (<) characters are not allowed.
<i>url</i>	Specifies the link. Supported URL types are http, https and cifs.

Defaults

There is no default URL list.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You use the url-list command in global configuration mode to create one or more lists of URLs. To allow access to the URLs in a list for a specific group policy or user, use the *listname* you create here with the **url-list** command in webvpn mode.

Examples

The following example shows how to create a URL list called *Marketing URLs* that provides access to www.cisco.com, www.example.com, and www.example.org. The following table provides values that the example uses for each application.

listname	displayname	url
Marketing URLs	Cisco Systems	http://www.cisco.com
Marketing URLs	Example Company, Inc.	http://www.example.com
Marketing URLs	Example Organization	http://www.example.org

```
hostname(config)# url-list Marketing URLs Cisco Systems http://www.cisco.com
hostname(config)# url-list Marketing URLs Example Company, Inc. http://www.example.com
hostname(config)# url-list Marketing URLs Example Organization http://www.example.org
```

Related Commands

Command	Description
clear configuration url-list	Removes all url-list commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
url-list	Use this command in webvpn mode to permit a group policy or user to access a previously configured list of urls.
show running-configuration url-list	Displays the current set of configured urls.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

url-list (webvpn)

To apply a list of WebVPN servers and URLs to a particular user or group policy, use the **url-list** command in group-policy webvpn configuration mode or in username webvpn configuration mode. To remove a list, including a null value created by using the **url-list none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a url list, use the **url-list none** command. Using the command a second time overrides the previous setting.

url-list { *value name* | **none** } [*index*]

no url-list

Syntax Description

<i>index</i>	Indicates the display priority on the home page.
none	Sets a null value for url lists. Prevents inheriting a list from a default or specified group policy.
value name	Specifies the name of a previously configured list of urls. To configure such a list, use the url-list command in global configuration mode.

Defaults

There is no default URL list.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using the command a second time overrides the previous setting.

Before you can use the **url-list** command in webvpn mode to identify a URL list that you want to display on the WebVPN home page for a user or group policy, you must create the list. Use the **url-list** command in global configuration mode to create one or more lists.

Examples

The following example applies a URL list called FirstGroupURLs for the group policy named FirstGroup and assigns it first place among the URL lists:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
```

Related Commands	Command	Description
	clear configure url-list <i>[listname]</i>	Removes all url-list commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
	show running-configuration url-list	Displays the current set of configured url-list commands.
	url-list	Use this command in webvpn mode, which you access in global configuration mode, to configure the set of URLs that WebVPN users can access.
	webvpn	Lets you enter webvpn mode. This can be webvpn configuration mode, group-policy webvpn configuration mode (to configure webvpn settings for a specific group policy), or username webvpn configuration mode (to configure webvpn settings for a specific user).

url-server

To identify an N2H2 or Websense server for use with the **filter** command, use the **url-server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

N2H2

```
url-server [<(if_name)>] vendor {smartfilter | n2h2} host <local_ip> [port <number>] [timeout <seconds>] [protocol {TCP [connections <number>]} | UDP]
```

```
no url-server [<(if_name)>] vendor {smartfilter | n2h2} host <local_ip> [port <number>] [timeout <seconds>] [protocol {TCP [connections <number>]} | UDP]
```

Websense

```
url-server (if_name) vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP | connections num_conns} | version]
```

```
no url-server (if_name) vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP | connections num_conns} | version]
```

Syntax Description

N2H2

connections	Limits the maximum number of TCP connections permitted.
<i>num_conns</i>	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host <i>local_ip</i>	The server that runs the URL filtering application.
<i>if_name</i>	(Optional) The network interface where the authentication server resides. If not specified, the default is inside.
port <i>number</i>	The N2H2 server port. The security appliance also listens for UDP replies on this port. The default port number is 4005.
protocol	The protocol can be configured using TCP or UDP keywords. The default is TCP.
timeout <i>seconds</i>	The maximum idle time permitted before the security appliance switches to the next server you specified. The default is 30 seconds.
vendor	Indicates URL filtering service, using either ‘smartfilter’ or ‘n2h2’ (for backward compatibility); however, ‘smartfilter’ is saved as the vendor string.

Websense

connections	Limits the maximum number of TCP connections permitted.
<i>num_conns</i>	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host <i>local_ip</i>	The server that runs the URL filtering application.
<i>if_name</i>	The network interface where the authentication server resides. If not specified, the default is inside.

timeout <i>seconds</i>	The maximum idle time permitted before the security appliance switches to the next server you specified. The default is 30 seconds.
protocol	The protocol can be configured using TCP or UDP keywords. The default is TCP protocol, Version 1.
vendor websense	Indicates URL filtering service vendor is Websense.
version	Specifies protocol Version 1 or 4 . The default is TCP protocol Version 1. TCP can be configured using Version 1 or Version 4. UDP can be configured using Version 4 only.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **url-server** command designates the server running the N2H2 or Websense URL filtering application. The limit is 16 URL servers in single context mode and 4 URL servers in multi mode; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the security appliance does not update the configuration on the application server; this must be done separately, according to the vendor instructions.

The **url-server** command must be configured before issuing the **filter** command for HTTPS and FTP. If all URL servers are removed from the server list, then all **filter** commands related to URL filtering are also removed.

Once you designate the server, enable the URL filtering service with the **filter url** command.

Use the **show url-server statistics** command to view server statistic information including unreachable servers.

Follow these steps to filter URLs:

- Step 1** Designate the URL filtering application server with the appropriate form of the vendor-specific **url-server** command.
- Step 2** Enable URL filtering with the **filter** command.
- Step 3** (Optional) Use the **url-cache** command to enable URL caching to improve perceived response time.
- Step 4** (Optional) Enable long URL and HTTP buffering support using the **url-block** command.

- Step 5** Use the **show url-block block statistics**, **show url-cache statistics**, or the **show url-server statistics** commands to view run information.

For more information about Filtering by N2H2, visit N2H2's website at:

<http://www.n2h2.com>

For more information on Websense filtering services, visit the following website:

<http://www.websense.com/>

Examples

Using N2H2, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Using Websense, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for URL responses received from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.

user-authentication

To enable user authentication, use the **user-authentication enable** command in group-policy configuration mode. To disable user authentication, use the **user-authentication disable** command. To remove the user authentication attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for user authentication from another group policy.

When enabled, user authentication requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel.

user-authentication {enable | disable}

no user-authentication

Syntax Description

disable	Disables user authentication.
enable	Enables user authentication.

Defaults

User authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Individual users authenticate according to the order of authentication servers that you configure. If you require user authentication on the primary security appliance, be sure to configure it on any backup servers as well.

Examples

The following example shows how to enable user authentication for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
secure-unit-authentication	Provides additional security by requiring the VPN client to authenticate with a username and password each time the client initiates a tunnel.
user-authentication-idle-timeout	Sets an idle timeout for individual users. If there is no communication activity on a user connection in the idle timeout period, the security appliance terminates the connection.

user-authentication-idle-timeout

To set an idle timeout for individual users behind hardware clients, use the **user-authentication-idle-timeout** command in group-policy configuration mode. To delete the idle timeout value, use the **no** form of this command. This option allows inheritance of an idle timeout value from another group policy. To prevent inheriting an idle timeout value, use the **user-authentication-idle-timeout none** command.

If there is no communication activity by a user behind a hardware client in the idle timeout period, the security appliance terminates the connection.

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

Syntax Description

minutes	Specifies the number of minutes in the idle timeout period. The range is from 1 through 35791394 minutes
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting an user authentication idle timeout value from a default or specified group policy.

Defaults

30 minutes.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The minimum is 1 minute, the default is 30 minutes, and the maximum is 10,080 minutes.

Examples

The following example shows how to set an idle timeout value of 45 minutes for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

Related Commands

Command	Description
user-authentication	Requires users behind hardware clients to identify themselves to the security appliance before connecting.

username

To add a user to the security appliance database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username you want to remove. To remove all usernames, use the **no** version of this command without appending a username.

```
username name {nopassword | password password [mschap | encrypted | nt-encrypted] }
                [privilege priv_level]
```

```
no username name
```

Syntax Description

encrypted	Indicates that the password is encrypted (if you did not specify mschap). When you define a password in the username command, the security appliance encrypts it when it saves it to the configuration for security purposes. When you enter the show running-config command, the username command does not show the actual password; it shows the encrypted password followed by the encrypted keyword. For example, if you enter the password “test,” the show running-config command output would appear to be something like the following: username pat password rvEdRh0xPC8be17s encrypted The only time you would actually enter the encrypted keyword at the CLI is if you are cutting and pasting a configuration to another security appliance and you are using the same password.
mschap	Specifies that the password will be converted to unicode and hashed using MD4 after you enter it. Use this keyword if users are authenticated using MSCHAPv1 or MSCHAPv2.
<i>name</i>	Specifies the name of the user as a string from 4 to 64 characters in length.
nopassword	Indicates that this user needs no password.
nt-encrypted	Indicates that the password is encrypted for use with MSCHAPv1 or MSCHAPv2. If you specified the mschap keyword when you added the user, then this keyword is displayed instead of the encrypted keyword when you view the configuration using the show running-config command. When you define a password in the username command, the security appliance encrypts it when it saves it to the configuration for security purposes. When you enter the show running-config command, the username command does not show the actual password; it shows the encrypted password followed by the nt-encrypted keyword. For example, if you enter the password “test,” the show running-config display would appear to be something like the following: username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted The only time you would actually enter the nt-encrypted keyword at the CLI is if you are cutting and pasting a configuration to another security appliance and you are using the same password.
password <i>password</i>	Sets the password as a string from 3 to 32 characters in length.
privilege <i>priv_level</i>	Sets a privilege level for this use from 0 to 15 (lowest to highest). The default privilege level is 2. This privilege level is used with command authorization.

Defaults

The default privilege level is 2.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	The mschap and nt-encrypted keywords were added.

Usage Guidelines

The **login** command uses this database for authentication.

If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged mode, you should enable command authorization. (See the **aaa authorization command** command.) Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use AAA authentication so the user will not be able to use the **login** command, or you can set all local users to level 1 so you can control who can use the **enable** password to access privileged EXEC mode.

By default, VPN users that you add with this command have no attributes or group policy association. You must configure all values explicitly using the **username attributes** command.

Examples

The following example shows how to configure a user named “anyuser” with a password of 12345678 and a privilege level of 12:

```
hostname(config)# username anyuser password 12345678 privilege 12
```

Related Commands

Command	Description
aaa authorization command	Configures command authorization.
clear config username	Clears the configuration for a particular user or for all users.
show running-config username	Displays the running configuration for a particular user or for all users.
username attributes	Enters username attributes mode, which lets you configure attributes for specific users.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

username attributes

To enter the username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure Attribute-Value Pairs for a specified user.

username {*name*} **attributes**

no username [*name*] **attributes**

Syntax Description

name Provides the name of the user.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Username	•	—	•	—	—

Command History

Release	Modification
7.0.1	This command was introduced.

Usage Guidelines

The internal user authentication database consists of the users entered with the username command. The login command uses this database for authentication. You can configure the username attributes using either the **username** command or the **username attributes** command.

The syntax of the commands in config-username mode have the following characteristics in common:

- The **no** form removes the attribute from the running configuration.
- The **none** keyword also removes the attribute from the running configuration. But it does so by setting the attribute to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

The **username attributes** command enters config-username mode, in which you can configure any of the following attributes:

Attribute	Function
group-lock	Name an existing tunnel-group with which the user is required to connect.
password-storage	Enables/disables storage of the login password on the client system.
vpn-access-hours	Specifies the name of a configured time-range policy.
vpn-filter	Specifies the name of a user-specific ACL.
vpn-framed-ip-address	Specifies the IP address and the net mask to be assigned to the client.
vpn-group-policy	Specifies the name of a group-policy from which to inherit attributes.
vpn-idle-timeout	Specifies the idle timeout period in minutes, or none to disable.
vpn-session-timeout	Specifies the maximum user connection time in minutes, or none for unlimited time.
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed.
vpn-tunnel-protocol	Specifies permitted tunneling protocols.
webvpn	Enters webvpn mode, in which you configure webvpn attributes.

You configure webvpn-mode attributes for the username by entering the **username attributes** command and then entering the **webvpn** command in username webvpn 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 username attributes configuration mode for a user named “anyuser”:

```
hostname(config)# username anyuser attributes
hostname(config-username)#
```

Related Commands

Command	Description
clear config username	Clears the username database.
show running-config username	Displays the running configuration for a particular user or for all users.
username	Adds a user to the security appliance database.
webvpn	Enters username webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

username-prompt

To customize the username prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **username-prompt** command from webvpn customization mode:

username-prompt {text | style} value

[no] **username-prompt** {text | style} value

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default is text of the username prompt is “USERNAME:”.

The default style of the username 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:

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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 Username:”, and the default style is changed with the font weight increased to bolder:

```
F1-asal(config)# webvpn
F1-asal(config-webvpn)# customization cisco
F1-asal(config-webvpn-custom)# username-prompt text Corporate Username:
F1-asal(config-webvpn-custom)# username-prompt style font-weight:bolder
```

Related Commands

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

user-parameter

To specify the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication, use the **user-parameter** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command.

user-parameter *name*



Note

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

Syntax Description

<i>string</i>	The name of the username parameter included in the HTTP POST request. The maximum name size is 128 characters.
---------------	--

Defaults

There is no default value or behavior.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an SSO server. The required command **user-parameter** specifies that the HTTP POST request must include a username parameter for SSO authentication.



Note

At login, the user enters the actual name value which is entered into the HTTP POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies that the username parameter userid be included in the HTTP POST request used for SSO authentication:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

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

validate-attribute

To validate RADIUS attributes when using RADIUS accounting, use the **validate attribute** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

This option is disabled by default.

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

Syntax Description

<i>attribute_number</i>	The RADIUS attribute to be validated with RADIUS accounting. Values range from 1-191. Vendor Specific Attributes are not supported.
-------------------------	---

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		
	Routed	Transparent	Single	Multiple	
				Context	System
radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When this command is configured, the security appliance will also do a match on these attributes in addition to the Framed IP attribute. Multiple instances of this command are allowed.

You can find a list of RADIUS attribute types at the Internet Assigned Numbers Authority website <http://www.iana.org/assignments/radius-types>

Examples

The following example shows how to enable RADIUS accounting for the user name RADIUS attribute:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# validate attribute 1
```

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

verify

To verify the checksum of a file, use the **verify** command in privileged EXEC mode.

verify *path*

verify /md5 *path* [*md5-value*]

Syntax Description	
/md5	(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
<i>md5-value</i>	(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system will calculate the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.
<i>path</i>	<ul style="list-style-type: none"> • disk0:/[path]/filename This option is only available for the ASA 5500 series adaptive security appliance, and indicates the internal Flash memory. You can also use flash instead of disk0; they are aliased. • disk1:/[path]/filename This option is only available for the ASA 5500 series adaptive security appliance, and indicates the external Flash memory card. • flash:/[path]/filename This option indicates the internal Flash card. For the ASA 5500 series adaptive security appliance, flash is an alias for disk0. • ftp://[user[:password]@]server[:port]/[path]/filename[;type=xx] The type can be one of the following keywords: <ul style="list-style-type: none"> – ap—ASCII passive mode – an—ASCII normal mode – ip—(Default) Binary passive mode – in—Binary normal mode • http[s]://[user[:password]@]server[:port]/[path]/filename • tftp://[user[:password]@]server[:port]/[path]/filename[;int=interface_name] Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the tftp-server command instead of in the verify command.

Defaults

The current flash device is the default file system.

**Note**

When you specify the **/md5** option, you can use a network file, such as ftp, http and tftp as the source. The **verify** command without the **/md5** option only lets you verify local images in Flash.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into Flash memory or onto a server. A variety of image information is available on Cisco.com.

To display the contents of Flash memory, use the **show flash** command. The Flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, use the **verify** command. Note, however, that the **verify** command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the security appliance and saved in the file system without detection. If a corrupt image is transferred successfully to the security appliance, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of the security appliance software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all security appliance software images for comparison against local system image values.

To perform the MD5 integrity check, issue the **verify** command using the **/md5** keyword. For example, issuing the **verify /md5 flash:cdisk.bin** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Examples

The following example shows the verify command used on an image file called cdisk.bin. Some of the text was removed for clarity:

```
hostname# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
hostname#
```

Related Commands

Command	Description
copy	Copies files.
dir	Lists the files in the system.

version

To specify the version of RIP used globally by the security appliance, use the **version** command in router configuration mode. To restore the defaults, use the **no** form of this command.

version {1 | 2}

no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The security appliance accepts Version 1 and Version 2 packets but sends only Version 1 packets.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip send version** and **rip receive version** commands on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the security appliance to send and receive RIP Version 2 packets on all interfaces:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.

virtual http

To configure a virtual HTTP server, use the **virtual http** command in global configuration mode. To disable the virtual server, use the **no** form of this command.

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

Syntax Description

<i>ip_address</i>	Sets the IP address for the virtual HTTP server on the security appliance. Make sure this address is an unused address that is routed to the security appliance.
warning	(Optional) Notifies users that the HTTP connection needs to be redirected to the security appliance. This keyword applies only for text-based browsers, where the redirect cannot happen automatically.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was deprecated because the inline basic HTTP authentication method used in prior releases was replaced by the redirection method; this command was no longer needed.
7.2(2)	This command was revived because you can now choose between using basic HTTP authentication (the default) or using HTTP redirection using the aaa authentication listener command. The redirection method does not require an extra command for cascading HTTP authentications.

Usage Guidelines

When you use HTTP authentication on the security appliance (see the **aaa authentication match** or the **aaa authentication include** command), the security appliance uses basic HTTP authentication by default. You can change the authentication method so that the security appliance redirects HTTP connections to web pages generated by the security appliance itself using the **aaa authentication listener** command with the **redirect** keyword.

However, if you continue to use basic HTTP authentication, then you might need the **virtual http** command when you have cascading HTTP authentications.

If the destination HTTP server requires authentication in addition to the security appliance, then the **virtual http** command lets you authenticate separately with the security appliance (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This command redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the security appliance. The security appliance prompts for the AAA server username and password. After the AAA server authenticates the user, the security appliance redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.

For inbound users (from lower security to higher security), you must also include the virtual HTTP address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual HTTP IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual HTTP address. A **static** statement is not required.

**Note**

Do not set the **timeout uauth** command duration to 0 seconds when using the **virtual http** command, because this setting prevents HTTP connections to the real web server.

Examples

The following example shows how to enable virtual HTTP along with AAA authentication:

```
hostname(config)# virtual http 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list ACL-IN remark This is the HTTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list ACL-IN remark This is the virtual HTTP address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list AUTH remark This is the HTTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list AUTH remark This is the virtual HTTP address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
aaa authentication listener http	Sets the method by which the security appliance authenticates.
clear configure virtual	Removes virtual command statements from the configuration.
show running-config virtual	Displays the IP address of the security appliance virtual server.

sysopt uauth allow-http-cache	When you enable the virtual http command, this command lets you use the username and password in the browser cache to reconnect to the virtual server.
virtual telnet	Provides a virtual Telnet server on the security appliance to let users authenticate with the security appliance before initiating other types of connections that require authentication.

virtual telnet

To configure a virtual Telnet server on the security appliance, use the **virtual telnet** command in global configuration mode. You might need to authenticate users with the virtual Telnet server if you require authentication for other types of traffic for which the security appliance does not supply an authentication prompt. To disable the server, use the **no** form of this command.

virtual telnet *ip_address*

no virtual telnet *ip_address*

Syntax Description

ip_address Sets the IP address for the virtual Telnet server on the security appliance. Make sure this address is an unused address that is routed to the security appliance.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the security appliance, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

You must configure authentication for Telnet access to the virtual Telnet address as well as the other services you want to authenticate using the **authentication match** or **aaa authentication include** command.

When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message “Authentication Successful.” Then, the user can successfully access other services that require authentication.

For inbound users (from lower security to higher security), you must also include the virtual Telnet address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual Telnet IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual Telnet address. A **static** statement is not required.

To logout from the security appliance, reconnect to the virtual Telnet IP address; you are prompted to log out.

Examples

This example shows how to enable virtual Telnet along with AAA authentication for other services:

```
hostname(config)# virtual telnet 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list ACL-IN remark This is the SMTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
hostname(config)# access-list ACL-IN remark This is the virtual Telnet address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list AUTH remark This is the SMTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
hostname(config)# access-list AUTH remark This is the virtual Telnet address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
clear configure virtual	Removes virtual command statements from the configuration.
show running-config virtual	Displays the IP address of the security appliance virtual server.
virtual http	When you use HTTP authentication on the security appliance, and the HTTP server also requires authentication, this command allows you to authenticate separately with the security appliance and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.

vlan

To assign a VLAN ID to a subinterface, use the **vlan** command in interface configuration mode. To remove a VLAN ID, use the **no** form of this command. Subinterfaces require a VLAN ID to pass traffic. VLAN subinterfaces let you configure multiple logical interfaces on a single physical interface. VLANs let you keep traffic separate on a given physical interface, for example, for multiple security contexts.

vlan *id*

no vlan

Syntax Description

<i>id</i>	Specifies an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.
-----------	---

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the interface command to an interface configuration mode command.

Usage Guidelines

You can only assign a single VLAN to a subinterface, and not to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the security appliance changes the old ID.

You need to enable the physical interface with the **no shutdown** command to let subinterfaces be enabled. If you enable subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Therefore, you cannot prevent traffic from passing through the physical interface by bringing down the interface. Instead, ensure that the physical interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical interface pass untagged packets, you can configure the **nameif** command as usual.

The maximum number of subinterfaces varies depending on your platform. See the *Cisco Security Appliance Command Line Configuration Guide* for the maximum subinterfaces per platform.

Examples

The following example assigns VLAN 101 to a subinterface:

```
hostname(config)# interface gigabitethernet0/0.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example changes the VLAN to 102:

```
hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
    vlan 101
    nameif dmz1
    security-level 50
    ip address 10.1.2.1 255.255.255.0

hostname(config)# interface gigabitethernet0/0.1
hostname(config-interface)# vlan 102

hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
    vlan 102
    nameif dmz1
    security-level 50
    ip address 10.1.2.1 255.255.255.0
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the current configuration of the interface.

vpdn group

To create or edit a vpdn group and configure PPPoE client settings, use the **vpdn group** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

```
vpdn group group_name {localname username | request dialout pppoe | ppp authentication
{chap | mschap | pap}}
```

```
no vpdn group group_name {localname name | request dialout pppoe | ppp authentication
{chap | mschap | pap}}
```



Note

PPPoE is not supported when failover is configured on the security appliance, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

vpdn group <i>group_name</i>	Specifies a name for the vpdn group
localname <i>username</i>	Links the user name to the vpdn group for authentication, and must match the name configured with the vpdn username command.
request dialout pppoe	Specifies to allow dialout PPPoE requests.
ppp authentication { chap mschap pap }}	Specifies the Point-to-Point Protocol (PPP) authentication protocol. The Windows client dial-up networking settings lets you specify what authentication protocol to use (PAP, CHAP, or MS-CHAP). Whatever you specify on the client must match the setting you use on the security appliance. Password Authentication Protocol (PAP) lets PPP peers authenticate each other. PAP passes the host name or username in clear text. Challenge Handshake Authentication Protocol (CHAP) lets PPP peers prevent unauthorized access through interaction with an access server. MS-CHAP is a Microsoft derivation of CHAP. PIX Firewall supports MS-CHAP Version 1 only (not Version 2.0). If an authentication protocol is not specified on the host, do not specify the ppp authentication option in your configuration.

Defaults

default behavior or values. See Usage Guidelines.

Command Modes

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

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

Command History

Release	Modification
7.2.1	This command was introduced.

Usage Guidelines

Virtual Private Dial-up Networking (VPDN) is used to provide long distance, point-to-point connections between remote dial-in users and a private network. VPDN on the security appliance uses the Layer 2 tunnelling technology PPPoE to establish dial-up networking connections from the remote user to the private network across a public network.

PPPoE is the Point-to-Point Protocol (PPP) over Ethernet. PPP is designed to work with network layer protocols such as IP, IPX, and ARA. PPP also has CHAP and PAP as built-in security mechanisms.

The **show vpdn session pppoe** command displays session information for PPPoE connections. The **clear configure vpdn group** command removes all **vpdn group** commands from the configuration and stops all the active L2TP and PPPoE tunnels. The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Because PPPoE encapsulates PPP, PPPoE relies on PPP to perform authentication and ECP and CCP functions for client sessions operating within the VPN tunnel. Additionally, PPPoE is not supported in conjunction with DHCP because PPP assigns the IP address for PPPoE.

**Note**

Unless the VPDN group for PPPoE is configured, PPPoE cannot establish a connection.

To define a VPDN group to be used for PPPoE, use the **vpdn group group_name request dialout pppoe** command. Then use the **pppoe client vpdn group** command from interface configuration mode to associate a VPDN group with a PPPoE client on a particular interface.

If your ISP requires authentication, use the **vpdn group group_name ppp authentication {chap | mschap | pap}** command to select the authentication protocol used by your ISP.

Use the **vpdn group group_name localname username** command to associate the username assigned by your ISP with the VPDN group.

Use the **vpdn username username password password** command to create a username and password pair for the PPPoE connection. The username must be a username that is already associated with the VPDN group specified for PPPoE.

**Note**

If your ISP is using CHAP or MS-CHAP, the username may be called the remote system name and the password may be called the CHAP secret.

The PPPoE client functionality is turned off by default, so after VPDN configuration, enable PPPoE with the **ip address if_name pppoe [setroute]** command. The **setroute** option causes a default route to be created if no default route exists.

As soon as PPPoE is configured, the security appliance attempts to find a PPPoE access concentrator with which to communicate. When a PPPoE connection is terminated, either normally or abnormally, the security appliance attempts to find a new access concentrator with which to communicate.

The following **ip address** commands should not be used after a PPPoE session is initiated because they will terminate the PPPoE session:

- **ip address outside pppoe**, because it attempts to initiate a new PPPoE session.
- **ip address outside dhcp**, because it disables the interface until the interface gets its DHCP configuration.

- **ip address outside** *address netmask*, because it brings up the interface as a normally initialized interface.

Examples

The following example creates a vdpn group *telecommuters* and configures the PPPoE client:

```
F1(config)# vpdn group telecommuters request dialout pppoe
F1(config)# vpdn group telecommuters localname user1
F1(config)# vpdn group telecommuters ppp authentication pap
F1(config)# vpdn username user1 password test1
F1(config)# interface GigabitEthernet 0/1
F1(config-subif)# ip address pppoe setroute
```

Related Commands

Command	Description
clear configure vpdn group	Removes all vpdn group commands from the configurations.
clear configure vpdn username	Removes all vpdn username commands from the configuration.
show vpdn group <i>group_name</i>	Displays the vpdn group configuration.
vpdn username	Creates a username and password pair for the PPPoE connection.

vpdn username

To create a username and password pair for PPPoE connections, use the **vpdn username** command in global configuration mode.

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]



Note

PPPoE is not supported when failover is configured on the security appliance, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

<i>username</i>	Specifies the username.
<i>password</i>	Specifies the password.
store-local	Stores the username and password in a special location of NVRAM on the security appliance. If an Auto Update Server sends a clear config command to the security appliance and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

Defaults

No default behavior or values. See Usage Guidelines.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **vpdn username** must be a username that is already associated with the VPDN group specified with the **vpdn group** *group_name* **localname** *username* command.

The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Examples

The following example creates the vpdn username *bob_smith* with the password *telecommuter9/8*:

```
F1(config)# vpdn username bob_smith password telecommuter9/8
```


Related Commands	Command	Description
	clear configure vpdn group	Removes all vpdn group commands from the configurations.
	clear configure vpdn username	Removes all vpdn username commands from the configuration.
	show vpdn group	Displays the vpdn group configuration.
	vpdn group	Create a vpdn group and configures PPPoE client settings,

vpn-access-hours

To associate a group policy with a configured time-range policy, use the **vpn-access-hours** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-range value from another group policy. To prevent inheriting a value, use the **vpn-access-hours none** command.

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

Syntax Description

none	Sets VPN access hours to a null value, thereby allowing no time-range policy. Prevents inheriting a value from a default or specified group policy.
<i>time-range</i>	Specifies the name of a configured time-range policy.

Defaults

Unrestricted.

Command Modes

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

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

Command History

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

Usage Guidelines

Examples

The following example shows how to associate the group policy named FirstGroup with a time-range policy called 824:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours 824
```

Related Commands

Command	Description
time-range	Sets days of the week and hours of the day for access to the network, including start and end dates.

vpn-addr-assign

To specify a method for assigning IP addresses to remote access clients, use the **vpn-addr-assign** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all configured Vpn address assignment methods from the security appliance, use the **no** version of this command. without arguments.

vpn-addr-assign {aaa | dhcp | local}

no vpn-addr-assign [aaa | dhcp | local]

Syntax Description

aaa	Obtains IP addresses from an external AAA authentication server.
dhcp	Obtains IP addresses via DHCP.
local	Assigns IP addresses from internal authentication server, and associates them with a tunnel group.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

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

Usage Guidelines

If you choose DHCP, you must also use the **dhcp-network-scope** command to define the range of IP addresses that the DHCP server can use.

If you choose local, you must also use the **ip local pool** command to define the range of IP addresses to use. You then use the **vpn-framed-ip-address** and **vpn-framed-netmask** commands to assign IP addresses and netmasks to individual users.

If you choose AAA, you obtain IP addresses from either a previously configured RADIUS server.

Examples

The following example shows how to configure DHCP as the address assignment method:

```
hostname(config)# vpn-addr-assign dhcp
```

Related Commands	Command	Description
	dhcp-network-scope	Specifies the range of IP addresses the security appliance DHCP server should use to assign addresses to users of a group policy.
	ip local pool	Creates a local IP address pool.
	vpn-framed-ip-address	Specifies the IP address to assign to a particular user.
	vpn-framed-ip-netmask	Specifies the netmask to assign to a particular user.

vpn-filter

To specify the name of the ACL to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the ACL, including a null value created by issuing the **vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **vpn-filter none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **vpn-filter** command to apply those ACLs.

vpn-filter { *value* *ACL name* | **none** }

no vpn-filter

Syntax Description

none	Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value <i>ACL name</i>	Provides the name of the previously configured access list.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

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

Usage Guidelines

WebVPN does not use the ACL defined in the **vpn-filter** command.

Examples

The following example shows how to set a filter that invokes an access list named `acl_vpn` for the group policy named `FirstGroup`:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter value acl_vpn
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.

vpn-framed-ip-address

To specify the IP address to assign to a particular user, use the **vpn-framed-ip-address** command in username mode. To remove the IP address, use the **no** form of this command.

vpn-framed-ip-address {*ip_address*}

no vpn-framed-ip-address

Syntax Description

ip_address Provides the IP address for this user.

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		
	Routed	Transparent	Single	Multiple Context	System
Username	•	—	•	—	—

Command History

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

Examples

The following example shows how to set an IP address of 10.92.166.7 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
```

Related Commands

Command	Description
vpn-framed-ip-netmask	Provides the subnet mask for this user.

vpn-framed-ip-netmask

To specify the subnet mask to assign to a particular user, use the **vpn-framed-ip-netmask** command in username mode. To remove the subnet mask, use the **no** form of this command.

vpn-framed-ip-netmask {*netmask*}

no vpn-framed-ip-netmask

Syntax Description

netmask Provides the subnet mask for this user.

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		
	Routed	Transparent	Single	Multiple Context	System
Username	•	—	•	—	—

Command History

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

Examples

The following example shows how to set a subnet mask of 255.255.255. 254 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
```



Note

If RADIUS only returns the subnet mask, the authentication uses the IP address from the local pool which has its own subnet netmask. It does not use the mask from RADIUS. To prevent this, return both the netmask and IP address from RADIUS.

Related Commands

Command	Description
vpn-framed-ip-address	Provides the IP address for this user.

vpn-group-policy

To have a user inherit attributes from a configured group policy, use the **vpn-group-policy** command in username configuration mode. To remove a group policy from a user configuration, use the **no** version of this command. Using this command lets users inherit attributes that you have not configured at the username level.

vpn-group-policy {group-policy name}

no vpn-group-policy {group-policy name}

Syntax Description

group-policy name	Provides the name of the group policy.
-------------------	--

Defaults

By default, VPN users have no group policy association.

Command Modes

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

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

Command History

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

Usage Guidelines

You can override the value of an attribute in a group policy for a particular user by configuring it in username mode, if that attribute is available in username mode.

Examples

The following example shows how to configure a user named anyuser to use attributes from the group policy named FirstGroup:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Adds a group policy to the security appliance database.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a group policy.

Command	Description
username	Adds a user to the security appliance database.
username attributes	Enters username attributes mode, which lets you configure AVPs for specific users.

vpn-idle-timeout

To configure a user timeout period use the **vpn-idle-timeout** command in group-policy configuration mode or in username configuration mode. If there is no communication activity on the connection in this period, the security appliance terminates the connection.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-idle-timeout none** command.

vpn-idle-timeout {*minutes* | **none**}

no vpn-idle-timeout

Syntax Description

<i>minutes</i>	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35791394.
<i>none</i>	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting a value from a default or specified group policy.

Defaults

30 minutes.

Command Modes

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

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

Command History

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

Examples

The following example shows how to set a VPN idle timeout of 15 minutes for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 30
```

Related Commands

group-policy	Creates or edits a group policy.
vpn-session-timeout	Configures the maximum amount of time allowed for VPN connections. At the end of this period of time, the security appliance terminates the connection.

vpn load-balancing

To enter vpn load-balancing mode, in which you can configure VPN load balancing and related functions, use the **vpn load-balancing** command in global configuration mode.

vpn load-balancing



Note

Only ASA Models 5540 and 5520 support VPN load balancing. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **vpn load-balancing** command to enter vpn load-balancing mode. The following commands are available in vpn load-balancing mode:

cluster encryption

cluster ip address

cluster key

cluster port

interface

nat

participate

priority

See the individual command descriptions for detailed information.

Examples

The following is an example of the **vpn load-balancing** command; note the change in the prompt:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

The following is an example of a VPN load-balancing command sequence that includes an interface command that specifies the public interface of the cluster as “test” and the private interface of the cluster as “foo”:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

Command	Description
clear configure vpn load-balancing	Removes the load-balancing runtime configuration and disables load balancing.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
show vpn load-balancing	Displays VPN load-balancing runtime statistics.

vpn-nac-exempt

To add an entry to the list of remote computer types that are exempt from posture validation, use the **vpn-nac-exempt** command in group-policy configuration mode.

```
vpn-nac-exempt os "os name" [filter {acl-name | none}] [disable]
```

To disable inheritance and specify that all hosts will be subject to posture validation, use the **none** keyword immediately following **vpn-nac-exempt**.

```
vpn-nac-exempt none
```

To remove an entry from the exemption list, use the **no** form of this command and name the operating system (and ACL) in the entry to be removed.

```
no vpn-nac-exempt [os "os name"] [filter {acl-name | none}] [disable]
```

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

```
no vpn-nac-exempt
```

Syntax

Description	
<i>acl-name</i>	Name of the ACL present in the security appliance configuration.
disable	Disables the entry in the exemption list without removing it from the list.
filter	Applies an ACL to filter the traffic if the computer's operating system matches the <i>os name</i> .
none	When entered immediately after vpn-nac-exempt , this keyword disables inheritance and specifies that all hosts will be subject to posture validation. When entered immediately after filter , this keyword indicates that the entry does not specify an ACL.
OS	Exempts an operating system from posture validation.
<i>os name</i>	Operating system name. Quotation marks are required only if the name includes a space (for example, "Windows XP").

Defaults

By default, the exemption list is empty.

The default value of the filter attribute is "none".

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Enter the **vpn-nac-exempt** once for each operating system (and ACL) to be matched to exempt remote hosts from posture validation.

Examples

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

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

The following examples exempts all hosts running Windows 98 and apply the ACL acl-1 to traffic from those hosts:

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

The following example adds the same entry to the exemption list, but disables it:

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

The following example removes the same entry from the exemption list, regardless of whether it is disabled:

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

The following example disables inheritance and specifies that all hosts will be subject to posture validation:

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

The following example removes all entries from the exemption list:

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

Related Commands

Command	Description
debug eap	Enables logging of EAP events to debug NAC messaging.
debug eou	Enables logging of EAP over UDP (EAPoUDP) events to debug NAC messaging.
debug nac	Enables logging of NAC events.
nac	Enables Network Admission Control on a group policy.

vpn-sessiondb logoff

To log off all or selected VPN sessions, use the **vpn-sessiondb logoff** command in global configuration mode.

vpn-sessiondb logoff { **remote** | **l2l** | **webvpn** | **email-proxy** | **protocol** *protocol-name* | **name** *username* | **ipaddress** *IPaddr* | **tunnel-group** *groupname* | **index** *indexnumber* | **all** }

Syntax Description

all	Logs off all VPN sessions.																
email-proxy	Logs off all e-mail proxy sessions.																
index <i>indexnumber</i>	Logs off a single session by index number. Specify the index number for the session.																
ipaddress <i>IPaddr</i>	Logs off sessions for the IP address hat you specify.																
l2l	Logs off all LAN-to-LAN sessions.																
name <i>username</i>	Logs off sessions for the username that you specify.																
protocol <i>protocol-name</i>	Logs off sessions for protocols that you specify. The protocols include: <table> <tr> <td>IKE</td><td>POP3S</td></tr> <tr> <td>IMAP4S</td><td>SMTPTS</td></tr> <tr> <td>IPSec</td><td>userHTTPS</td></tr> <tr> <td>IPSecLAN2LAN</td><td>vcaLAN2LAN</td></tr> <tr> <td>IPSecLAN2LANOverNatT</td><td></td></tr> <tr> <td>IPSecOverNatT</td><td></td></tr> <tr> <td>IPSecoverTCP</td><td></td></tr> <tr> <td>IPSecOverUDP</td><td></td></tr> </table>	IKE	POP3S	IMAP4S	SMTPTS	IPSec	userHTTPS	IPSecLAN2LAN	vcaLAN2LAN	IPSecLAN2LANOverNatT		IPSecOverNatT		IPSecoverTCP		IPSecOverUDP	
IKE	POP3S																
IMAP4S	SMTPTS																
IPSec	userHTTPS																
IPSecLAN2LAN	vcaLAN2LAN																
IPSecLAN2LANOverNatT																	
IPSecOverNatT																	
IPSecoverTCP																	
IPSecOverUDP																	
remote	Logs off all remote-access sessions.																
tunnel-group <i>groupname</i>	Logs off sessions for the tunnel group that you specify.																
webvpn	Logs off all WebVPN sessions.																

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

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

Examples

The following example shows how to log off all remote-access sessions:

```
hostname# vpn-sessiondb logoff remote
```

The next example shows how to log off all IPSec sessions:

```
hostname# vpn-sessiondb logoff protocol IPSec
```

vpn-sessiondb max-session-limit

To limit VPN sessions to a lower value than the security appliance allows, use the **vpn-sessiondb max-session-limit** command in global configuration mode. To remove the session limit, use the **no** version of this command. To overwrite the current setting, use the command again.

vpn-sessiondb max-session-limit *{session-limit}*

no vpn-sessiondb max-session-limit

Syntax Description

session-limit Specifies the maximum number of VPN sessions permitted.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command applies to IPsec VPN sessions,.

Examples

The following example shows how to set a maximum VPN session limit of 450:

```
hostname# vpn-sessiondb max-session-limit 450
```

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and WebVPN sessions.
vpn-sessiondb max-webvpn-session-limit	Sets a maximum number of WebVPN sessions.

vpn-sessiondb max-webvpn-session-limit

To limit WebVPN sessions to a lower value than the security appliance allows, use the **vpn-sessiondb max-webvpn-session-limit** command in global configuration mode. To remove the session limit, use the **no** version of this command. To overwrite the current setting, use the command again.

vpn-sessiondb max-webvpn-session-limit {*session-limit*}

no vpn-sessiondb max-webvpn-session-limit

Syntax Description

session-limit Specifies the maximum number of WebVPN sessions permitted.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

This command applies to WebVPN sessions.

Examples

The following example shows how to set a maximum WebVPN session limit of 75:

```
hostname (config)# vpn-sessiondb max-webvpn-session-limit 75
```

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and WebVPN sessions.
vpn-sessiondb max-vpn-session-limit	Sets a maximum number of VPN sessions.

vpn-session-timeout

To configure a maximum amount of time allowed for VPN connections, use the **vpn-session-timeout** command in group-policy configuration mode or in username configuration mode. At the end of this period of time, the security appliance terminates the connection.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-session-timeout none** command.

vpn-session-timeout {*minutes* | **none**}

no vpn-session-timeout

Syntax Description

<i>minutes</i>	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35791394.
none	Permits an unlimited session timeout period. Sets session timeout with a null value, thereby disallowing a session timeout. Prevents inheriting a value from a default or specified group policy.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

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

Examples

The following example shows how to set a VPN session timeout of 180 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

Related Commands

group-policy	Creates or edits a group policy.
vpn-idle-timeout	Configures the user timeout period. If there is no communication activity on the connection in this period, the security appliance terminates the connection.

vpn-simultaneous-logins

To configure the number of simultaneous logins permitted for a user, use the **vpn-simultaneous-logins** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy. Enter 0 to disable login and prevent user access.

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

Syntax Description

integer A number between 0 and 2147483647.

Defaults

The default is 3 simultaneous logins.

Command Modes

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

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

Command History

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

Usage Guidelines

Enter 0 to disable login and prevent user access.

Examples

The following example shows how to allow a maximum of 4 simultaneous logins for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

To configure a VPN tunnel type (IPSec, L2TP over IPSec, or WebVPN), use the **vpn-tunnel-protocol** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpn-tunnel-protocol {webvpn | l2tp-ipsec | IPSec}

no vpn-tunnel-protocol [webvpn | l2tp-ipsec | IPSec]

Syntax Description

IPSec	Negotiates an IPSec tunnel between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
l2tp-ipsec	Negotiates an IPSec tunnel for an L2TP connection.
webvpn	Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client

Defaults

IPSec.

Command Modes

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

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

Command History

Release	Modification
7.0(1)(1)	This command was introduced.
7.2(1)	The l2tp-ipsec keyword was added.

Usage Guidelines

Use this command to configure one or more tunneling modes. You must configure at least one tunneling mode for users to connect over a VPN tunnel.

Examples

The following example shows how to configure WebVPN and IPSec tunneling modes for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol webvpn
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

vpnclient connect

To attempt to establish an Easy VPN Remote connection to the configured server or servers, use the **vpnclient connect** command in global configuration mode.

vpnclient connect

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		
	Routed	Transparent	Single	Multiple	
				Context	System
EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Examples

The following example shows how to attempt to establish an Easy VPN Remote connection to a configured EasyVPN server:

```
hostname(config)# vpnclient connect
hostname(config)#
```


vpnclient disconnect

To disconnect Easy VPN Remote connection, use the **vpnclient disconnect** command in global configuration mode.

vpnclient disconnect

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		
	Routed	Transparent	Single	Multiple Context	System
EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Examples

The following example shows how to disconnect an Easy VPN Remote connection:

```
hostname(config)# vpnclient disconnect
hostname(config)#
```

vpnclient enable

To enable the Easy VPN Remote feature, use the **vpnclient enable** command in global configuration mode. To disable the Easy VPN Remote feature, use the **no** form of this command:

vpnclient enable

no vpnclient enable

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505.

If you enter the **vpnclient enable** command, the ASA 5505 functions as a Easy VPN hardware client (also called “Easy VPN Remote”). If you enter the **no vpnclient enable** command, it functions as an Easy VPN server (also called a “headend”). It can function only as a client or a server.

Examples

The following example shows how to enable the Easy VPN Remote feature:

```
hostname(config)# vpnclient enable
hostname(config)#
```

The following example shows how to disable the Easy VPN Remote feature:

```
hostname(config)# no vpnclient enable
hostname(config)#
```

vpnclient ipsec-over-tcp

To configure the ASA 5505 running as an Easy VPN hardware client to use TCP-encapsulated IPSec, use the **vpnclient ipsec-over-tcp** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

Syntax Description

port	(Optional) Specifies the use of a particular port.
<i>tcp_port</i>	(Required if you specify the keyword port .) Specifies the TCP port number to be used for a TCP-encapsulated IPSec tunnel.

Defaults

The Easy VPN Remote connection uses port 10000 if the command does not specify a port number.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN hardware client (also called “Easy VPN Remote”).

By default, the Easy VPN client and server encapsulate IPSec in User Datagram Protocol (UDP) packets. Some environments, such as those with certain firewall rules, or NAT and PAT devices, prohibit UDP. To use standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) in such environments, you must configure the client and the server to encapsulate IPSec within TCP packets to enable secure tunneling. If your environment allows UDP, however, configuring IPSec over TCP adds unnecessary overhead.

If you configure an ASA 5505 to use TCP-encapsulated IPSec, enter the following command to let it send large packets over the outside interface:

```
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

This command clears the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether the packet can be fragmented. This command lets the Easy VPN hardware client send packets that are larger than the MTU size.

Examples

The following example shows how to configure the Easy VPN hardware client to use TCP-encapsulated IPSec, using the default port 10000, and to let it send large packets over the outside interface:

```
hostname(config)# vpnclient ipsec-over-tcp  
hostname(config)# crypto ipsec df-bit clear-df outside  
hostname(config)#
```

The next example shows how to configure the Easy VPN hardware client to use TCP-encapsulated IPSec, using the port 10501, and to let it send large packets over the outside interface:

```
hostname(config)# vpnclient ipsec-over-tcp port 10501  
hostname(config)# crypto ipsec df-bit clear-df outside  
hostname(config)#
```

vpnclient mac-exempt

To exempt devices behind an Easy VPN Remote connection from individual user authentication requirements, use the **vpnclient mac-exempt** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

```
vpnclient mac-exempt mac_addr_1 mac_mask_1 [mac_addr_2 mac_mask_2...mac_addr_n
mac_mask_n]
```

```
no vpnclient mac-exempt
```

Syntax Description

<i>mac_addr_1</i>	MAC address, in dotted hexadecimal notation, specifying a manufacturer and serial number of a device for which to exempt individual user authentication. For more than one device, specify each MAC address, separating each with a space and the respective network mask. The first 6 characters of the MAC address identify the device manufacturer, and the last 6 characters are the serial number. The last 24 bits are the unit's serial number in hexadecimal format.
<i>mac_mask_1</i>	Network mask for the corresponding MAC address. Use a space to separate the network mask and any subsequent MAC address and network mask pairs.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Devices such as Cisco IP phones, wireless access points, and printers are incapable of performing authentication, and therefore do not authenticate when individual unit authentication is enabled. If individual user authentication is enabled, you can use this command to exempt such devices from authentication. The exemption of devices from individual user authentication is also called “device pass-through.”

The format for specifying the MAC address and mask in this command uses three hex digits, separated by periods; for example, the MAC mask ffff.ffff.ffff matches just the specified MAC address. A MAC mask of all zeroes matches no MAC address, and a MAC mask of ffff.ff00.0000 matches all devices made by the same manufacturer.

Examples

Cisco IP phones have the Manufacturer ID 00036b, so the following command exempts any Cisco IP phone, including Cisco IP phones, you might add in the future:

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

The next example provides greater security but less flexibility because it exempts one specific Cisco IP phone:

```
hostname(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
hostname(config)#
```

vpnclient management

To generate IPsec tunnels for management access to the Easy VPN hardware client, use the **vpnclient management** command in global configuration mode.


```
vpnclient management tunnel ip_addr_1 ip_mask_1 [ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n]
```

vpnclient management clear

To remove the attribute from the running configuration, use the **no** form of this command, which sets up IPsec tunnels exclusively for management in accordance with the **split-tunnel-policy** and **split-tunnel-network-list** commands.

no vpnclient management

Syntax Description

clear	Uses normal routing to provide management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client. This option does not create management tunnels.
 Note Use this option if a NAT device is operating between the client and the Internet.	
<i>ip_addr</i>	IP address of the host or network for which to build a management tunnel from the Easy VPN hardware client. Use this argument with the tunnel keyword. Specify one or more IP addresses, separating each with a space and the respective network mask.
<i>ip_mask</i>	Network mask for the corresponding IP address. Use a space to separate the network mask and any subsequent IP address and network mask pairs.
tunnel	Automates the setup of IPsec tunnels specifically for management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN Client (also called “Easy VPN Remote”). It assumes the ASA 5505 configuration contains the following commands:

vpnclient server to specify the peer.

vpnclient mode to specify the client mode (PAT) or network extension mode.

One of the following:

- **vpnclient vpngroup** to name the tunnel group and the IKE pre-shared key used for authentication on the Easy VPN server.
- **vpnclient trustpoint** to name the trustpoint identifying the RSA certificate to use for authentication

vpnclient enable to enable the ASA 5505 as an Easy VPN Client.

**Note**

The public address of an ASA 5505 behind a NAT device is inaccessible unless you add static NAT mappings on the NAT device.

Examples

The following example shows how to generate an IPSec tunnel from the outside interface of the ASA 5505 to the host with the IP address/mask combination 192.168.10.10 255.255.255.0:

```
hostname(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
hostname(config)#
```

The following example shows how to provide management access to the outside interface of the ASA 5505 without using IPSec:

```
hostname(config)# vpnclient management clear
hostname(config)#
```


vpnclient mode

To configure the Easy VPN Remote connection for either client mode or network extension mode, use the **vpnclient mode** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient mode {client-mode | network-extension-mode}

no vpnclient mode

Syntax Description

client-mode	Configures the Easy VPN Remote connection to use client mode (PAT).
network-extension-mode	Configures the Easy VPN Remote connection to use network extension mode (NEM).

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN Client (also called “Easy VPN Remote”). The Easy VPN Client supports one of two modes of operation: client mode or NEM. The mode of operation determines whether the inside hosts, relative to the Easy VPN Client, are accessible from the Enterprise network over the tunnel. Specifying a mode of operation is mandatory before making a connection because Easy VPN Client does not have a default mode.

- In client mode, the Easy VPN client performs port address translation (PAT) for all VPN traffic from its inside hosts. This mode requires no IP address management for either the inside address of the hardware client (which has a default RFC 1918 address assigned to it) or the inside hosts. Because of PAT, the inside hosts are not accessible from the enterprise network.
- In NEM, all nodes on the inside network and the inside interface are assigned addresses routable across the enterprise network. The inside hosts are accessible from the enterprise network over a tunnel. Hosts on the inside network are assigned IP addresses from an accessible subnet (statically or through DHCP). PAT is not applied to the VPN traffic when in network extension mode.

**Note**

If the Easy VPN hardware client is using NEM and has connections to secondary servers, use the **crypto map set reverse-route** command on each headend device to configure dynamic announcements of the remote network using Reverse Route Injection (RRI).

Examples

The following example shows how to configure an Easy VPN Remote connection for client mode:

```
hostname(config)# vpnclient mode client-mode  
hostname(config)#
```

The following example shows how to configure an Easy VPN Remote connection for NEM:

```
hostname(config)# vpnclient mode network-extension-mode  
hostname(config)#
```

vpnclient nem-st-autoconnect

To configure the Easy VPN Remote connection to automatically initiate IPsec data tunnels when NEM and split tunneling are configured, use the **vpnclient nem-st-autoconnect** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

Syntax Description

This command has no keywords or arguments.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN Client (also called “Easy VPN Remote”).

Before entering the **vpnclient nem-st-autoconnect** command, ensure that network extension mode is enabled for the hardware client. Network extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. IPsec encapsulates all traffic from the private network behind the hardware client to networks behind the security appliance. PAT does not apply. Therefore, devices behind the security appliance have direct access to devices on the private network behind the hardware client over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel. After the tunnel is up, either side can initiate data exchange.



Note

You must also configure the Easy VPN server to enable network extension mode. To do so, use the **nem enable** command in group-policy configuration mode.

IPsec data tunnels are automatically initiated and sustained when in network extension mode, except when split-tunneling is configured.

Examples

The following example shows how to configure an Easy VPN Remote connection to automatically connect in network extension mode with split-tunneling configured. Network extension mode is enabled for the group policy FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
hostname(config)# vpnclient nem-st-autoconnect
hostname(config)#
```

Related Commands

Command	Description
nem	Enables network extension mode for hardware clients.

vpnclient server-certificate

To configure the Easy VPN Remote connection to accept only connections to Easy VPN servers with the specific certificates specified by the certificate map, use the **vpnclient server-certificate** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

Syntax Description

certmap_name Specifies the name of a certificate map that specifies the acceptable Easy VPN server certificate. The maximum length is 64 characters.

Defaults

Easy VPN server certificate filtering is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Use this command to enable Easy VPN server certificate filtering. You define the certificate map itself using the `crypto ca certificate map` and `crypto ca certificate chain` commands.

Examples

The following example shows how to configure an Easy VPN Remote connection to support only connections to Easy VPN servers with the certificate map name `homeservers`:

```
hostname(config)# vpnclient server-certificate homeservers
hostname(config)#
```

Related Commands

Command	Description
certificate	Adds the indicated certificate.
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN Remote connection.

vpnclient server

To configure the primary and secondary IPsec servers, for the Easy VPN Remote connection, use the **vpnclient server** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server *ip_primary_address* [*ip_secondary_address_1* ... *ipsecondary_address_10*]

no vpnclient server

Syntax Description

<i>ip_primary_address</i>	IP address or DNS name of the primary Easy VPN (IPsec) server. Any ASA or VPN 3000 Concentrator Series can act as an Easy VPN server.
<i>ip_secondary_address_n</i>	(Optional) List of the IP addresses or DNS names of up to ten backup Easy VPN servers. Use a space to separate the items in the list.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

A server must be configured before a connection can be established. The **vpnclient server** command supports IPv4 addresses, the names database, or DNS names and resolves addresses in that order.

You can use either the IP address or the hostname of a server.

Examples

The following example associates the name headend-1 with the address 10.10.10.10 and uses the **vpnclient server** command to specify three servers: headend-dns.domain.com (primary), headend-1 (secondary), and 192.168.10.10 (secondary):

```
hostname(config)# names
hostname(config)# 10.10.10.10 headend-1
hostname(config)# vpnclient server headend-dns.domain.com headend-1 192.168.10.10
hostname(config)#
```

The following example shows how to configure a VPN client primary IPsec server with the IP address 10.10.10.15 and secondary servers with the IP addresses 10.10.10.30 and 192.168.10.45.

```
hostname(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10  
hostname(config)#
```


vpnclient trustpoint

To configure the RSA identity certificate to be used by the Easy VPN Remote connection, use the **vpnclient trustpoint** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient trustpoint *trustpoint_name* [**chain**]

no vpnclient trustpoint

Syntax Description

chain	Sends the entire certificate chain.
<i>trustpoint_name</i>	Specifies the name of a trustpoint identifying the RSA certificate to use for authentication.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505 and only when using digital certificates.

Define the trustpoint using the **crypto ca trustpoint** command. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint sub mode control CA-specific configuration parameters which specify how the security appliance obtains the CA certificate, how the security appliance obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

Examples

The following example shows how to configure an Easy VPN Remote connection to use the specific identity certificate named central and to send the entire certificate chain:

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters the trustpoint submode for the specified trustpoint and manages trustpoint information.

vpnclient username

To configure the VPN username and password for the Easy VPN Remote connection, use the **vpnclient username** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient username *xauth_username* **password** *xauth password*

no vpnclient username

Syntax Description

<i>xauth_password</i>	Specifies the password to use for XAUTH. The maximum length is 64 characters.
<i>xauth_username</i>	Specifies the username to use for XAUTH. The maximum length is 64 characters.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

The XAUTH username and password parameters are used when secure unit authentication is disabled and the server requests XAUTH credentials. If secure unit authentication is enabled, these parameters are ignored, and the security appliance prompts the user for a username and password.

Examples

The following example shows how to configure the Easy VPN Remote connection to use the XAUTH username testuser and the password ppurkml:

```
hostname(config)# vpnclient username testuser password ppurkml
hostname(config)#
```

vpnclient vpngroup

To configure the VPN tunnel group name and password for the Easy VPN Remote connection, use the **vpnclient vpngroup** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient vpngroup *group_name* **password** *preshared_key*

no vpnclient vpngroup

Syntax Description

<i>group_name</i>	Specifies the name of the VPN tunnel group configured on the Easy VPN server. The maximum length is 64 characters, and no spaces are allowed.
<i>preshared_key</i>	The IKE pre-shared key used for authentication by the Easy VPN server. The maximum length is 128 characters.

Defaults

If the configuration of the ASA 5505 running as an Easy VPN client does not specify a tunnel group, the client attempts to use an RSA certificate.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN client (also called “Easy VPN Remote”).

Use the pre-shared key as the password. You must configure a server before establishing a connection.

Examples

The following example shows how to configure an Easy VPN Remote connection with a VPN tunnel group with the group name TestGroup1 and the password my_key123.

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
hostname(config)#
```

Related Commands

Command	Description
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN connection.


wccp

To allocate space and to enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **wccp** command in global configuration mode. To disable the service group and deallocate space, use the no form of this command.

wccp { **web-cache** | *service-number* } [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]

no wccp { **web-cache** | *service-number* } [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [0 | 7]]

Syntax Description

web-cache	Specifies the web-cache service.
	 Note Web cache counts as one service. The maximum number of services, including those assigned with the service-number argument are 256
<i>service-number</i>	A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254 and up to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the web-cache keyword.
redirect-list	(Optional) Used with an access list that controls traffic redirected to this service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list. The access list should only contain network addresses. Port-specific entries are not supported.
<i>access-list</i>	Specifies the name of the access list.
group-list	(Optional) Access list that determines which web caches are allowed to participate in the service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
password	(Optional) Specifies Message Digest 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded.
<i>password</i>	Specifies the password to be used for authentication. The password argument can be up to seven characters in length.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable WCCP for participation in a service group:

```
hostname(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

wccp redirect

To enable packet redirection on the ingress of an interface using Web Cache Communication Protocol (WCCP), use the **wccp redirect** command. To disable WCCP redirection, use the no form of this command.

wccp interface *interface_name* *service* **redirect in**

no wccp interface *interface_name* *service* **redirect in**

Syntax Description

<i>interface_name</i>	Name of the interface where packets should be redirected..
<i>service</i>	Specifies the service group. You can specify the web-cache keyword, or you can specify the identification number (from 0 to 99) of the service.
in	Specifies redirection when packet comes into this interface

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable WCCP redirection on the inside interface for the web-cache service:

```
hostname(config)# wccp interface inside web-cache redirect in
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp	Enables support of WCCP with service groups.

web-agent-url

To specify the SSO server URL to which the security appliance makes SSO authentication requests, use the **web-agent-url** command in webvpn-sso-siteminder configuration mode. This is an SSO with CA SiteMinder command.

To remove an SSO server authentication URL, use the **no** form of this command.

web-agent-url *url*

no web-agent-url *url*



Note

This command is required for SSO authentication.

Syntax Description

<i>url</i>	Specifies the authentication URL of the SSO server. Must contain http:// or https://.
------------	---

Defaults

By default, an authentication URL is not configured.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single-sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once. The SSO server has a URL that handles authentication requests.

Use the **web-agent-url** command to configure the security appliance to send authentications to this URL. Before configuring the authentication URL, you must create the SSO server using the **sso-server** command.

Examples

The following example, entered in webvpn-sso-siteminder configuration mode, specifies an authentication URL of http://www.example.com/webvpn:

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
```

```
hostname(config-webvpn-sso-siteminder)#
```

Related Commands	Command	Description
	max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
	policy-server-secret	Creates a secret key used to encrypt authentication requests to an SSO server.
	request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
	show webvpn sso-server	Displays the operating statistics for an SSO server.
	sso-server	Creates a single sign-on server.

web-applications

To customize the Web Application box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-applications** command from webvpn customization mode:

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

title	Specifies you are changing the title.
message	Specifies you are changing the message displayed under the title.
dropdown	Specifies you are changing the dropdown box.
text	Specifies you are changing the text.
style	Specifies you are changing the HTML style.
<i>value</i>	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default title text is “Web Application”.

The default title style is background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text is “Enter Web Address (URL)”.

The default message style is background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is “Web Bookmarks”.

The default dropdown style is border:1px solid black;font-weight:bold;color:black;font-size:80%.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

The following example changes the title to “Applications”, and the color of the text to blue:

```
F1-asal(config)# webvpn
F1-asal(config-webvpn)# customization cisco
F1-asal(config-webvpn-custom)# web-applications title text Applications
F1-asal(config-webvpn-custom)# web-applications title style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

web-bookmarks

To customize the Web Bookmarks title or links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-bookmarks** command from webvpn customization mode:

web-bookmarks {link {style *value*} | title {style *value* | text *value*}}

[no] **web-bookmarks** {link {style *value*} | title {style *value* | text *value*}}

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

link	Specifies you are changing the links.
title	Specifies you are changing the title.
style	Specifies you are changing the HTML style.
text	Specifies you are changing the text.
<i>value</i>	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default link style is color:#669999;border-bottom: 1px solid #669999;text-decoration:none.

The default title style is color:#669999;background-color:#99CCCC;font-weight:bold.

The default title text is “Web Bookmarks”.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

The following example customizes the Web Bookmarks title to “Corporate Web Bookmarks”:

```
F1-asal(config)# webvpn
F1-asal(config-webvpn)# customization cisco
F1-asal(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.

webvpn (group-policy and username modes)

To enter this webvpn mode, use the **webvpn** command in group-policy configuration mode or in username configuration mode. To remove all commands entered in webvpn mode, use the **no** form of this command. These webvpn commands apply to the username or group policy from which you configure them.

Webvpn commands for group policies and usernames define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter.

webvpn

no webvpn

Syntax Description

This command has no arguments or keywords.

Defaults

WebVPN is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Webvpn mode, which you enter from global configuration mode, lets you configure global settings for WebVPN. The **webvpn** command in group-policy attributes configuration mode or username attributes configuration mode applies the settings specified in the webvpn command to the group or user specified in the parent command. In other words, webvpn mode, described in this section, and which you enter from group-policy or username mode, lets you customize a WebVPN configuration for specific users or group policies.

The webvpn attributes that you apply for a specific group policy in group-policy attributes mode override those specified in the default group policy. The WebVPN attributes that you apply for a specific user in username attributes mode override both those in the default group policy and those in the group policy to which that user belongs. Essentially, these commands let you tweak the settings that would otherwise be inherited from the default group or the specified group policy. For information about the WebVPN settings, see the description of the **webvpn** command in global configuration mode.

The following table lists the attributes you can configure in webvpn group-policy attributes and username attributes mode. See the individual command descriptions for details.

Attribute	Description
auto-signon	Configures the security appliance to automatically pass WebVPN user login credentials on to internal servers, providing a single sign-on method for WebVPN users.
customization	Specifies a preconfigured WebVPN customization to apply.
deny-message	Specifies a message to display to the user when access is denied.
filter	Identifies the access list to be used for WebVPN connections.
functions	Configures file access and file browsing, MAPI Proxy, and URL entry over WebVPN.
homepage	Sets the URL of the webpage that displays when WebVPN users log in.
html-content-filter	Identifies Java, ActiveX, images, scripts, and cookies to filter for WebVPN sessions.
http-comp	Specifies the HTTP compression algorithm to use.
keep-alive-ignore	Specifies the maximum object size to ignore for updating the session.
port-forward	Enables WebVPN application access.
port-forward-name	Configures the display name that identifies TCP port forwarding to end users.
sso-server	Configures the SSO server name.
svc	Configures SSL VPN Client attributes.
url-list	Identifies a list of servers and URLs that users can access via WebVPN.

Examples

The following example shows how to enter webvpn mode for the group policy named “FirstGroup”:

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

The following example shows how to enter webvpn mode for the username named “test”:

```
hostname(config)# group-policy test attributes
hostname(config-username)# webvpn
hostname(config-webvpn)#
```

Related Commands

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

who

To display active Telnet administration sessions on the security appliance, use the **who** command in privileged EXEC mode.

who [*local_ip*]

Syntax Description

local_ip (Optional) Specifies to limit the listing to one internal IP address or network address, 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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **who** command allows you to display the TTY_ID and IP address of each Telnet client that is currently logged into the security appliance.

Examples

This example shows the output of the **who** command when a client is logged into the security appliance through a Telnet session:

```
hostname# who
0: 100.0.0.2
hostname# who 100.0.0.2
0: 100.0.0.2
hostname#
```

Related Commands

Command	Description
kill	Terminate a Telnet session.
telnet	Adds Telnet access to the security appliance console and sets the idle timeout.

window-variation

To drop a connection with a window size variation, use the **window-variation** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

window variation { **allow-connection** | **drop-connection** }

no window variation { **allow-connection** | **drop-connection** }

Syntax Description

allow-connection	Allows the connection.
drop-connection	Drops the connection.

Defaults

The default action is to allow the connection.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **window-variation** command in tcp-map configuration mode to drop all connections with a window size that has been shrunk.

The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without having accepted too much data. From the TCP specification, “shrinking the window” is strongly discouraged. When this condition is detected, the connection can be dropped.

Examples

The following example shows how to drop all connections with a varied window size:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# window-variation drop-connection
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
```

```
hostname(config-pmap)# class cmap  
hostname(config-pmap)# set connection advanced-options tmap  
hostname(config)# service-policy pmap global
```

Related Commands

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

wins-server

To set the IP address of the primary and secondary WINS servers, use the **wins-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a WINS server from another group policy. To prevent inheriting a server, use the **wins-server none** command.

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

Syntax Description

none	Sets wins-servers to a null value, thereby allowing no WINS servers. Prevents inheriting a value from a default or specified group policy.
value <i>ip_address</i>	Specifies the IP address of the primary and secondary WINS servers.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Every time you issue the **wins-server** command you overwrite the existing setting. For example, if you configure WINS server x.x.x.x and then configure WINS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole WINS server. The same holds true for multiple servers. To add a WINS server rather than overwrite previously configured servers, include the IP addresses of all WINS servers when you enter this command.

Examples

The following example shows how to configure WINS servers with the IP addresses 10.10.10.15, 10.10.10.30, and 10.10.10.45 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

write erase

To erase the startup configuration, use the **write erase** command in privileged EXEC mode. The running configuration remains intact.

write erase

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines This command is not supported within a security context. Context startup configurations are identified by the **config-url** command in the system configuration. If you want to delete a context configuration, you can remove the file manually from the remote server (if specified) or clear the file from Flash memory using the **delete** command in the system execution space.

Examples The following example erases the startup configuration:

```
hostname# write erase
Erase configuration in flash memory? [confirm] y
```

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
delete	Removes a file from Flash memory.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

write memory

To save the running configuration to the startup configuration, use the **write memory** command in privileged EXEC mode.

write memory [**all** [/noconfirm]]

Syntax Description

/noconfirm	Eliminates the confirmation prompt when you use the all keyword.
all	From the system execution space in multiple context mode, this keyword saves all context configurations as well as the system configuration.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(1)	You can now save all context configurations with the all keyword.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line. Changes are only preserved between reboots if you save them to the startup configuration, which is the configuration loaded into running memory at startup. The location of the startup configuration for single context mode and for the system in multiple context mode can be changed from the default location (a hidden file) to a location of your choosing using the **boot config** command. For multiple context mode, a context startup configuration is at the location specified by the **config-url** command in the system configuration.

In multiple context mode, you can enter the **write memory** command in each context to save the current context configuration. To save all context configurations, enter the **write memory all** command in the system execution space. Context startup configurations can reside on external servers. In this case, the security appliance saves the configuration back to the server specified by the **config-url** command, except for HTTP and HTTPS URLs, which do not allow you to save the configuration back to the server. After the security appliance saves each context with the **write memory all** command, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

```
The context 'context a' could not be saved due to Unavailability of resources
```

- For contexts that are not saved because the remote destination is unreachable, the following message appears:

The context 'context a' could not be saved due to non-reachability of destination

- For contexts that are not saved because the context is locked, the following message appears:

Unable to save the configuration for the following contexts as these contexts are locked.
context 'a' , context 'x' , context 'z' .

A context is only locked if another user is already saving the configuration or in the process of deleting the context.

- For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:

Unable to save the configuration for the following contexts as these contexts have read-only config-urls:
context 'a' , context 'b' , context 'c' .

- For contexts that are not saved because of bad sectors in the Flash memory, the following message appears:

The context 'context a' could not be saved due to Unknown errors

Because the system uses the admin context interfaces to access context startup configurations, the **write memory** command also uses the admin context interfaces. The **write net** command, however, uses the context interfaces to write a configuration to a TFTP server.

The **write memory** command is equivalent to the **copy running-config startup-config** command.

Examples

The following example saves the running configuration to the startup configuration:

```
hostname# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
hostname#
```

Related Commands

Command	Description
admin-context	Sets the admin context.
configure memory	Merges the startup configuration with the running configuration.
config-url	Specifies the location of the context configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
write net	Copies the running configuration to a TFTP server.

write net

To save the running configuration to a TFTP server, use the **write net** command in privileged EXEC mode.

write net [*server*:*filename*] | :*filename*

Syntax Description

<i>:filename</i>	<p>Specifies the path and filename. If you already set the filename using the tftp-server command, then this argument is optional.</p> <p>If you specify the filename in this command as well as a name in the tftp-server command, the security appliance treats the tftp-server command filename as a directory, and adds the write net command filename as a file under the directory.</p> <p>To override the tftp-server command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path. If your TFTP server does not support this type of URL, use the copy running-config tftp command instead.</p> <p>If you specified the TFTP server address using the tftp-server command, you can enter the filename alone preceded by a colon (:).</p>
<i>server</i> :	<p>Sets the TFTP server IP address or name. This address overrides the address you set in the tftp-server command, if present.</p> <p>The default gateway interface is the highest security interface; however, you can set a different interface name using the tftp-server command.</p>

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line.

In multiple context mode, this command saves only the current configuration; you cannot save all contexts with a single command. You must enter this command separately for the system and for each context. The **write net** command uses the context interfaces to write a configuration to a TFTP server. The **write memory** command, however, uses the admin context interfaces to save to the startup configuration because the system uses the admin context interfaces to access context startup configurations.

The **write net** command is equivalent to the **copy running-config tftp** command.

Examples

The following example sets the TFTP server and filename in the **tftp-server** command:

```
hostname# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
hostname# write net
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command is not populated.

```
hostname# write net 10.1.1.1:/configs/contextbackup.cfg
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command supplies the directory name, and the server address is overridden.

```
hostname# tftp-server 10.1.1.1 configs
hostname# write net 10.1.2.1:context.cfg
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
copy running-config tftp	Copies the running configuration to a TFTP server.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write memory	Saves the running configuration to the startup configuration.

write standby

To copy the security appliance or context running configuration to the failover standby unit, use the **write standby** command in privileged EXEC mode.

write standby

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For Active/Standby failover, the **write standby** command writes the configuration stored in the RAM of the active failover unit to the RAM on the standby unit. Use the **write standby** command if the primary and secondary unit configurations have different information. Enter this command on the active unit.

For Active/Active failover, the **write standby** command behaves as follows:

- If you enter the **write standby** command in the system execution space, the system configuration and the configurations for all of the security contexts on the security appliance is written to the peer unit. This includes configuration information for security contexts that are in the standby state. You must enter the command in the system execution space on the unit that has failover group 1 in the active state.
- If you enter the **write standby** command in a security context, only the configuration for the security context is written to the peer unit. You must enter the command in the security context on the unit where the security context appears in the active state.



Note

The **write standby** command replicates the configuration to the running configuration of the peer unit; it does not save the configuration to the startup configuration. To save the configuration changes to the startup configuration, use the **copy running-config startup-config** command on the same unit that you entered the **write standby** command. The command will be replicated to the peer unit and the configuration saved to the startup configuration.

When Stateful Failover is enabled, the **write standby** command also replicates state information to the standby unit after the configuration replication is complete.

Examples

The following example writes the current running configuration to the standby unit:

```
hostname# write standby
Building configuration...
[OK]
hostname#
```

Related Commands

Command	Description
failover	Forces the standby unit to reboot.
reload-standby	

write terminal

To show the running configuration on the terminal, use the **write terminal** command in privileged EXEC mode.

write terminal

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines This command is equivalent to the **show running-config** command.

Examples The following example writes the running configuration to the terminal:

```
hostname# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

zonelabs-integrity fail-close

To configure the security appliance so that connections to VPN clients close when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command in global configuration mode. To reinstate the default whereby the VPN connections remain open on failure of the Zone Labs connection, use the **no** form of this command.

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the connection remains open on failure.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If the primary Zone Labs Integrity Firewall Server does not respond to the security appliance, the security appliance still establishes VPN client connections to the private network by default. It also maintains open, existing connections. This ensures that the enterprise VPN is not disrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command.

To return to the default condition whereby the security appliance maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command.

Examples

The following example configures the security appliance to close the VPN client connections if the Zone Labs Integrity Firewall Server fails to respond or if the connection is interrupted:

```
hostname(config)# zonelabs-integrity fail-close
hostname(config)#
```

Related Commands	Command	Description
	zonelabs-integrity fail-open	Specifies that VPN client connections to the security appliance remain open after the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
	zonelabs-integrity fail-timeout	Specifies the time in seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.
	zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.

zonelabs-integrity fail-open

To keep remote VPN client connections to the security appliance open after the connection between the security appliance and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command in global configuration mode. To close connections to VPN clients upon failure of the Zone Labs server connection, use the **no** form of this command.

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

Syntax Description

This command has no arguments or keywords.

Defaults

By default, remote VPN connections remain open if the security appliance does not establish or maintain a connection to the Zone Labs Integrity Firewall Server.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If the primary Zone Labs Integrity Firewall Server does not respond to the security appliance, the security appliance still establishes VPN client connections to the private network by default. It also maintains existing open connections. This ensures that the enterprise VPN is not disrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command. To then return to the default condition whereby the security appliance maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command or the **no zonelabs-integrity fail-open** command.

Examples

The following example reinstates the default condition whereby the VPN client connections remain open if the connection to the Zone Labs Integrity Firewall Server fails:

```
hostname(config)# zonelabs-integrity fail-open
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the security appliance close VPN client connections when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-timeout	Specifies the time in seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.

zonelabs-integrity fail-timeout

To specify the time in seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Server unreachable, use the **zonelabs-integrity fail-timeout** command in global configuration mode. To restore the default timeout of 10 seconds, use the **no** form of this command without an argument.

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

Syntax Description

timeout The number of seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Servers unreachable. The acceptable range is from 5 to 20 seconds.

Defaults

The default timeout value is 10 seconds.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If the security appliance waits for the specified number of seconds without a response from the Zone Labs server, the server is declared nonresponsive. Connections to VPN clients either remain open by default or if configured to do so with the **zonelabs-integrity fail-open** command. If, however, the **zonelabs-integrity fail-close** command has been issued, the connections will close when the security appliance declares the Integrity server unresponsive.

Examples

The following example configures the security appliance to declare the active Zone Labs Integrity Server to be unreachable after 12 seconds:

```
hostname(config)# zonelabs-integrity fail-timeout 12
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-open	Specifies that VPN client connections to the security appliance remain open after the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-close	Specifies that the security appliance close VPN client connections when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.

zonelabs-integrity interface

To specify a security appliance interface for communication with the Zone Labs Integrity Server, use the **zonelabs-integrity interface** command in global configuration mode. To reset the Zone Labs Integrity Firewall Server interface back to the default of none, use the **no** form of this command.

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

Syntax Description

interface Specifies the security appliance interface on which the Zone Labs Integrity Firewall Server communicates. It is often an interface name created with the **nameif** command.

Defaults

By default, the Zone Labs Integrity Firewall Server interface is set to none.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example configures three Zone Labs Integirty Servers using IP addresses ranging from 10.0.0.5 to 10.0.0.7. The commands also configure the security appliance to listen to the server on port 300 and on an interface called inside:

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
hostname(config)# zonelabs-integrity port 300
hostname(config)# zonelabs-integrity interface inside
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.

Command	Description
zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity port

To specify a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server, use the **zonelabs-integrity port** command in global configuration mode. To revert to the default port of 5054 for the Zone Labs Integrity Firewall Server, use the **no** form of this command.

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

Syntax Description

port	Specifies a Zone Labs Integrity Firewall Server port on the security appliance.
<i>port_number</i>	The number of the Zone Labs Integrity Firewall Server port. It can range from 10 to 10000.

Defaults

The default Zone Labs Integrity Firewall Server port is 5054.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The security appliance listens to the Zone Labs Integrity Firewall Server on the port and interface configured with the **zonelabs-integrity port** and **zonelabs-integrity interface** commands respectively.



Note

The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the security appliance and then reestablish the client VPN session.

Examples

The following example configures a Zone Labs Integrity Servers using the IP address 10.0.0.5. The commands also configure the security appliance to listen to the active Zone Labs server on port 300 instead of the default 5054 port:

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5
hostname(config)# zonelabs-integrity port 300
hostname(config)#
```

Related Commands	Command	Description
	zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
	zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.
	zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
	zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity server-address

To add Zone Labs Integrity Firewall Servers to the security appliance configuration, use the **zonelabs-integrity server-address** command in global configuration mode. Specify the Zone Labs server by either IP address or hostname.

To remove Zone Labs Integrity Firewall Servers from the running configuration, use the **no** form of this command without arguments.

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address



Note

While the user interfaces appear to support the configuration of multiple Integrity Servers, the security appliance only supports one server at a time in the current release.

Syntax Description

<i>hostname</i>	Specifies the hostname of the Zone Labs Integrity Firewall Server. See the name command for hostname guidelines.
<i>ip-address</i>	Specifies the IP address of the Zone Labs Integrity Firewall Server.

Command Default

By default, no Zone Labs Integrity Firewall Servers are configured.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

With this release, you can configure one Zone Labs Integrity Firewall Server. If that server fails, configure another Integrity Server first and then reestablish the client VPN session.

To specify a server by hostname, you must first configure the Zone Labs server name using the **name** command. Before using the **name** command, use the **names** command to enable it.



Note

The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the security appliance and then reestablish the client VPN session.

Examples

The following example assigns the server name ZL-Integrity-Svr to the IP address 10.0.0.5 and configures a Zone Labs Integrity Server using that name:

```
hostname(config)# names
hostname(config)# name 10.0.0.5 ZL-Integrity-Svr
hostname(config)# zonelabs-integrity server-address ZL-Integrity-Svr
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the security appliance close VPN client connections when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity ssl-certificate-port

To specify a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate, use the **zonelabs-integrity ssl-certificate-port** command in global configuration mode. To revert to the default port number (80), use the **no** form of this command without an argument.

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

Syntax Description

cert-port-number Specifies a port number on which the security appliance expects the Zone Labs Integrity Firewall Server to connect when requesting an SSL certificate.

Defaults

By default, the security appliance expects the Zone Labs Integrity Firewall Server to request an SSL certificate on port 80.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

For SSL communications between the security appliance and the Zone Labs Integrity Firewall Server, the security appliance is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (security appliance) must be authenticated by the client (Zone Labs server). The **zonelabs-integrity ssl-certificate-port** command specifies the port to which the Zone Labs server connects when requesting the SSL server certificate.

Examples

The following example configures port 30 on the security appliance to receive SSL certificate requests from the Zone Labs Integrity Server:

```
hostname(config)# zonelabs-integrity ssl-certificate-port 30
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity ssl-client-authentication

To enable authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance, use the **zonelabs-integrity ssl-client-authentication** command in global configuration mode with the *enable* argument. To disable authentication of the Zone Labs SSL certificate, use the *disable* argument or use the **no** form of this command without an argument.

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

Syntax Description

<i>enable</i>	Specifies that the security appliance authenticates the SSL certificate of the Zone Labs Integrity Firewall Server.
<i>disable</i>	Specifies the IP address of the Zone Labs Integrity Firewall Server.

Defaults

By default, security appliance authentication of the Zone Labs Integrity Firewall Server SSL certificate is disabled.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

For SSL communications between the security appliance and the Zone Labs Integrity Firewall Server, the security appliance is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (security appliance) must be authenticated by the client (Zone Labs server). Authentication of the client certificate is optional, however. You use the **zonelabs-integrity ssl-client-authentication** command to enable or disable security appliance authentication of the Zone Lab server (SSL client) certificate.

Examples

The following example configures the security appliance to authenticate the SSL certificate of the Zone Labs Integrity Server:

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
hostname(config)#
```

Related Commands	Command	Description
	zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
	zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
	zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.
	zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.

