



CHAPTER 15

Configuring Management Access

This chapter contains the following topics:

- [Configuring ASDM Access, page 15-1](#)
- [Configuring CLI Parameters, page 15-2](#)
- [Configuring the Security Appliance as a TFTP Client, page 15-6](#)
- [Configuring ICMP Access, page 15-7](#)
- [Configuring SNMP, page 15-8](#)
- [Configuring SNMP, page 15-8](#)
- [Configuring Management Access Rules, page 15-23](#)
- [Configuring AAA for System Administrators, page 15-24](#)

Configuring ASDM Access

To use ASDM, you need to enable the HTTPS server, and allow HTTPS connections to the FWSM.

The FWSM allows a maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 80 ASDM instances between all contexts. You can control the number of ASDM sessions allowed per context using resource classes. (See the “[Configuring Resource Classes](#)” section on [page 9-16](#).) To configure ASDM access to the FWSM, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > ASDM/HTTPS pane, click **Add**.
The Add HTTP Configuration dialog box appears.
 - Step 2** From the Interface Name drop-down list, choose the interface to use for ASDM access.
 - Step 3** In the IP Address field, add the IP address of the network or host that is allowed access.
 - Step 4** From the Mask drop-down list, choose the mask associated with the network or host that is allowed access.
 - Step 5** Click **OK**.
 - Step 6** Verify that the Enable HTTP Server check box is checked (this is the default setting).
 - Step 7** Click **Apply**.

The changes are saved to the running configuration.

Configuring CLI Parameters

This section includes the following topics:

- [Adding a Banner, page 15-2](#)
- [Configuring SSH Access, page 15-3](#)
- [Configuring Telnet Access, page 15-4](#)
- [Customizing a CLI Prompt, page 15-5](#)

Adding a Banner

You can configure a message to display when a user connects to the security appliance, before a user logs in, or before a user enters privileged EXEC mode.

See the following guidelines:

- From a security perspective, it is important that your banner discourage unauthorized access. Do not use the words welcome or please, as they appear to invite intruders in. The following banner sets the correct tone for unauthorized access:

```
You have logged in to a secure device. If you are not authorized to access this
device,
log out immediately or risk possible criminal consequences.
```

- See RFC 2196 for guidelines about banner messages.
- Only ASCII characters are allowed, including new line (Enter), which counts as two characters.
- Do not use tabs in the banner, because they are not preserved in the CLI version.
- There is no length limit for banners other than those for RAM and flash memory.
- You can dynamically add the hostname or domain name of the FWSM by including the strings \$(hostname) and \$(domain).
- If you configure a banner in the system configuration, you can use that banner text within a context by using the \$(system) string in the context configuration
- After a banner is added, FWSM Telnet or SSH sessions may close if:
 - There is not enough system memory available to process the banner message(s).
 - A TCP write error occurs when attempting to display banner message(s).

To add a message of the day, login, or session banner, perform the following steps:

Step 1 From the Configuration > Device Management > Management Access > Command Line (CLI) > Banner pane, add your banner text to the field for the type of banner you are creating for the CLI:

- Session (exec) banner—This banner appears when a user accesses privileged EXEC mode at the CLI.
- Login Banner—This banner appears when a user logs in to the CLI.
- Message-of-the-day (motd) Banner—This banner appears when a user first connects to the CLI.

Step 2 Click **Apply**.

The banner is added and the changes are saved to the running configuration.

Configuring SSH Access

The FWSM allows SSH connections to the FWSM for management purposes. The FWSM allows a maximum of 5 concurrent SSH connections per context, if available, with a maximum of 100 connections divided between all contexts. You can control the number of SSH sessions allowed per context using resource classes. (See the “[Configuring Resource Classes](#)” section on page 9-16.) *In the admin context only, you can have up to 15 Telnet and 15 SSH sessions concurrently.*



Note

For CLI users: note that if you have two or more concurrent Telnet or SSH sessions and one of the sessions is at the More prompt, the other sessions may hang until the More prompt is dismissed. To disable the More prompt and avoid this situation, enter the **pager lines 0** command.

SSH is an application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities. The FWSM supports the SSH remote shell functionality provided in SSH Versions 1 and 2 and supports DES and 3DES ciphers.



Note

XML management over SSL and SSH are not supported.

This section includes the following topics:

- [Configuring SSH Access, page 15-3](#)
- [Using an SSH Client, page 15-4](#)

Configuring SSH Access

To configure SSH access to the FWSM, perform the following steps:

- Step 1** From the Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH) pane, click **Add**.
- The Add Secure Shell Configuration dialog box appears.
- Step 2** From the Interface Name drop-down list, choose the interface to use for SSH access.
- Step 3** In the IP Address field, add the IP address of the network or host that is allowed access.
- Step 4** From the Mask drop-down list, choose the mask associated with the network or host that is allowed access.
- Step 5** Click **OK**.
- Step 6** From the Allowed SSH Versions drop-down list, choose **1**, **2** or **1&2**. 1&2 is the default.
- Step 7** To change the timeout value, in the Timeout field type a value in minutes. The default timeout value is 60 minutes.
- Step 8** Click **Apply**.

- Step 1** Click **OK**.
 - Step 2** From the Allowed SSH Versions drop-down list, choose **1, 2** or **1&2**. 1&2 is the default.
 - Step 3** To change the timeout value, in the Timeout field type a value in minutes. The default timeout value is 60 minutes.
 - Step 4** Click **Apply**.
The changes are saved to the running configuration.
-

Using an SSH Client

To gain access to the FWSM CLI using SSH, at the SSH client enter the username “pix” and enter the login password (see the [“Device Name/Password”](#) section on page 7-7). By default, the password is “cisco.”

When starting an SSH session, a dot (.) displays on the FWSM terminal before the SSH user authentication prompt appears, as follows:

```
hostname(config)# .
```

The display of the dot does not affect the functionality of SSH. The dot appears on the terminal when generating a server key or decrypting a message using private keys during SSH key exchange before user authentication occurs. These tasks can take up to two minutes or longer. The dot is a progress indicator that verifies that the FWSM is busy and has not hung.

Configuring Telnet Access

The FWSM allows Telnet connections to the FWSM for management purposes. You cannot use Telnet to the lowest security interface unless you use Telnet inside an IPsec tunnel (see the [“Allowing a VPN Management Connection”](#) section on page 15-5).

The FWSM allows a maximum of 5 concurrent Telnet connections per context, if available, with a maximum of 100 connections divided between all contexts. You can control the number of Telnet sessions allowed per context using resource classes. (See the [“Configuring Resource Classes”](#) section on page 9-16.) *In admin context only, you can have up to 15 Telnet and 15 SSH sessions concurrently.*



Note

For CLI users: note that if you have two or more concurrent Telnet or SSH sessions and one of the sessions is at the More prompt, the other sessions may hang until the More prompt is dismissed. To disable the More prompt and avoid this situation, enter the **pager lines 0** command.

Note that concurrent access to the FWSM is not recommended. In some cases, two Telnet sessions issuing the same commands might cause one of the sessions to hang until a key is depressed on the other session.

To configure Telnet access to the FWSM, perform the following steps:

- Step 1** From the Configuration > Device Management > Management Access > Command Line (CLI) > Telnet pane, click **Add**.
The Add Telnet Configuration dialog box appears.
- Step 2** From the Interface Name drop-down list, choose the interface to use for Telnet access.

- Step 6** To change the timeout value, in the Timeout field type a value in minutes. The default timeout value is 5 minutes.
- Step 7** Click **Apply**.
- The changes are saved to the running configuration.
-

Allowing a VPN Management Connection

The FWSM supports IPsec for management access. An IPsec VPN ensures that IP packets can safely travel over insecure networks such as the Internet. All communication between two VPN peers occurs over a secure tunnel, which means the packets are encrypted and authenticated by the peers.

The FWSM can connect to another VPN concentrator, such as a Cisco PIX firewall or a Cisco IOS router, using a site-to-site tunnel. You specify the peer networks that can communicate over the tunnel. In the case of the FWSM, the only address available on the FWSM end of the tunnel is the interface itself.

In routed mode, the FWSM can also accept connections from VPN clients, either hosts running the Cisco VPN client, or VPN concentrators such as the Cisco PIX firewall or Cisco IOS router running the Easy VPN client. Unlike a site-to-site tunnel, you do not know in advance the IP address of the client. Instead, you rely on client authentication. Transparent firewall mode does not support remote clients. Transparent mode does support site-to-site tunnels.

The FWSM can support 5 concurrent IPsec connections, with a maximum of 10 concurrent connections divided between all contexts. You can control the number of IPsec sessions allowed per context using resource classes. (See the “[Configuring Resource Classes](#)” section on page 9-16.)

You cannot configure VPN using ASDM. To configure VPN at the CLI, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide using the CLI*.

Customizing a CLI Prompt

The CLI Prompt pane lets you customize the prompt used during CLI sessions. By default, the prompt shows the hostname of the FWSM. In multiple context mode, the prompt also displays the context name. You can display the following items in the CLI prompt.

context	(Multiple mode only) Displays the name of the current context.
domain	Displays the domain name.
hostname	Displays the hostname.

priority	Displays the failover priority as pri (primary) or sec (secondary).
state	Displays the traffic-passing state of the unit. The following values are displayed for the state: <ul style="list-style-type: none"> act—Failover is enabled, and the unit is actively passing traffic. stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state. actNoFailover—Failover is not enabled, and the unit is actively passing traffic. stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit.

To customize the prompt used during CLI sessions so that it shows something other than the hostname or context name, complete the following steps:

-
- Step 1** In single mode, go to the Configuration > Device Management > Management Access > CLI Prompt pane. In multiple mode in the System, go to the Configuration > Device Management > Device Administration > CLI Prompt pane
- Step 2** , do any of the following to customize the prompt:
- To add an attribute to the prompt, click the attribute in the Available Prompts list and then click **Add**. You can add multiple attributes to the prompt. The attribute is moved from the Available Prompts list to the Selected Prompts list.
 - To remove an attribute from the prompt, click the attribute in the Selected Prompts list and then click **Delete**. The attribute is moved from the Selected Prompts list to the Available Prompts list.
 - To change the order in which the attributes appear in the command prompt, click the attribute in the Selected Prompts list and click **Move Up** or **Move Down** to change the order.
- The prompt is changed and displays in the CLI Prompt Preview field.
- Step 3** Click **Apply**.
- The new prompt is saved to the running configuration.
-

Configuring the Security Appliance as a TFTP Client

TFTP is a simple client/server file transfer protocol described in RFC783 and RFC1350 Rev. 2. You can configure the FWSM as a TFTP *client* so that it can transfer a copy of its running configuration file to a TFTP *server* using File > Save Running Configuration to TFTP Client or Tools > Command Line Interface. In this way, you can back up and propagate configuration files to multiple FWSMs.

The FWSM supports only one TFTP client. The full path to the TFTP client is specified in Configuration > Device Management > Management Access > File Access > TFTP Client. Once configured here, you can use a colon (:) to specify the IP address in the CLI **configure net** and **copy** commands. However, any other authentication or configuration of intermediate devices necessary for communication from the FWSM to the TFTP client is done apart from this function.

To configure the FWSM as a TFTP client for saving configuration files to a TFTP server, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > File Access > TFTP Client pane, check **Enable**.
 - Step 2** From the Interface Name drop-down list, choose the interface to use as a TFTP client.
 - Step 3** In the IP Address field, add the IP address of the TFTP server where configuration files will be saved.
 - Step 4** In the Path field, add the path to the TFTP server where configuration files will be saved.
For example: /tftpboot/asa/config3
 - Step 5** Click **Apply**.

The changes are saved to the running configuration. This TFTP server will be used to save the FWSM configuration files. For more information, see [Save Running Configuration to TFTP Server, page 3-3](#).

Configuring ICMP Access

By default, ICMP (including ping) is not allowed to an FWSM interface (or through the FWSM). ICMP is an important tool for testing your network connectivity; however, it can also be used to attack the FWSM or your network. We recommend allowing ICMP during your initial testing, but then disallowing it during normal operation.



Note

See the “[Rule Limits](#)” section on page A-7 for information about the maximum number of ICMP rules allowed for the entire system. For allowing ICMP traffic *through* the FWSM, see the “[Configuring Access Rules](#)” section on page 20-9.

We recommend that permission is always granted for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPsec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

If you configure ICMP rules, then the FWSM uses a first match to the ICMP traffic followed by an implicit deny all. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the FWSM discards the ICMP packet and generates a syslog message.

To configure ICMP access rules, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > ICMP pane, click **Add**.
If you want to insert a rule in the ICMP table, click the rule that the new rule will precede, and click **Insert**.
The Create ICMP Rule dialog box appears in the right-hand pane.
 - Step 2** From the ICMP Type drop-down list, choose the type of ICMP message for this rule.
[Table 15-1](#) lists the types of ICMP messages.

Table 15-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

Step 3 From the Interface selection list, choose the destination FWSM interface the rule is to be applied to.

Step 4 In the IP Address field, add a specific IP address for the host or network or click **Any Address**.

Step 5 From the Mask drop-down list, choose the network mask.

Step 6 Click **OK**.

The dialog box closes.

Step 7 Click **Apply**.

The ICMP rule is added to the end of the ICMP table and the change is saved to the running configuration.

Configuring SNMP

This section describes how to configure SNMP, and includes the following topics:

- [Information About SNMP, page 15-9](#)
- [SNMP Overview, page 15-10](#)
- [Configuring an SNMP Agent and Management Station, page 15-21](#)
- [Configuring SNMP Traps, page 15-22](#)

Information About SNMP

The Simple Network Management Protocol (SNMP) enables the monitoring of network devices from a central location. The FWSM supports network monitoring using SNMP Versions 1 and 2c, as well as traps and SNMP read access, but does not support SNMP write access.

You can configure the FWSM to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the security appliance. Use CiscoWorks for Windows or any other SNMP V1, MIB-II-compliant browser to receive SNMP traps and browse a MIB.

The FWSM has an SNMP agent that notifies designated management stations if events occur that are pre-defined to require a notification, for example, when a link in the network goes up or down. The notification it sends includes an SNMP OID, identifying itself to the management stations.

The FWSM SNMP agent also replies when a management station asks for information.

This section includes the following topics:

- [Information About SNMP Terminology, page 15-9](#)
- [Information About the Management Information Base and Traps, page 15-10](#)

Information About SNMP Terminology

The following terms are commonly used when working with SNMP:

Term	Description
Management stations	The PCs or workstations set up to monitor SNMP events and manage devices such as the FWSM.
SNMP Agent	The SNMP server running on the FWSM. The agent responds to requests for information and actions from the management station. The agent also controls access to the its management information base (MIB), the collection of objects that can be viewed or changed by the SNMP manager.
OID	The system object identifier (OID) that identifies a device to its a management station and indicates to users the source of information monitored and displayed.
MIB	Management Information Bases, or standardized data structures, for collecting information about packets, connections, buffers, failovers, and so on. MIBs are defined by product and the protocols and hardware standards used by most network devices. SNMP management stations can browse MIBs and request specific data or events be sent as they occur. Some MIB data can be modified for administrative purposes.
Trap	Predefined events that generate a message from the SNMP agent to the management station. Events include alarm conditions such as link up, link down, or syslog event.
Browsing	Monitoring the health of a device from the management station by pulling required information from the device SNMP agent. This activity may include doing an snmpget or snmpwalk of the MIB tree from the management station.

Information About the Management Information Base and Traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. A trap reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. Standard traps are compiled into the FWSM software.

If needed, you can also download RFCs, standard MIBs, and standard traps from the IETF website: <http://www.ietf.org/>

Download Cisco MIBs from the following website: <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Download Cisco OIDs from the following location: <ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz>.

SNMP Overview

The FWSM provides support for network monitoring using SNMP V1 and V2c. The FWSM supports traps and SNMP read access, but does not support SNMP write access.

You can configure the FWSM to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the FWSM. MIBs are a collection of definitions, and the FWSM maintains a database of values for each definition. Browsing a MIB entails issuing an SNMP get request from the NMS. Use CiscoWorks for Windows or any other SNMP v1 or v2c, MIB-II-compliant browser to receive SNMP traps and browse a MIB.

Table 15-2 lists supported MIBs and traps for the FWSM and, in multiple mode, for each context. After you download the MIBs, compile them for your NMS.



Note

Limit the frequency of using SNMP to obtain data, because it might degrade performance. In addition, to collect resource usage data efficiently, schedule polling on a per-context basis.

Table 15-2 SNMP MIB and Trap Support

MIB and Trap	Description
CISCO-CRYPTO-ACCELERATOR-MIB	The FWSM supports browsing of the MIB.
<ul style="list-style-type: none"> • CISCO-ENTITY-MIB • CISCO-ENTITY-ALARM-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-ENTITY-REDUNDANCY-MIB 	<p>The FWSM supports browsing of the following groups and tables:</p> <ul style="list-style-type: none"> • entLogicalTable • entPhysicalTable <p>The FWSM sends the following traps:</p> <ul style="list-style-type: none"> • alarm-asserted • alarm-cleared • config-change • fru-insert • fru-remove • redun-switchover

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB	<p>The FWSM supports browsing of the following tables:</p> <ul style="list-style-type: none"> • cippfIpProfileTable • cippfIpFilterExtTable • cippfIpFilterStatsTable • cippfIpFilterTable <p>The following example shows how to retrieve entries displayed from the show access-list command through SNMP operations on the cippfIpfilterTable and cippfIpfilterStatsTable objects.</p> <pre> ! interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! hostname# show access-list access-list aaa line 1 extended permit tcp any any eq www (hitcnt=0) 0xe0998155 snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 returns as SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.3.97.97.97 = INTEGER: 2 <<<< 2 means extended access-list SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.1.1 = STRING: "aaa" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.2.1 = STRING: "aaa" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.1.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.2.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes src network SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes src network mask SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes dest network SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes dest network mask SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.3.97.97.97.1 = INTEGER: 6 <-- 6 stands for tcp protocol number SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.3.97.97.97.1 = Gauge32: 0 <-0 means any port SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.3.97.97.97.1 = Gauge32: 0 <-0 means any port. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.3.97.97.97.1 = Gauge32: 80 <- www translates to 80 </pre>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.3.97.97.97.1 = Gauge32: 0 <- 0 means any port. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.3.97.97.97.1 = INTEGER: 2 <- 2 means log for ACL is disabled. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.3.97.97.97.1 = INTEGER: 1 <- 1 means ACL log enabled. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.3.97.97.97.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.3.97.97.97.1 = Counter64: 0 <<<< 0 is current ACL hit counter for ACL 'aaa' where "3.97.97.97" denotes the access-list name in ASCII characters. The access-list name "aaa" translates to 97.97.97, where "97" is the ASCII equivalent of the character "a." The "3" denotes the number of characters in the ASCII list name. The following example shows an unexpanded access-list with a network object-group, which can be retrieved through SNMP operations. The hit counter for individual access-lists is aggregated and displayed in the SNMP OID "cippfIpFilterHits." ! interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! object-group network src-network network-object 50.1.1.1 255.255.255.255 network-object 50.1.1.2 255.255.255.255 network-object 50.1.1.3 255.255.255.255 object-group network dest-network network-object 60.1.1.1 255.255.255.255 network-object 60.1.1.2 255.255.255.255 network-object 60.1.1.3 255.255.255.255 access-list aaa extended permit tcp object-group src-network object-group dest-network ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! hostname(config)# show access-list </pre>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> access-list mode auto-commit access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list aaa; 9 elements access-list aaa line 1 extended permit tcp object-group src-network object-group dest-network 0x705bc913 <---- only exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.1 (hitcnt=0) 0xcb224dc0 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.2 (hitcnt=0) 0x324aa638 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.3 (hitcnt=0) 0xca52e993 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.1 (hitcnt=0) 0xa45db454 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.2 (hitcnt=0) 0xd69df47f <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.3 (hitcnt=0) 0xb06956a6 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.1 (hitcnt=0) 0xcd7aeba4 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.2 (hitcnt=0) 0x3210272d <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.3 (hitcnt=0) 0xa2b03187 <---- not exposed snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 SNMPv2-SMI::enterprises.9.9.278.1.1.1.2.3.97.97.97 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.3.97.97.97.1 = INTEGER: 6 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.3.97.97.97.1 = STRING: "src-network" <--- source network object group name SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.3.97.97.97.1 = STRING: "dest-network" <-- destination network object-group name.. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.3.97.97.97.1 = "" </pre>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.3.97.97.97.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.3.97.97.97.1 = Counter64: 0 <-- aggregated ACL hit counter The following example shows access-list entries displayed in the show ipv6 access-list command can be retrieved and displayed through SNMP operations. interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ipv6 address 2000:400:3:1::100/64 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ipv6 address 2001:400:3:1::100/64 ! ! ipv6 access-list allow_ipv6 permit tcp any any eq www ! access-group allow_ipv6 in interface inside access-group allow_ipv6 in interface outside ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! FWSM# show ipv6 access-list ipv6 access-list allow_ipv6; 1 elements ipv6 access-list allow_ipv6 line 1 permit tcp any any eq www (hitcnt=0) 0xfabbd56 snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 returns as SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.10.97.108.108.111.119.9 5.105.112.118.54 = INTEGER: 3 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.1.3 = STRING: "allow_ipv6" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.2.3 = STRING: "allow_ipv6" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.1.3 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.2.3 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 95.105.112.118.54.1 = Gauge32: 0 </pre>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 6 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.10.97.108.108.111.119. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.10.97.108.108.111.119. 95.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.10.97.108.108.111.119. 95.105.112.118.54.1 = Gauge32: 80 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.10.97.108.108.111.119. 95.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.10.97.108.108.111.119. 95.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.10.97.108.108.111.119. 95.105.112.118.54.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.10.97.108.108.111.119.9 5.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.10.97.108.108.111.119.9 5.105.112.118.54.1 = Counter64: 0 </pre> <p>Note You cannot perform an SNMP query for either type of access-list.</p> <p>You cannot perform an SNMP query for access-list entries expanded because of the use of an object-group. You can only perform an SNMP query for unexpanded access-lists using an object-group. You can only perform an SNMP query for an aggregated access-list hit counter for an access-list using an object-group. You cannot perform an SNMP query for the hit counter for access-list entries expanded because of an object-group in an access-list.</p> <p>You cannot perform an SNMP query for access-list names configured with more than 112 characters.</p>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-FIREWALL-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following group:</p> <ul style="list-style-type: none"> • cfwSystem <p>The information in cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context.</p> <p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> • cfwConnectionStatTable
CISCO-IPSEC-FLOW-MONITOR-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM sends the following traps:</p> <ul style="list-style-type: none"> • start • stop
CISCO-L4L7-RESOURCE-LIMIT-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following traps:</p> <ul style="list-style-type: none"> • limit-reached • rate-limit-reached <p>The FWSM supports browsing of the following tables:</p> <ul style="list-style-type: none"> • ciscoL4L7ResourceLimitTable • ciscoL4L7ResourceRateLimitTable
CISCO-MEMORY-POOL-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> • ciscoMemoryPoolTable—The memory usage described in this table applies only to the Cisco ASA general-purpose processor, and not to the network processors.
CISCO-NAT-EXT-MIB	<p>The FWSM supports browsing of the MIB.</p>
CISCO-PROCESS-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> • cpmCPUTotalTable <p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> • rising threshold
CISCO-REMOTE-ACCESS-MONITOR-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> • session-threshold-exceeded
CISCO-SYSLOG-MIB	<p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> • clogMessageGenerated <p>You cannot browse this MIB.</p>

Table 15-2 *SNMP MIB and Trap Support (continued)*

MIB and Trap	Description
CISCO-UNIFIED-FIREWALL-MIB	The FWSM supports browsing of the MIB. The FWSM supports browsing of the following group: <ul style="list-style-type: none">• <code>cufwUrlFilterGlobals</code>—This group provides global URL filtering statistics.
IF-MIB	The FWSM supports browsing of the following tables: <ul style="list-style-type: none">• <code>ifTable</code>• <code>ifXTable</code>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
IP-FORWARD-MIB	<p>The FWSM supports browsing of the following table: inetCidrRouteTable.</p> <p>The following example shows how entries displayed from the show route command can be retrieved through SNMP operations.</p> <pre> ! interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! hostname# show route 50.0.0.0 255.0.0.0 is directly connected, inside 60.0.0.0 255.0.0.0 is directly connected, outside </pre> <p>An SNMP request from the inetCidrRouteTable returns:</p> <pre> snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.2.1.4.24.7 returns IP-MIB::ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1 <---- ifindex IP-MIB::ip.24.7.1.7.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2 <---- Inindex IP-MIB::ip.24.7.1.8.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 3 <---- refer local IP-MIB::ip.24.7.1.8.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 3 <---- refer local IP-MIB::ip.24.7.1.9.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2 <---- 2 means local or connected route IP-MIB::ip.24.7.1.9.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2 <---- 2 means local or connected route IP-MIB::ip.24.7.1.10.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.10.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.11.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.11.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.12.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 0 <--- primary metric 0 for connected route IP-MIB::ip.24.7.1.12.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 0 <--- primary metric 0 for connected route IP-MIB::ip.24.7.1.13.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.13.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.14.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.14.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.15.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.15.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.16.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.16.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.17.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1 <----- 1 means route is active IP-MIB::ip.24.7.1.17.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1 <----- 1 means route is active </pre>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
IP-FORWARD-MIB (Continued)	<p>For an SNMP request to retrieve the SNMP OID "inetCidrRouteIfIndex" from the inetCidrRouteTable, enter the following:</p> <pre>snmpget 60.0.0.2 -c public -v 2c ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 returns as IP-MIB::ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1</pre> <p>Note You cannot perform an SNMP query for IPv6 route entries.</p> <p>Up to a three-minute delay may occur between route entries displayed in the show route command, and you can perform an SNMP query for this entry.</p>

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
IP-MIB	<p>The FWSM supports browsing of the following table: ipNetToPhysicalTable</p> <p>The following examples show how entries displayed through the show arp command can be retrieved through SNMP operations.</p> <pre>interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 !</pre> <pre>hostname# show arp inside 50.0.0.1 0004.23b3.9dea outside 60.0.0.1 000e.0c4e.f6cc</pre> <p>For an SNMP request from the ipNetToPhysicalTable, enter the following:</p> <pre>snmpwalk 60.0.0.2 -c public -v 2c IP-MIB::ip.35 returns</pre> <pre>IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 = Hex-STRING: 00 04 23 B3 9D EA IP-MIB::ip.35.1.4.2.1.4.60.0.0.1 = Hex-STRING: 00 0E 0C 4E F6 CC</pre> <p>For an SNMP request for a specific IP address from the ipNetToPhysicalTable, enter the following:</p> <pre>snmpwalk 60.0.0.2 -c public -v 2c IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 returns</pre> <pre>IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 = Hex-STRING: 00 04 23 B3 9D EA</pre> <p>The ipNetToPhysicalTable object is indexed by ipNetToPhysicalIfIndex, ipNetToPhysicalNetAddressType, and ipNetToPhysicalNetAddress, in which ipNetToPhysicalIfIndex will be the VLAN interface number. The ipNetToPhysicalNetAddress object is the IP address for which the MAC entry is to be retrieved. Only the ipNetToPhysicalPhysAddress object is populated from ipNetToPhysicalTable to retrieve the MAC address for the indexed IP address.</p> <p>Note Up to a three-minute delay may occur between ARP entries displayed in the show arp command, and you can perform an SNMP query for this entry.</p>
MIB-II	<p>The FWSM supports browsing of the following group and table:</p> <ul style="list-style-type: none"> • system

Table 15-2 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
NAT-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> packet-discard <p>The FWSM supports browsing of the following tables:</p> <ul style="list-style-type: none"> natAddrBindTable natAddrPortBindTable
RFC1213-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> ip.ipAddrTable
SNMP core traps	<p>The FWSM sends the following SNMP core traps:</p> <ul style="list-style-type: none"> authentication—An SNMP request fails because the NMS did not authenticate with the correct community string. linkup—An interface has transitioned to the “up” state. linkdown—An interface is down, for example, if you removed the nameif command. coldstart—The FWSM is running after a reload.
SNMPv2-MIB	<p>The FWSM supports browsing of the following:</p> <ul style="list-style-type: none"> snmp
TCP-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> tcpConnectionTable
UDP-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> udpEndpointTable

Configuring an SNMP Agent and Management Station

This section includes the following topics:

- [Configuring the SNMP Agent, page 15-21](#)
- [Adding an SNMP Management Station, page 15-22](#)

Configuring the SNMP Agent

To configure an SNMP agent, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > SNMP pane, in the Community String (default) field, add a default community string.
- Step 2** Enter the password used by the SNMP management stations when sending requests to the FWSM. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The FWSM uses the password to determine if the incoming SNMP request is

valid. The password is a case-sensitive value up to 32 characters in length. Spaces are not permitted. The default is "public." SNMPv2c allows separate community strings to be set for each management station. If no community string is configured for any management station, the value set here will be used by default.

- Step 3** In the Contact field, add the name of the FWSM system administrator. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- Step 4** In the Location field, add the location of the FWSM being managed by SNMP. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- Step 5** In the Listening Port field, add the number of the FWSM port that listens for SNMP requests from management stations; or keep the default, port number 161.
- Step 6** Click **Apply**.

The SNMP agent is configured and the changes are saved to the running configuration.

Adding an SNMP Management Station

To add an SNMP management station, perform the following steps:

- Step 1** From the Configuration > Device Management > Management Access > SNMP pane, click **Add**.
The Add SNMP Host Access Entry dialog box appears.
 - Step 2** From the Interface Name drop-down menu, choose the interface where the SNMP host resides.
 - Step 3** In the IP Address field, add the SNMP host IP address.
 - Step 4** In the UDP Port field, add the SNMP host UDP port, or keep the default, port 162.
 - Step 5** In the Community String field, add the SNMP host community string. If no community string is specified for a management station, the value set in Community String (default) field on the SNMP pane will be used.
 - Step 6** From the SNMP Version drop-down menu, choose the SNMP version used by the SNMP host.
 - Step 7** Check the Poll or Trap check boxes to specify the method for communicating with this management station.
 - Step 8** Click **OK**.
The dialog box closes.
 - Step 9** Click **Apply**.
The management station is configured and changes are saved to the running configuration.
-

Configuring SNMP Traps

To designate which traps the SNMP agent generates and how they are collected and sent to network management stations, perform the following steps:

- Step 1** From the Configuration > Device Management > Management Access > SNMP pane, click **Configure Traps**.

- The SNMP Trap Configuration dialog box appears.
- Step 2** Click the SNMP events to notify through SNMP traps.
- Step 3** Click **OK**.
- The dialog box closes.
- Step 4** Click **Apply**.
- The SNMP traps are configured and the changes are saved to the running configuration.
-

Configuring Management Access Rules

Access Rules specifically permit or deny traffic to or from a particular peer (or peers) while Management Access Rules provide access control for to-the-box traffic. For example, in addition to detecting IKE Denial of Service attacks, you can block them using management access rules.

To add a Management Access Rule, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > Management Access Rules pane, from the Add menu, click **Add Management Access Rule**.
- The Add Management Access Rules dialog box appears.
- Step 2** From the Interface drop-down list, choose an interface for applying the rule.
- Step 3** In the Action field, click one of the following:
- **Permit** (permits this traffic)
 - **Deny** (denies this traffic)
- Step 4** In the Source field, choose Any, or click the ellipsis (...) to browse for an address.
- Step 5** In the Service field, add a service name for the rule traffic, or click the ellipsis (...) to browse for a service.
- Step 6** (Optional) In the Description field, add a description for this management access rule.
- Step 7** (Optional) If you want to receive log messages for this management access rule, check **Enable Logging** and then from the Logging Level drop-down list, choose the level of logging to apply to this rule.
- Step 8** (Optional) To configure advanced options, click **More Options**. You can configure the following settings:
- If you want to turn off this Management Access Rule, uncheck **Enable Rule**.
 - To add a source service in the Source Service field; or click the ellipsis (...) to browse for a source service.

The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
 - To configure the logging interval (if you enable logging and choose a non-default setting), enter a value in seconds in the Logging Interval field.
 - To select a predefined time range for this rule, from the Time Range drop-down list, choose a time range; or click the ellipsis (...) to browse for a time range.

The Add Time Range dialog box appears. For information about adding a time range, see [Configuring Time Ranges, page 19-13](#).

- Step 9** Click **OK**.
The dialog box closes and the Management Access rule is added.
- Step 10** Click **Apply**.
The rule is saved in the running configuration.
-

Configuring AAA for System Administrators

This section describes how to enable authentication and command authorization for system administrators. Before you configure AAA for system administrators, first configure the local database or AAA server according to the [“Adding a User Account”](#) section on page 14-14 or the [“Configuring AAA Server Groups”](#) section on page 14-7.

This section includes the following topics:

- [Configuring Authentication for CLI, ASDM, and enable command Access, page 15-24](#)
- [Configuring Command Authorization, page 15-25](#)
- [Configuring Management Access Accounting, page 15-33](#)
- [Recovering from a Lockout, page 15-34](#)

Configuring Authentication for CLI, ASDM, and enable command Access

If you enable CLI authentication, the FWSM prompts you for your username and password to log in. After you enter your information, you have access to user EXEC mode.

To enter privileged EXEC mode, enter the **enable** command or the **login** command (if you are using the local database only).

If you configure **enable** authentication, the FWSM prompts you for your username and password. If you do not configure **enable** authentication, enter the system enable password when you enter the **enable** command (set by the **enable password** command). However, if you do not use **enable** authentication, after you enter the **enable** command, you are no longer logged in as a particular user. To maintain your username, use **enable** authentication.

For authentication using the local database, you can use the **login** command, which maintains the username but requires no configuration to turn on authentication.



Note

Before the FWSM can authenticate a Telnet, SSH, or HTTP user, you must first configure access to the FWSM according to the [“Secure Shell”](#) section on page 13-4, [“Telnet”](#) section on page 13-6, or [“Configuring ASDM Access”](#) section on page 15-1. These panes identify the IP addresses that are allowed to communicate with the FWSM.

To configure CLI, ASDM, or **enable** authentication, perform the following steps:

- Step 1** To authenticate users who use the **enable** command, go to Configuration > Device Management > Users/AAA > AAA Access > Authentication, and configure the following settings:
- a. Check the **Enable** check box.

- b. From the Server Group drop-down list, choose a server group name or the LOCAL database.
 - c. (Optional) If you chose a AAA server, you can configure the FWSM to use the local database as a fallback method if the AAA server is unavailable. Click the **Use LOCAL when server group fails** check box. We recommend that you use the same username and password in the local database as the AAA server because the FWSM prompt does not give any indication which method is being used.
- Step 2** To authenticate users who access the CLI or ASDM, go to Configuration > Device Management > Users/AAA > AAA Access > Authentication, and configure the following settings:
- a. Check one or more of the following check boxes:
 - **HTTP/ASDM**—Authenticates the ASDM client that accesses the FWSM using HTTPS. You only need to configure HTTP authentication if you want to use a AAA server. By default, ASDM uses the local database for authentication even if you do not configure this command. HTTP management authentication does not support the SDI protocol for a AAA server group.
 - **SSH**—Authenticates users who access the FWSM using SSH.
 - **Telnet**—Authenticates users who access the FWSM using Telnet.
 - b. For each service that you checked, from the Server Group drop-down list, choose a server group name or the LOCAL database.
 - c. (Optional) If you chose a AAA server, you can configure the FWSM to use the local database as a fallback method if the AAA server is unavailable. Click the **Use LOCAL when server group fails** check box. We recommend that you use the same username and password in the local database as the AAA server because the FWSM prompt does not give any indication which method is being used.
- Step 3** Click **Apply**.
-

Configuring Command Authorization

If you want to control the access to commands, the FWSM lets you configure command authorization, where you can determine which commands that are available to a user. By default when you log in, you can access user EXEC mode, which offers only minimal commands. When you enter the **enable** command (or the **login** command when you use the local database), you can access privileged EXEC mode and advanced commands, including configuration commands.

This section includes the following topics:

- [Command Authorization Overview, page 15-25](#)
- [Configuring Local Command Authorization, page 15-27](#)
- [Configuring TACACS+ Command Authorization, page 15-29](#)

Command Authorization Overview

This section describes command authorization, and includes the following topics:

- [Supported Command Authorization Methods, page 15-26](#)
- [About Preserving User Credentials, page 15-26](#)
- [Security Contexts and Command Authorization, page 15-27](#)

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the FWSM. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the FWSM places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user's privilege level and below. Note that all users access user EXEC mode when they first log in (commands at level 0 or 1). The user needs to authenticate again with the **enable** command to access privileged EXEC mode (commands at level 2 or higher), or they can log in with the **login** command (local database only).



Note

You can use local command authorization without any users in the local database and without CLI or **enable** authentication. Instead, when you enter the **enable** command, you enter the system enable password, and the FWSM places you in level 15. You can then create enable passwords for every level, so that when you enter **enable n** (2 to 15), the FWSM places you in level *n*. These levels are not used unless you turn on local command authorization (see [“Configuring Local Command Authorization”](#) below). (See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for more information about **enable**.)

- TACACS+ server privilege levels—On the TACACS+ server, configure the commands that a user or group can use after they authenticate for CLI access. Every command that a user enters at the CLI is checked with the TACACS+ server.

About Preserving User Credentials

When a user logs into the FWSM, they are required to provide a username and password for authentication. The FWSM retains these session credentials in case further authentication is needed later in the session.

When the following configurations are in place, a user needs only to authenticate with the local server upon login. Subsequent serial authorization uses the saved credentials. The user is also prompted for the privilege level 15 password. When exiting privileged mode, the user is authenticated again. User credentials are not retained in privileged mode.

- Local server is configured to authenticate user access.
- Privilege level 15 command access is configured to require a password.
- User's account is configured for serial only authorization (no access to console or ASDM).
- User's account is configured for privilege level 15 command access.

The following table shows how credentials are used in this case by the FWSM.

Credentials required	Username and Password Authentication	Serial Authorization	Privileged Mode Command Authorization	Privileged Mode Exit Authorization
Username	Yes	No	No	Yes
Password	Yes	No	No	Yes
Privileged Mode Password	No	No	Yes	No

Security Contexts and Command Authorization

The following are important points to consider when implementing command authorization with multiple security contexts:

- AAA settings are discrete per context, not shared between contexts.

When configuring command authorization, you must configure each security context separately. This provides you the opportunity to enforce different command authorizations for different security contexts.

When switching between security contexts, administrators should be aware that the commands permitted for the username specified when they login may be different in the new context session or that command authorization may not be configured at all in the new context. Failure to understand that command authorizations may differ between security contexts could confuse an administrator. This behavior is further complicated by the next point.

- New context sessions started with the **changeto** command always use the default “enable_15” username as the administrator identity, regardless of what username was used in the previous context session. This behavior can lead to confusion if command authorization is not configured for the enable_15 user or if authorizations are different for the enable_15 user than for the user in the previous context session.

This behavior also affects command accounting, which is useful only if you can accurately associate each command that is issued with a particular administrator. Because all administrators with permission to use the **changeto** command can use the enable_15 username in other contexts, command accounting records may not readily identify who was logged in as the enable_15 username. If you use different accounting servers for each context, tracking who was using the enable_15 username requires correlating the data from several servers.

When configuring command authorization, consider the following:

- An administrator with permission to use the **changeto** command effectively has permission to use all commands permitted to the enable_15 user in each of the other contexts.
- If you intend to authorize commands differently per context, ensure that in each context the enable_15 username is denied use of commands that are also denied to administrators who are permitted use of the **changeto** command.

When switching between security contexts, administrators can exit privileged EXEC mode and enter the **enable** command again to use the username they need.



Note

The system execution space does not support AAA commands; therefore, command authorization is not available in the system execution space.

Configuring Local Command Authorization

Local command authorization lets you assign commands to one of 16 privilege levels (0 to 15). By default, each command is assigned either to privilege level 0 or 15. You can define each user to be at a specific privilege level, and each user can enter any command at their privilege level or below. The FWSM supports user privilege levels defined in the local database, a RADIUS server, or an LDAP server (if you map LDAP attributes to RADIUS attributes. See the “[Configuring LDAP Attribute Maps](#)” section on page 14-15.)

This section includes the following topics:

- [Local Command Authorization Prerequisites, page 15-28](#)

- [Default Command Privilege Levels, page 15-28](#)
- [Assigning Privilege Levels to Commands and Enabling Authorization, page 15-29](#)

Local Command Authorization Prerequisites

Complete the following tasks as part of your command authorization configuration:

- Configure **enable** authentication. (See the [“Configuring Authentication for CLI, ASDM, and enable command Access”](#) section on page 15-24.)

enable authentication is essential to maintain the username after the user accesses the **enable** command.

Alternatively, you can use the **login** command (which is the same as the **enable** command with authentication; for the local database only), which requires no configuration. We do not recommend this option because it is not as secure as **enable** authentication.

You can also use CLI authentication, but it is not required.

- See the following prerequisites for each user type:
 - Local database users—Configure each user in the local database at a privilege level from 0 to 15. To configure the local database, see the [“Adding a User Account”](#) section on page 14-14.
 - RADIUS users—Configure the user with Cisco VSA CVPN3000-Privilege-Level with a value between 0 and 15.
 - LDAP users—Configure the user with a privilege level between 0 and 15, and then map the LDAP attribute to Cisco VAS CVPN3000-Privilege-Level according to the [“Configuring LDAP Attribute Maps”](#) section on page 14-15.

Default Command Privilege Levels

By default, the following commands are assigned to privilege level 0. All other commands are at level 15.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

If you move any configure mode commands to a lower level than 15, be sure to move the **configure** command to that level as well, otherwise, the user will not be able to enter configuration mode.

Assigning Privilege Levels to Commands and Enabling Authorization

To assign a command to a new privilege level, and enable authorization, follow these steps:

-
- Step 1** To enable command authorization, go to Configuration > Device Management > Users/AAA > AAA Access > Authorization, and check **Enable authorization for command access > Enable**.
- Step 2** From the Server Group drop-down list, choose **LOCAL**.
- Step 3** When you enable local command authorization, you have the option of manually assigning privilege levels to individual commands or groups of commands or enabling the predefined user account privileges.
- To use predefined user account privileges, click **Set ASDM Defined User Roles**.
The ASDM Defined User Roles Setup dialog box shows the commands and their levels. Click **Yes** to use the predefined user account privileges: Admin (privilege level 15, with full access to all CLI commands; Read Only (privilege level 5, with read-only access); and Monitor Only (privilege level 3, with access to the Monitoring section only).
 - To manually configure command levels, click **Configure Command Privileges**.
The Command Privileges Setup dialog box appears. You can view all commands by choosing **--All Modes--** from the Command Mode drop-down list, or you can choose a configuration mode to view the commands available in that mode. For example, if you choose **context**, you can view all commands available in context configuration mode. If a command can be entered in user EXEC/privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately.
The Variant column displays show, clear, or cmd. You can set the privilege only for the show, clear, or configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the **show** or **clear** prefix) or as the **no** form.
To change the level of a command, double-click it or click **Edit**. You can set the level between 0 and 15. You can only configure the privilege level of the *main* command. For example, you can configure the level of all **aaa** commands, but not the level of the **aaa authentication** command and the **aaa authorization** command separately.
To change the level of all shown commands, click **Select All** and then **Edit**.
Click **OK** to accept your changes.
- Step 4** To support administrative user privilege levels from RADIUS, check **Perform authorization for exec shell access > Enable**.
Without this option, the FWSM only supports privilege levels for local database users and defaults all other types of users to level 15.
This option also enables management authorization for local, RADIUS, LDAP (mapped), and TACACS+ users..
- Step 5** Click **Apply**.
-

Configuring TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the FWSM sends the command and username to the TACACS+ server to determine if the command is authorized.

When configuring command authorization with a TACACS+ server, do not save your configuration until you are sure it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the FWSM. If you still get locked out, see the [“Recovering from a Lockout” section on page 15-34](#).

Be sure that your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the FWSM. For example, in your TACACS+ server pool, include one server connected to interface 1, and another to interface 2. You can also configure local command authorization as a fallback method if the TACACS+ server is unavailable. In this case, you need to configure local users and command privilege levels according to the [“Configuring Command Authorization” section on page 15-25](#).

This section includes the following topics:

- [TACACS+ Command Authorization Prerequisites, page 15-30](#)
- [Configuring Commands on the TACACS+ Server, page 15-30](#)
- [Enabling TACACS+ Command Authorization, page 15-33](#)

TACACS+ Command Authorization Prerequisites

Configure CLI and **enable** authentication (see the [“Configuring Authentication for CLI, ASDM, and enable command Access” section on page 15-24](#)).

Configuring Commands on the TACACS+ Server

You can configure commands on a Cisco Secure Access Control Server (ACS) TACACS+ server as a shared profile component, for a group, or for individual users. For third-party TACACS+ servers, see your server documentation for more information about command authorization support.

See the following guidelines for configuring commands in Cisco Secure ACS Version 3.1; many of these guidelines also apply to third-party servers:

- The FWSM sends the commands to be authorized as “shell” commands, so configure the commands on the TACACS+ server as shell commands.



Note Cisco Secure ACS might include a command type called “pix-shell.” Do not use this type for FWSM command authorization.

- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by **permit** or **deny**.

For example, to allow the **show running-configuration aaa-server** command, add **show running-configuration** to the command box, and type **permit aaa-server** in the arguments box.

- You can permit all arguments of a command that you do not explicitly deny by selecting the **Permit Unmatched Args** check box.

For example, you can configure just the **show** command, and then all the **show** commands are allowed. We recommend using this method so that you do not have to anticipate every variant of a command, including abbreviations and **?**, which shows CLI usage (see [Figure 15-1](#)).

Figure 15-1 *Permitting All Related Commands*

The screenshot shows a configuration window with a 'Commands' box containing the text 'show'. To the right, there is a 'Permit Unmatched Args' checkbox which is checked. Below these boxes is an empty text input field and two buttons: 'Add Command' and 'Remove Command'. A vertical ID number '114412' is located on the right side of the window.

- For commands that are a single word, you *must* permit unmatched arguments, even if there are no arguments for the command, for example **enable** or **help** (see [Figure 15-2](#)).

Figure 15-2 *Permitting Single Word Commands*

The screenshot shows a configuration window with a 'Commands' box containing the text 'enable'. To the right, there is a 'Permit Unmatched Args' checkbox which is checked. Below these boxes is an empty text input field and two buttons: 'Add Command' and 'Remove Command'. A vertical ID number '114411' is located on the right side of the window.

- To disallow some arguments, enter the arguments preceded by **deny**.
For example, to allow **enable**, but not **enable password**, enter **enable** in the commands box, and **deny password** in the arguments box. Be sure to select the Permit Unmatched Args check box so that **enable** alone is still allowed (see [Figure 15-3](#)).

Figure 15-3 Disallowing Arguments

The screenshot shows a configuration window with two panes. The left pane has 'enable' selected. The right pane contains 'deny password' and a checked checkbox labeled 'Permit Unmatched Args'. Below the panes is an empty text input field and two buttons: 'Add Command' and 'Remove Command'. A vertical label '114410' is on the right side.

- When you abbreviate a command at the command line, the FWSM expands the prefix and main command to the full text, but it sends additional arguments to the TACACS+ server as you enter them.

For example, if you enter **sh log**, then the FWSM sends the entire command to the TACACS+ server, **show logging**. However, if you enter **sh log mess**, then the FWSM sends **show logging mess** to the TACACS+ server, and not the expanded command **show logging message**. You can configure multiple spellings of the same argument to anticipate abbreviations (see Figure 15-4).

Figure 15-4 Specifying Abbreviations

The screenshot shows a configuration window with two panes. The left pane has 'show' selected. The right pane contains 'permit logging', 'permit logging message', and 'permit logging mess' and an unchecked checkbox labeled 'Permit Unmatched Args'. Below the panes is an empty text input field and two buttons: 'Add Command' and 'Remove Command'. A vertical label '114414' is on the right side.

- We recommend that you allow the following basic commands for all users:
 - **show checksum**
 - **show curpriv**
 - **enable**
 - **help**
 - **show history**
 - **login**
 - **logout**
 - **pager**

- **show pager**
- **clear pager**
- **quit**
- **show version**

Enabling TACACS+ Command Authorization

Before you enable TACACS+ command authorization, be sure that you are logged into the FWSM as a user that is defined on the TACACS+ server, and that you have the necessary command authorization to continue configuring the FWSM. For example, you should log in as an admin user with all commands authorized. Otherwise, you could become unintentionally locked out.

To configure TACACS+ command authorization, perform the following steps:

-
- Step 1** To perform command authorization using a TACACS+ server, go to Configuration > Device Management > Users/AAA > AAA Access > Authorization, and check the **Enable authorization for command access > Enable** check box.
 - Step 2** From the Server Group drop-down list, choose a AAA server group name.
 - Step 3** (Optional) you can configure the FWSM to use the local database as a fallback method if the AAA server is unavailable. Click the **Use LOCAL when server group fails** check box. We recommend that you use the same username and password in the local database as the AAA server because the FWSM prompt does not give any indication which method is being used.
 - Step 4** Click **Apply**.
-

Configuring Management Access Accounting

To enable accounting for management access, perform the following steps:

-
- Step 1** You can only account for users that first authenticate with the FWSM, so configure authentication using the [“Configuring Authentication for CLI, ASDM, and enable command Access”](#) section on page 15-24.
 - Step 2** To enable accounting of users when they enter the **enable** command:
 - a. Go to Configuration > Device Management > Users/AAA > AAA Access > Accounting, and check the **Require accounting to allow accounting of user activity > Enable** check box.
 - b. From the Server Group drop-down list, choose a RADIUS or TACACS+ server group name.
 - Step 3** To enable accounting of users when they access the FWSM using Telnet, SSH, or the serial console:
 - a. Under the Require accounting for the following types of connections area, check the check boxes for Serial, SSH, and/or Telnet.
 - b. For each connection type, from the Server Group drop-down list, choose a RADIUS or TACACS+ server group name.
 - Step 4** To configure command accounting:
 - a. Under the Require command accounting area, check **Enable**.
 - b. From the Server Group drop-down list, choose a TACACS+ server group name. RADIUS is not supported.

You can send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI.

- c. If you customize the command privilege level using the Command Privilege Setup dialog box (see the “[Assigning Privilege Levels to Commands and Enabling Authorization](#)” section on page 15-29), you can limit which commands the FWSM accounts for by specifying a minimum privilege level in the Privilege level drop-down list. The FWSM does not account for commands that are below the minimum privilege level.

Step 5 Click **Apply**.

Recovering from a Lockout

In some circumstances, when you turn on command authorization or CLI authentication, you can be locked out of the FWSM CLI. You can usually recover access by restarting the FWSM. However, if you already saved your configuration, you might be locked out. [Table 15-3](#) lists the common lockout conditions and how you might recover from them.

Table 15-3 CLI Authentication and Command Authorization Lockout Scenarios

Feature	Lockout Condition	Description	Workaround: Single Mode	Workaround: Multiple Mode
Local CLI authentication	No users in the local database	If you have no users in the local database, you cannot log in, and you cannot add any users.	Log in and reset the passwords and aaa commands.	Session into the FWSM from the switch. From the system execution space, you can change to the context and add a user.
TACACS+ command authorization TACACS+ CLI authentication RADIUS CLI authentication	Server down or unreachable and you do not have the fallback method configured	If the server is unreachable, then you cannot log in or enter any commands.	<ol style="list-style-type: none"> 1. Log in and reset the passwords and AAA commands. 2. Configure the local database as a fallback method so you do not get locked out when the server is down. 	<ol style="list-style-type: none"> 1. If the server is unreachable because the network configuration is incorrect on the FWSM, session into the FWSM from the switch. From the system execution space, you can change to the context and reconfigure your network settings. 2. Configure the local database as a fallback method so you do not get locked out when the server is down.

Table 15-3 CLI Authentication and Command Authorization Lockout Scenarios (continued)

Feature	Lockout Condition	Description	Workaround: Single Mode	Workaround: Multiple Mode
TACACS+ command authorization	You are logged in as a user without enough privileges or as a user that does not exist	You enable command authorization, but then find that the user cannot enter any more commands.	Fix the TACACS+ server user account. If you do not have access to the TACACS+ server and you need to configure the FWSM immediately, then log into the maintenance partition and reset the passwords and aaa commands.	Session into the FWSM from the switch. From the system execution space, you can change to the context and complete the configuration changes. You can also disable command authorization until you fix the TACACS+ configuration.
Local command authorization	You are logged in as a user without enough privileges	You enable command authorization, but then find that the user cannot enter any more commands.	Log in and reset the passwords and aaa commands.	Session into the FWSM from the switch. From the system execution space, you can change to the context and change the user level.

