shun through snmp-server user Commands

shun

To block connections from an attacking host, use the **shun** command in privileged EXEC mode. To disable a shun, use the **no** form of this command.

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

Syntax Description

dest_port	(Optional) Specifies the destination port of a current connection that you want to drop when you place the shun on the source IP address.
dest_ip	(Optional) Specifies the destination address of a current connection that you want to drop when you place the shun on the source IP address.
protocol	(Optional) Specifies the IP protocol of a current connection that you want to drop when you place the shun on the source IP address, such as UDP or TCP. By default, the protocol is 0 (any protocol).
source_ip	Specifies the address of the attacking host. If you only specify the source IP address, all future connections from this address are dropped; current connections remain in place. To drop a current connection and also place the shun, specify the additional parameters of the connection. Note that the shun remains in place for all future connections from the source IP address, regardless of destination parameters.
source_port	(Optional) Specifies the source port of a current connection that you want to drop when you place the shun on the source IP address.
vlan_id	(Optional) Specifies the VLAN ID where the source host resides.

Defaults

The default protocol is 0 (any protocol).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **shun** command lets you block connections from an attacking host. All future connections from the source IP address are dropped and logged until the blocking function is removed manually or by the Cisco IPS sensor. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, then you drop the matching connection as well as placing a shun on all future connections from the source IP address; all future connections are shunned, not just those that match these specific connection parameters.

You can only have one **shun** command per source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the ASA configuration.

Whenever an interface configuration is removed, all shuns that are attached to that interface are also removed. If you add a new interface or replace the same interface (using the same name), then you must add that interface to the IPS sensor if you want the IPS sensor to monitor that interface.

Examples

The following example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the ASA connection table reads as follows:

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

Apply the **shun** command using the following options:

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

The command deletes the specific current connection from the ASA connection table and also prevents all future packets from 10.1.1.27 from going through the ASA.

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
show conn	Shows all active connections.
show shun	Displays the shun information.

shutdown

To disable an interface, use the **shutdown** command in interface configuration mode. To enable an interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

All physical interfaces are shut down by default. Allocated interfaces in security contexts are not shut down in the configuration.

Command Modes

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

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

Command History

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

Usage Guidelines

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Note This command only disables the software interface. The physical link remains up, and the directly connected device is still recognized as being up even when the corresponding interface is configured with the **shutdown** command.

Examples

The following example enables a main interface:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

The following example enables a subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
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 shuts down the subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
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)# shutdown
```

Related Commands

Command	Description
clear xlate	Resets all translations for existing connections, causing the connections to be reset.
interface	Configures an interface and enters interface configuration mode.

shutdown (ca-server mode)

To disable the local Certificate Authority (CA) server and render the enrollment interface inaccessible to users, use the **shutdown** command in CA server configuration mode. To enable the CA server, lock down the configuration from changes, and to render the enrollment interface accessible, use the **no** form of this command.

[**no**] **shutdown**

Syntax Description

This command has no arguments or keywords.

Defaults

Initially, by default, the CA server is shut down.

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**
Ca server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command in CA server mode is similar to the **shutdown** command in interface mode. At setup time, the local CA server is shutdown by default and must be enabled using the **no shutdown** command. When you use the **no shutdown** command for the first time, you enable the CA server and generate the CA server certificate and keypair.

Note The CA configuration cannot be changed once you lock it and generate the CA certificate by issuing the **no shutdown** command.

To enable the CA server and lock down the current configuration with the **no shutdown** command, a 7-character password is required to encode and archive a PKCS12 file containing the CA certificate and keypair that is to be generated. The file is stored to the storage identified by a previously specified **database path** command.

Examples

The following example disables the local CA server and renders the enrollment interface inaccessible:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# shutdown
hostname(config-ca-server)#
```

The following example enables the local CA server and makes the enrollment interface accessible:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no shutdown
hostname(config-ca-server)#

hostname(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...

hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
show crypto ca server	Displays the status of the CA configuration.

sla monitor

To create an SLA operation, use the **sla monitor** command in global configuration mode. To remove the SLA operation, use the **no** form of this command.

sla monitor *sla_id*

no sla monitor *sla_id*

Syntax Description

sla_id	Specifies the ID of the SLA being configured. If the SLA does not already exist, it is created. Valid values are from 1 to 2147483647.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **sla monitor** command creates SLA operations and enters SLA Monitor configuration mode. Once you enter this command, the command prompt changes to `hostname(config-sla-monitor)#` to indicate that you are in SLA Monitor configuration mode. If the SLA operation already exists, and a type has already been defined for it, then the prompt appears as `hostname(config-sla-monitor-echo)#`. You can create a maximum of 2000 SLA operations. Only 32 SLA operations may be debugged at any time.

The **no sla monitor** command removes the specified SLA operation and the commands used to configure that operation.

After you configure an SLA operation, you must schedule the operation with the **sla monitor schedule** command. You cannot modify the configuration of the SLA operation after scheduling it. To modify the the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

To display the current configuration settings of the operation, use the **show sla monitor configuration** command. To display operational statistics of the SLA operation, use the **show sla monitor operation-state command**. To see the SLA commands in the configuration, use the **show running-config sla monitor** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
frequency	Specifies the rate at which the SLA operation repeats.
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor schedule	Schedules the SLA operation.
timeout	Sets the amount of time the SLA operation waits for a response.
track rtr	Creates a tracking entry to poll the SLA.

sla monitor schedule

To schedule an SLA operation, use the **sla monitor schedule** command in global configuration mode. To remove SLA operation schedule, and place the operation in the pending state, use the **no** form of this command.

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

Syntax Description

after *hh*:*mm*:*ss*	Indicates that the operation should start the specified number of hours, minutes, and seconds after the command was entered.
ageout *seconds*	(Optional) Specifies the number of seconds to keep the operation in memory when it is not actively collecting information. After an SLA operation ages out, it is removed from the running configuration.
day	Number of the day to start the operation on. Valid values are from 1 to 31. If a day is not specified, then the current day is used. If you specify a day you must also specify a month.
hh:*mm*[:*ss*]	Specifies an absolute start time in 24-hour notation. Seconds are optional. The next time the specified time occurs is implied unless you specify a *month* and a *day*.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Sets the number of seconds the operation actively collects information.
month	(Optional) Name of the month to start the operation in. If a month is not specified, then the current month is used. I f you specify a month you must also specify a day. You can enter the full English name of the month or just the first three letters.
now	Indicates that the operation should start as soon as the command is entered.
pending	Indicates that no information is collected. This is the default state.
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.
sla-id	The ID of the SLA operation being scheduled.
start-time	Sets the time when the SLA operation starts.

Defaults

The defaults are as follows:

- SLA operations are in the **pending** state until the scheduled time is met. This means that the operation is enabled but not actively collecting data.
- The default **ageout** time is 0 seconds (never ages out).
- The default **life** is 3600 seconds (one hour).

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

When an SLA operation is in an active state, it immediately begins collecting information. The following time line shows the age-out process of the operation:

```
W---------------------X---------------------Y---------------------Z
```

- W is the time the SLA operation was configured with the **sla monitor** command.
- X is the start time of the SLA operation. This is when the operation became “active”.
- Y is the end of life as configured with the **sla monitor schedule** command (the **life** seconds have counted down to zero).
- Z is the age out of the operation.

The age out process, if used, starts counting down at W, is suspended between X and Y, and is reset to its configured size are starts counting down again at Y. When an SLA operation ages out, the SLA operation configuration is removed from the running configuration. It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation configuration time and start time (X and W) must be less than the age-out seconds.

The **recurring** keyword is only supported for scheduling single SLA operations. You cannot schedule multiple SLA operations using a single **sla monitor schedule** command. The **life** value for a recurring SLA operation should be less than one day. The **ageout** value for a recurring operation must be “never” (which is specified with the value 0), or the sum of the **life** and **ageout** values must be more than one day. If the recurring option is not specified, the operations are started in the existing normal scheduling mode.

You cannot modify the configuration of the SLA operation after scheduling it. To modify the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

Examples

The following example shows SLA operation 25 scheduled to begin actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity. When this SLA operation ages out, all configuration information for the SLA operation is removed from the running configuration.

```
hostname(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

The following example shows SLA operation 1 schedule to begin collecting data after a 5-minute delay. The default life of one hour applies.

```
hostname(config)# sla monitor schedule 1 start after 00:05:00
```

The following example shows SLA operation 3 scheduled to begin collecting data immediately and is scheduled to run indefinitely:

```
hostname(config)# sla monitor schedule 3 life forever start-time now
```

The following example shows SLA operation 15 scheduled to begin automatically collecting data every day at 1:30 a.m.:

```
hostname(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor	Defines an SLA monitoring operation.

smart-tunnel auto-signon enable

To enable smart tunnel auto sign-on in clientless (browser-based) SSL VPN sessions, use the **smart-tunnel auto-signon enable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

To remove the **smart-tunnel auto-signon enable** command from the group policy or username and inherit it from the default group-policy, use the **no** form of this command.

no smart-tunnel auto-signon enable *list* [**domain** *domain*] [port *port*] [realm *realm string*]

Syntax Description

domain *domain*	(Optional). Name of the domain to be added to the username during authentication. If you enter a domain, enter the **use-domain** keyword in the list entries.
list	The name of a smart tunnel auto sign-on list already present in the ASA webvpn configuration. To view the smart tunnel auto sign-on list entries in the SSL VPN configuration, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.
port	Specifies which port performs auto sign-on.
realm	Configures a realm for the authentication.

Defaults

No defaults exist for this command.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	This command was introduced.
8.4(1)	Optional *realm* and *port* arguments were introduced.

Usage Guidelines

The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.

You must use the **smart-tunnel auto-signon** *list* command to create a list of servers first. You can assign only one list to a group policy or username.

A realm string is associated with the protected area of the website and is passed back to the browser either in the authentication prompt or in the HTTP headers during authentication. If adminstrators do not know the corresponding realm, they should perform logon once and get the string from the prompt dialog.

Administrators can now optionally specify a port number for the corresponding hosts. For Firefox, if no port number is specified, auto sign-on is performed on HTTP and HTTPS, accessed by the default port numbers 80 and 443 respectively.

Examples

The following commands enable the smart tunnel auto sign-on list named HR:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR
hostname(config-group-webvpn)
```

The following command enables the smart tunnel auto sign-on list named HR and adds the domain named CISCO to the username during authentication:

```
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

The following command removes the smart tunnel auto sign-on list named HR from the group policy and inherits the smart tunnel auto sign-on list command from the default group policy:

```
hostname(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

Related Commands

Command	Description
smart-tunnel auto-signon *list*	Creates a list of servers for which to automate the submission of credentials in smart tunnel connections.
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration on the ASA.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel *list*	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel auto-signon list

To create a list of servers for which to automate the submission of credentials in smart tunnel connections, use the **smart-tunnel auto-signon list** command in webvpn configuration mode.Use this command for each server you want to add to a list.

To remove an entry from a list, use the **no** form of this command, specifying both the list and the IP address or hostname, as it appears in the ASA configuration.

no smart-tunnel auto-signon *list* [**use-domain**] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

To display the smart tunnel auto sign-on list entries, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.

To remove an entire list of servers from the ASA configuration, use the **no** form of the command, specifying only the list.

no smart-tunnel auto-signon *list*

Syntax Description

host	Server to be identified by its host name or wildcard mask.
hostname-mask	Host name or wildcard mask to auto-authenticate to.
ip	Server to be identified by its IP address and netmask.
ip-address [*netmask*]	Sub-network of hosts to auto-authenticate to.
list	Name of a list of remote servers. Use quotation marks around the name if it includes a space. The string can be up to 64 characters. The ASA creates the list if it is not present in the configuration. Otherwise, it adds the entry to the list.
use-domain	(Optional) Add the Windows domain to the username if authentication requires it. If you enter this keyword, be sure to specify the domain name when assigning the smart tunnel list to one or more group policies, or usernames.

Defaults

No defaults exist for this command.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.

Following the population of a smart tunnel auto sign-on list, use the **smart-tunnel auto-signon enable** *list* command in group policy webvpn or username webvpn mode to assign the list.

Examples

The following command adds all hosts in the subnet and adds the Windows domain to the username if authentication requires it:

```
asa2(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56 255.255.255.0
```

The following command removes that entry from the list:

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

The command shown above also removes the list named HR if the entry removed is the only entry in the list. Otherwise, the following command removes the entire list from the ASA configuration:

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR
```

The following command adds all hosts in the domain to the smart tunnel auto sign-on list named intranet:

```
asa2(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

The following command removes that entry from the list:

```
asa2(config-webvpn)# no smart-tunnel auto-signon intranet host *.exampledomain.com
```

Related Commands

Command	Description
smart-tunnel auto-signon enable	Enables smart tunnel auto sign-on for the group policy or username specified in the command mode.
smart-tunnel auto-signon enable *list*	Assigns a smart tunnel auto sign-on list to a group policy or username
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access > Start Smart Tunnels** button on the Clientless SSL VPN portal page.

smart-tunnel auto-start

To start smart tunnel access automatically upon user login in a clientless (browser-based) SSL VPN session, use the **smart-tunnel auto-start** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel auto-start *list*

To remove the **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

list	*list* is the name of a smart tunnel list already present in the ASA webvpn configuration. To view any smart tunnel list entries already present in the SSL VPN configuration, enter the **show running-config webvpn** command in privileged EXEC mode.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command requires that you use the **smart-tunnel list** command to create the list of applications first.

This option to start smart tunnel access upon user login applies only to Windows.

Examples

The following commands start smart tunnel access for a list of applications named apps1:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
hostname(config-group-webvpn)
```

The following commands remove the list named apps1 from the group policy and inherit the smart tunnel commands from the default group policy:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the Clientless SSL VPN configuration, including all smart tunnel list entries.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel disable

To prevent smart tunnel access through clientless (browser-based) SSL VPN sessions, use the **smart-tunnel disable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel disable

To remove a **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

By default, smart tunnels are not enabled, so the **smart-tunnel disable** command is necessary only if the (default) group policy or username configuration contains a **smart-tunnel auto-start** or **smart-tunnel enable** command that you do not want applied for the group policy or username in question.

Examples

The following commands prevent smart tunnel access:

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

Related Commands

Command	Description
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel enable

To enable smart tunnel access through clientless (browser-based) SSL VPN sessions, use the **smart-tunnel enable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel enable *list*

To remove the **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

list	*list* is the name of a smart tunnel list already present in the ASA webvpn configuration. To view the smart tunnel list entries in the SSL VPN configuration, enter the **show running-config webvpn** command in privileged EXEC mode.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **smart-tunnel enable** command assigns a list of applications eligible for smart tunnel access to a group policy or username. It requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the clientless-SSL-VPN portal page. Alternatively, you can use the **smart-tunnel auto-start** command to start smart tunnel access automatically upon user login.

Both commands require that you use the **smart-tunnel list** command to create the list of applications first.

Examples

The following commands enable the smart tunnel list named apps1:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
hostname(config-group-webvpn)
```

The following commands remove the list named apps1 from the group policy and inherit the smart tunnel list from the default group policy:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the Clientless SSL VPN configuration, including all smart tunnel list entries.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel list

To populate a list of applications that can use a clientless (browser-based) SSL VPN session to connect to private sites, use the **smart-tunnel list** command in webvpn configuration mode. To remove an application from a list, use the **no** form of the command, specifying the entry. To remove an entire list of applications from the ASA configuration, use the **no** form of the command, specifying only the list.

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

no smart-tunnel list *list*

Syntax Description

application	Name of the application to be granted smart tunnel access. The string can be up to 64 characters.
hash	(Optional and applicable only for Windows) To obtain this value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at http://support.microsoft.com/kb/841290/. After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:/fciv.exe), then enter **fciv.exe -sha1** *application* at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash. The SHA-1 hash is always 40 hexadecimal characters.
list	Name of a list of applications or programs. Use quotation marks around the name if it includes a space. The CLI creates the list if it is not present in the configuration. Otherwise, it adds the entry to the list.
path	For Mac OS, the full path to the application. For Windows, the filename of the application; or a full or partial path to the application, including its filename. The string can be up to 128 characters.
platform *OS*	(Optional if the OS is Microsoft Windows) Enter **windows or mac** to specify the host of the application.

Defaults

Windows is the default platform.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	Added **platform** *OS*.

Usage Guidelines

You can configure more than one smart tunnel list on an ASA, but you cannot assign more than one smart tunnel list to a given group policy or username. To populate a smart tunnel list, enter the **smart-tunnel list** command once for each application, entering the same *list* string, but specifying an *application* and *path* that is unique for the OS. Enter the command once for each *OS* you want the list to support.

The session ignores a list entry if the OS does not match the one indicated in the entry. It also ignores an entry if the path to the application is not present.

To view the smart tunnel list entries in the SSL VPN configuration, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.

The *path* must match the one on the computer, but it does not have to be complete. For example, the *path* can consist of nothing more than the executable file and its extension.

Smart tunnels have the following requirements:

- The remote host originating the smart tunnel connection must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000; or Mac OS 10.4 or 10.5.
- Users of Microsoft Windows Vista who use smart tunnels or port forwarding must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the Tools > Internet Options > Security tab. Vista users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer’s vulnerability to attack.
- The browser must be enabled with Java, Microsoft ActiveX, or both.
- Smart tunnel support for Mac OS requires Safari 3.1.1 or later.

On Microsoft Windows, only Winsock 2, TCP-based applications are eligible for smart tunnel access.

On Mac OS, applications using TCP that are dynamically linked to the SSL library can work over a smart tunnel. The following types of applications do not work over a smart tunnel:

- Applications using dlopen or dlsym to locate libsocket calls
- Statically linked applications to locate libsocket calls
- Mac OS applications that use two-level name spaces.
- Mac OS, console-based applications, such as Telnet, SSH, and cURL.
- Mac OS, PowerPC-type applications. To determine the type of a Mac OS application, right-click its icon and select Get Info.

On Mac OS, only applications started from the portal page can establish smart tunnel sessions. This requirement includes smart tunnel support for Firefox. Using Firefox to start another instance of Firefox during the first use of a smart tunnel requires the user profile named csco_st. If this user profile is not present, the session prompts the user to create one.

The following limitations apply to smart tunnels:

- If the remote computer requires a proxy server to reach the ASA, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. In this configuration, smart tunnels support only basic authentication.
- The smart tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library on a Microsoft Windows OS. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.
- A group policy or local user policy supports no more than one list of applications eligible for smart tunnel access and one list of smart tunnel auto sign-on servers.
- A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

Note A sudden problem with smart tunnel access may be an indication that a *path* value is not up-to-date with an application upgrade. For example, the default path to an application typically changes following the acquisition of the company that produces the application and the next upgrade.

Entering a hash provides a reasonable assurance that clientless SSL VPN does not qualify an illegitimate file that matches the string you specified in the *path*. Because the checksum varies with each version or patch of an application, the *hash* you enter can only match one version or patch on the remote host. To specify a *hash* for more than one version of an application, enter the **smart-tunnel list** command once for each version, entering the same *list* string, but specifying the unique *application* string and unique *hash* value in each command.

Note You must maintain the smart tunnel list in the future if you enter *hash* values and you want to support future versions or patches of an application with smart tunnel access. A sudden problem with smart tunnel access may be an indication that the application list containing *hash* values is not up-to-date with an application upgrade. You can avoid this problem by not entering a *hash*.

Following the configuration of a smart tunnel list, use the **smart-tunnel auto-start** or **smart-tunnel enable** command to assign the list to group policies or usernames.

Examples

The following command adds the Microsoft Windows application Connect to a smart tunnel list named apps1:

```
hostname(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

The following command adds the Windows application msimn.exe and requires that the hash of the application on the remote host match the last string entered to qualify for smart tunnel access:

```
hostname(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

The following command provides smart tunnel support for the Mac OS browser Safari:

```
hostname(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

Related Commands

Command	Description
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration on the ASA.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access > Start Smart Tunnels** button on the Clientless SSL VPN portal page.

smart-tunnel network

To create a list of hosts to use for configuring smart tunnel tunnel policies, use the **smart-tunnel network** command in webvpn configuration mode. To disallow a list of hosts for smart tunnel tunnel policies, use the [no] form of this command.

smart-tunnel network

no smart-tunnel network

Syntax Description

host *host mask*	The hostname mask, such as *.cisco.com.
ip *ip address*	The IP address of a network.
netmask	The Netmask of a network.
network name	The name of the network to apply to tunnel policy.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

When the smart tunnel is turned on, you can allow traffic outside of the tunnel with the **smart-tunnel network** command, which configures the network (a set of hosts), and the **smart-tunnel tunnel-policy** command, which uses the specified smart-tunnel network to enforce a policy on a user.

Examples

The following is a sample of how the **smart-tunnel network** command is used:

```
hostname(config-webvpn)# smart-tunnel network testnet ip 192.168.0.0 255.255.255
```

Related Commands

Command	Description
smart-tunnel tunnel-policy	Uses the specified smart-tunnel network to enforce a policy on a user.

smart-tunnel tunnel-policy

To apply smart tunnel tunnel policies to a particular group or user policy, use the **smart-tunnel tunnel-policy** command in configuration webvpn mode. To unapply smart tunnel tunnel policies to a particular group, use the [no] form of this command.

smart-tunnel tunnel-policy

no smart-tunnel tunnel-policy

Syntax Description

excludespecified	Tunnels only networks that are outside of the networks specified by network name.
network name	Lists networks to be tunneled.
tunnelall	Makes everything tunneled (encrypted).
tunnelspecified	Tunnels only networks specified by network name.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.3.1	This command was introduced.

Usage Guidelines

When the smart tunnel is turned on, you can allow traffic outside of the tunnel with the **smart-tunnel network** command, which configures the network (a set of hosts), and the **smart-tunnel tunnel-policy** command, which uses the specified smart-tunnel network to enforce a policy on a user.

Examples

The following is a sample of how the **smart-tunnel tunnel-policy**command is used:

```
hostname(config-username-webvpn)# smart-tunnel tunnel-policy tunnelspecified testnet
```

Related Commands

Command	Description
smart-tunnel network	Creates a list of hosts for configuring smart tunnel policies.

smtp from-address

To specify the e-mail address to use in the E-mail From: field for all e-mails generated by the local CA server (such as distribution of one-time passwords) use the **smtp from-address** command in CA server configuration mode. To reset the e-mail address to the default, use the **no** form of this command.

smtp from-address *e-mail_address*

no smtp from-address

Syntax Description

e-mail_address	Specifies the e-mail address appearing in the From: field of all e-mails generated by the CA server.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example specifies that the From: field of all e-mails from the local CA server include ca-admin@asa1-ca.example.com:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address ca-admin@asa1-ca.example.com
hostname(config-ca-server)#
```

The following example resets the From: field of all e-mails from the local CA server to the default address admin@asa1-ca.example.com:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address admin@asa1-ca.example.com
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
smtp subject	Customizes the text to appear in the subject field of all e-mails generated by the local CA server.

smtp subject

To customize the text that appears in the subject field of all e-mails generated by the local Certificate Authority (CA) server (such as distribution of one-time passwords), use the **smtp subject** command in CA server configuration mode. To reset the text to the default, use the **no** form of this command.

smtp subject *subject-line*

no smtp subject

Syntax Description

subject-line	Specifies the text appearing in the Subj: field of all e-mails sent from the CA server. The maximum number of characters is 127.

Defaults

By default, the text in the Subj: field is “Certificate Enrollment Invitation”.

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
Ca server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example specifies that the text *Action: Enroll for a certificate* appear in the Subj: field of all e-mails from the CA server:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp subject Action: Enroll for a certificate
hostname(config-ca-server)#
```

The following example resets the Subj: field text for all e-mails from the CA server to the default text “Certificate Enrollment Invitation”:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no smtp subject
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the local CA server.

smtps

To enter SMTPS configuration mode, use the **smtps** command in global configuration mode. To remove any commands entered in SMTPS command mode, use the **no** version of this command. SMTPS is a TCP/IP protocol that lets you to send e-mail over an SSL connection.

smtps

no smtps

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to enter SMTPS configuration mode:

```
hostname(config)# smtps
hostname(config-smtps)#
```

Related Commands

Command	Description
clear configure smtps	Removes the SMTPS configuration.
show running-config smtps	Displays the running configuration for SMTPS.

smtp-server

To configure an SMTP server, use the **smtp-server** command in global configuration mode. To remove the attribute from the configuration, use the **no** form of this command.

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

Syntax Description

backup_server	Identifies a backup SMTP server to relay event messages if the primary SMTP server is unavailable. Use either an IP address or hostname (configured using the **name** command).
primary_server	Identifies the primary SMTP server. Use either an IP address or hostname (configured using the **name** command).

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The ASA includes an internal SMTP client that the Events system can use to notify external entities that a certain event has occurred. You can configure SMTP servers to receive these event notices, and then forward them to specified e-mail addresses. The SMTP facility is active only when you enable E-mail events to the ASA.

Examples

The following example shows how to set an SMTP server with an IP address of 10.1.1.24, and a backup SMTP server with an IP address of 10.1.1.34:

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp cpu threshold rising

To configure the threshold value for a high CPU threshold and the threshold monitoring period, use the **snmp cpu threshold rising** command in global configuration mode. To not configure the threshold value and threshold monitoring period, use the **no** form of this command.

snmp cpu threshold rising *threshold_value monitoring_period*

no snmp cpu threshold rising *threshold_value monitoring_period*

Syntax Description

monitoring_period	Defines the monitoring period in minutes.
threshold_value	Defines the threshold level as a percentage of CPU usage.

Defaults

If the **snmp cpu threshold rising** command is not configured, the default for the high threshold level is set at over 70 percent of CPU usage, and the default for the critical threshold level isset at over 95 percent of CPU usage. The default monitoring period is set to one minute.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	This command was introduced. Does not apply to the ASA Services Module.

Usage Guidelines

You cannot configure the critical CPU threshold level, which is maintained at a constant 95 percent. Valid threshold values range from 10 to 94 percent of CPU usage. Valid values for the monitoring period range from 1 to 60 minutes.

Examples

The following example shows how to configure the SNMP CPU threshold level to 75 percent of CPU usage and a monitoring period of 30 minutes:

```
hostname(config)# snmp cpu threshold 75% 30
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP-related traps.
snmp link threshold	Defines the SNMP interface threshold value.
snmp-server enable	Enables SNMP on the ASA.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp link threshold

To configure the threshold value for an SNMP physical interface and the threshold value for system memory usage, use the **snmp link threshold** command in global configuration mode. To clear the threshold value for an SNMP physical interface and the threshold value for system memory usage, use the **no** form of this command.

snmp link threshold *threshold_value*

no snmp link threshold *threshold_value*

Syntax Description

threshold_value	Defines the threshold value as a percentage of CPU usage.

Defaults

If you do not configure the **snmp link threshold** command, the default threshold value is 70 percent of CPU usage and system memory usage.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

Valid threshold values range from 30 to 99 percent of physical interfaces. The **snmp link threshold** command is available only in the admin context.

Examples

The following example shows how to configure the SNMP interface threshold value to 75 percent for all physical interfaces:

```
hostname(config)# snmp link threshold 75%
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP-related traps.
snmp cpu threshold rising	Defines the SNMP CPU threshold value.
snmp-server enable	Enables SNMP on the ASA.

Command	Description
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-map

To identify a specific map for defining the parameters for SNMP inspection, use the **snmp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

snmp-map *map_name*

no snmp-map *map_name*

Syntax Description

map_name	The name of the SNMP map.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **snmp-map** command to identify a specific map to use for defining the parameters for SNMP inspection. When you enter this command, the system enters the SNMP map configuration mode, which lets you enter the different commands used for defining the specific map. After defining the SNMP map, you use the **inspect snmp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface.

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enables SNMP application inspection.
policy-map	Associates a class map with specific security actions.

snmp-server community

To set the SNMP community string, use the **snmp-server community** command in global configuration mode. To remove the SNMP community string, use the **no** form of this command.

snmp-server community [*0* | *8*] *community-string*

no snmp-server community [*0* | *8*] *community-string*

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) community string will follow.
8	Specifies that an encrypted community string will follow.
community-string	Sets the SNMP community string, which is the password in encrypted or unencrypted (clear text) format. The community string can have a maximum of 32 characters.

Defaults

The default community string is “public.”

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.2(1)	The *text* argument was changed to the *community-string* argument.
8.3(1)	Support for encrypted passwords was added.

Usage Guidelines

The SNMP community string is a shared secret among the SNMP management station and the network nodes being managed. It is used only for Version 1 and 2c communication between the management station and the device. The ASA uses a key to determine whether or not the incoming SNMP request is valid.

For example, you could designate a site with a community string and then configure the routers, the ASA, and the management station with this same string. The ASA uses this string and does not respond to requests with an invalid community string.

After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible.

The encrypted community string is always generated by the ASA; you normally enter the clear text form.

Note If you downgrade from version 8.3(1) to a lower version of the ASA software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the **no key config-key password encryption** command, then save the results.

Examples

The following example sets the community string to ”onceuponatime”:

```
hostname(config)# snmp-server community onceuponatime
```

The following example sets an encrypted community string:

```
hostname(config)# snmp-server community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

The following example sets an unencrypted community string:

```
hostname(config)# snmp-server community 0 cisco
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP counters.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server contact

To set the SNMP server contact name, use the **snmp-server contact** command in global configuration mode. To remove the SNMP contact name, use the **no** form of this command.

snmp-server contact *text*

no snmp-server contact [*text*]

Syntax Description

text	Specifies the name of the contact person or the ASA system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the SNMP server contact to EmployeeA:

```
hostname(config)# snmp-server contact EmployeeA
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server enable	Enables SNMP on the ASA.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable

To enable the SNMP server on the ASA, use the **snmp-server enable** command in global configuration mode. To disable the SNMP server, use the **no** form of this command.

snmp-server enable

no snmp-server enable

Syntax Description

This command has no arguments or keywords.

Defaults

The SNMP server is enabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can enable and disable SNMP easily, without configuring and reconfiguring SNMP traps or other configuration.

Examples

The following example enables SNMP, configures the SNMP host and traps, and then sends traps as syslog messages.

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community onceuponatime
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact EmployeeB
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.

Command	Description
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable traps

To enable the ASA to send traps to the NMS, use the **snmp-server enable traps** command in global configuration mode. To disable traps, use the **no** form of this command.

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **ikev2** [*trap*] [...] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

Syntax Description

all	Enables all traps.
connection-limit-reached	Enables connection limit reached traps.
cpu threshold rising	Enables CPU threshold rising traps.
entity [*trap*]	Enables entity traps. Traps for **entity** include the following: • **config-change** • **fru-insert** • **fru-remove** • **cpu-temperature** • **fan-failure** • **power-supply** • **power-supply-failure** • **power-supply-temperature** • **chassis-temperature** • **power-supply-presence** • **chassis-fan-failure**
ipsec [*trap*]	Enables IPsec traps. Traps for **ipsec** include the following: • **start** • **stop**
ikev2 [*trap*]	Enables IKEv2 IPsec traps. Traps for **ikev2** include: • **start** • **stop**
link-threshold	Enables link threshold reached traps.
memory-threshold	Enables memory threshold reached traps.
nat [*trap*]	Enables NAT-related traps. Traps for **nat** include the following: • **packet-discard**
remote-access [*trap*]	Enables remote access traps. Traps for **remote-access** include the following: • **session-threshold-exceeded**

snmp [*trap*]	Enables SNMP traps. By default, all SNMP traps are enabled. Traps for **snmp** include the following: • **authentication** • **linkup** • **linkdown** • **coldstart** • **warmstart**
syslog	Enables syslog message traps.

Defaults

The default configuration has all **snmp** traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**). If you enter this command and do not specify a trap type, then the default is **syslog**. (The default **snmp** traps continue to be enabled along with the **syslog** trap.) All other traps are disabled by default.

You can disable these traps using the **no** form of this command with the **snmp** keyword. The **clear configure snmp-server** command restores the default enabling of SNMP traps.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(1)	The following traps have been added: **snmp warmstart**, **nat packet-discard**, **link-threshold**, **memory-threshold**, **entity power-supply**, **entity fan-failure**, **entity cpu-temperature**, **cpu threshold rising**, and **connection-limit-reached**. These traps do not apply to the ASASM.
8.6(1)	The following traps have been added to support the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X: **entity power-supply-failure**, **entity chassis-fan-failure**, **entity power-supply-presence**, **entity chassis-temperature**, and **entity power-supply-temperature**.
9.0(1)	Support for multiple context mode was added for IKEv2 and IPsec.

Usage Guidelines

To enable individual traps or sets of traps, enter this command for each feature type. To enable all traps, enter the **all** keyword.

To send traps to the NMS, enter the **logging history** command, then enable logging using the **logging enable** command.

Traps generated in the admin context only include the following:

- **connection-limit-reached**

- **entity**
- **memory-threshold**

Traps generated through the admin context only for physically connected interfaces in the system context include the following:

- **interface-threshold**

All other traps are available in the admin and user contexts.

Note In multi-mode, the **fan-failure** trap, the **power-supply-failure** trap, and the **cpu-temperature** trap are generated only from the admin context, and not the user contexts (applies only to the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X). These traps do not apply to the ASA 5505.

If the CPU usage is greater than the configured threshold value for the configured monitoring period, a **cpu threshold rising** trap is generated.

When the used system memory reaches 80 percent, the **memory-threshold** trap is generated.

Note SNMP does not monitor voltage sensors.

Examples

The following example enables SNMP, configures the SNMP host and traps, then sends traps as syslog messages:

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community onceuponatime
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact EmployeeB
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server group

To configure a new SNMP group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

no snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

Syntax Description

auth	Specifies packet authentication without encryption.
group-name	Specifies the name of the group.
noauth	Specifies no packet authentication.
priv	Specifies packet authentication with encryption.
v3	Specifies that the group is using the SNMP Version 3 security model, which is the most secure of the supported security models. This version allows you to explicitly configure authentication characteristics.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.
8.3(1)	Support for password encryption was added.

Usage Guidelines

To use the Version 3 security model, you must first configure an SNMP group, then configure an SNMP user, and then configure an SNMP host. You must also specify Version 3 and a security level. When a community string is configured internally, two groups with the name “public” are automatically created—one for the Version 1 security model and one for the Version 2c security model. When you delete a community string, both configured groups are automatically deleted.

Note A user that is configured to belong to a certain group should have the same security model as the group.

During bootup or upgrade of the ASA, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

Note If you downgrade from version 8.3(1) to a lower version of the ASA software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the **no key config-key password encryption** command, then save the results.

Examples

The following example show how the ASA can receive SNMP requests using the SNMP Version 3 security model, which includes creating a group, creating a user, and creating a host:

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP configuration counters.
snmp-server host	Sets the SNMP host address.
snmp-server user	Creates a new SNMP user.

snmp-server host

To specify the NMS that can use SNMP on the ASA, use the **snmp-server host** command in global configuration mode. To disable the NMS, use the **no** form of this command.

snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

no snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) community string will follow.
8	Specifies that an encrypted community string will follow.
community	Specifies that a non-default string is required for requests from the NMS, or when generating traps sent to the NMS. Valid only for SNMP Version 1 or 2c.
community-string	Specifies the password-like community string that is sent with the notification or in a request from the NMS. The community string can have a maximum of 32 characters. Can be in encrypted or unencrypted (clear text) format.
hostname	Specifies the SNMP notification host, which is usually an NMS or SNMP manager.
interface	Specifies the interface name through which the NMS communicates with the ASA.
ip_address	Specifies the IP address of an NMS to which SNMP traps should be sent or from which the SNMP requests come. Supports *only* IPv4 addresses.
poll	(Optional) Specifies that the host is allowed to browse (poll), but no traps can be sent.
port	Sets the UDP port number of the NMS host.
trap	(Optional) Specifies that only traps can be sent, and that this host is not allowed to browse (poll).
udp-port	(Optional) Specifies that SNMP traps must be sent to an NMS host on a non-default port.
username	Specifies the username to embed in the trap PDU that is sent to the host. Valid only for SNMP Version 3.
version {**1** | **2c** | **3**}	(Optional) Sets the SNMP notification version to use for sending traps to Version 1, 2c, or 3.

Defaults

The default UDP port is 162.

The default version is 1.

SNMP traps are enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.2(1)	• SNMP Version 3 is supported. • The *username* argument was introduced. • The *text* argument was changed to the *community-string* argument. • The *interface_name* argument was changed to the *interface* argument.
8.3(1)	Support for encrypted passwords was added.

Usage Guidelines

If you configure the **snmp-server host** command on a port that is currently in use, the following message appears:

Warning **The UDP port** *port* **is in use by another feature. SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

To use the Version 3 security model, you must configure an SNMP group first, then an SNMP user, and then an SNMP host. The username must already be configured on the device. When a device is configured as the standby unit of a failover pair, the SNMP engine ID and user configuration are replicated from the active unit. This action allows a transparent switchover from an SNMP Version 3 query perspective. No configuration changes are necessary in the NMS to accommodate a switchover event.

After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible.

The encrypted community string is always generated by the ASA; you normally enter the clear text form.

During bootup or upgrade of the ASA, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

Note If you downgrade from version 8.3(1) to a lower version of the ASA software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the **no key config-key password encryption** command, then save the results.

Examples

The following example sets the host to 192.0.2.5, which is attached to the inside interface:

```
hostname(config)# snmp-server host inside 192.0.2.5
hostname(config)# snmp-server host inside 192.0.2.5 version 3 md5aes128 udp-port 190
```

The following example show how the ASA can receive SNMP requests using the SNMP Version 3 security model, which includes creating a group, creating a user, and creating a host:

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

The following example sets the host to use an encrypted community string:

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

The following example sets the host to use an unencrypted community string:

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 0 cisco
```

Related Commands

Command	Description
clear configure snmp-server	Clears SNMP configuration counters.
snmp-server enable	Enables SNMP on the ASA.
snmp-server group	Configures a new SNMP group.
snmp-server user	Configures a new SNMP user.

snmp-server listen-port

To set the listening port for SNMP requests, use the **snmp-server listen-port** command in global configuration mode. To restore the default port, use the **no** form of the command.

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

Syntax Description

lport	The port on which incoming requests will be accepted[1].

[1] The **snmp-server listen-port** command is only available in admin context, and is not available in the system context.

Defaults

The default port is 161.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you configure the **snmp-server listen-port** command on a port that is currently in use, the following message appears:

Warning **The UDP port *port* is in use by another feature. SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

Examples

The following example sets the listening port to 192:

```
hostname(config)# snmp-server listen-port 192
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server location

To set the ASA location for SNMP, use the **snmp-server location** command in global configuration mode. To remove the location, use the **no** form of this command.

snmp-server location *text*

no snmp-server location [*text*]

Syntax Description

location *text*	Specifies the security appliance location. The **location** *text* is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the ASA location for SNMP as Building 42, Sector 54:

```
hostname(config)# snmp-server location Building 42, Sector 54
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.

snmp-server user

To configure a new SNMP user, use the **snmp-server user** command in global configuration mode. To remove a specified SNMP user, use the **no** form of this command.

snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

Syntax Description

128	(Optional) Specifies the use of the 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of the 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of the 256-bit AES algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the AES algorithm for encryption.
auth	(Optional) Specifies which authentication level should be used.
auth-password	(Optional) Specifies a string that enables the agent to receive packets from the host. The minimum length is one character; the recommended length is at least eight characters, and should include letters and numbers. The maximum length is 64 characters. You can specify a plain-text password or a localized MD5 digest. If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd, where aa, bb, and cc are hexadecimal values. The digest should be exactly 16 octets long.
des	(Optional) Specifies the use of the 56-bit DES algorithm for encryption.
encrypted	(Optional) Specifies whether or not the password appears in encrypted format. Encrypted passwords must be in hexadecimal format.
group-name	Specifies the name of the group to which the user belongs.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
priv	Specifies packet authentication with encryption.
priv-password	(Optional) Specifies a string that indicates the privacy user password. The minimum length is one character; the recommended length is at least eight characters, and should include letters and numbers. The maximum length is 64 characters. You can specify a plain-text password or a localized MD5 digest. If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd, where aa, bb, and cc are hexadecimal values. The digest should be exactly 16 octets long.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
username	Specifies the name of the user on the host that connects to the agent.
v3	Specifies that the SNMP Version 3 security model should be used. Allows the use of the **encrypted, priv,** or **auth** keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

An SNMP user must be part of an SNMP group. To use the Version 3 security model, you must first configure an SNMP group, then configure an SNMP user, and then configure an SNMP host.

Note If you forget a password, you cannot recover it, and must reconfigure the user.

When the snmp-server user configuration is displayed on the console or written to a file (for example, the startup-configuration file), the localized authentication and privacy digests always appear instead of a plain-text password. This usage is required by RFC 3414, Section 11.2.

Note You must have a 3DES or AES feature license to configure users with the 3DES or AES algorithm.

During bootup or upgrade of the ASA, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

Examples

The following example shows how the ASA can receive SNMP requests using the SNMP Version 3 security model:

```
hostname(config)# snmp-server group engineering v3 auth
hostname(config)# snmp-server user engineering v3 auth sha mypassword
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
snmp-server enable	Enables SNMP on the ASA.
snmp-server group	Creates a new SNMP group.
snmp-server host	Sets the SNMP host address.