



CHAPTER 16

Configuring Management Access

This chapter contains the following topics:

- [Configuring Device Access for ASDM, Telnet, or SSH, page 16-1](#)
- [Configuring CLI Parameters, page 16-2](#)
- [Configuring File Access, page 16-4](#)
- [Configuring Configuring ICMP Access, page 16-7](#)
- [Configuring a Management Interface, page 16-9](#)
- [Configuring SNMP, page 16-9](#)
- [Configuring Management Access Rules, page 16-19](#)
- [Configuring AAA for System Administrators, page 16-20](#)

Configuring Device Access for ASDM, Telnet, or SSH

This section describes how to allow clients to access the device using ASDM, Telnet, or SSH. To configure access to the security appliance, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH pane, click **Add**.
- The Add Device Access Configuration dialog box appears in the right-hand pane.
- Step 2** Choose the type of session from the three options listed: ASDM/HTTPS, Telnet, or SSH.
- Step 3** From the Interface Name drop-down list, choose the interface to use for administrative access.
- Step 4** In the IP Address field, add the IP address of the network or host that is allowed access.
- Step 5** From the Mask drop-down list, choose the mask associated with the network or host that is allowed access.
- Step 6** For ASDM/HTTPS sessions, verify that the Enable HTTP Server check box is checked (this is the default setting).
- Step 7** Make sure that port number 443 is specified (this is the default setting).
- Step 8** For Telnet sessions, the default timeout value is 5 minutes. To change this value, type a new one in the Telnet Timeout field.
- Step 9** For SSH sessions, choose the allowed SSH version(s) from the drop-down list.

- Step 10** For SSH sessions, the default timeout value is 60 minutes. To change this value, type a new one in the SSH Timeout field.
- Step 11** Click **Apply**.
The changes are saved to the running configuration.
-

Configuring CLI Parameters

This section includes the following topics:

- [Adding a Banner, page 16-2](#)
- [Customizing a CLI Prompt, page 16-3](#)
- [Changing the Console Timeout Period, page 16-4](#)

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 security appliance 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, security appliance 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.
- ASDM Banner—This banner appears when a user connects to ASDM, following user authentication. The user is given two options for dismissing the banner:
 - Continue—Dismiss the banner and complete login as usual.
 - Disconnect—Dismiss the banner and terminate the connection.

Step 2 Click **Apply**.

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

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 security appliance. 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 From the Configuration > Device Management > Management Access > CLI Prompt pane, 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 2 Click **Apply**.

The new prompt is saved to the running configuration.

Changing the Console Timeout Period

To change the console timeout period, or the duration of time the management console remains active before automatically shutting down, perform the following steps:

Step 1 From the Configuration > Device Management > Management Access > Command Line (CLI) > Console Timeout pane, add a new timeout value in minutes.

To specify unlimited, enter 0. The default value is 0.

Step 2 Click **Apply**.

The console timeout is changed, and the changes are saved to the running configuration.

Configuring File Access

This section includes the following topics.

- [Configuring the FTP Client Mode, page 16-4](#)
- [Configuring the Security Appliance as a Secure Copy Server, page 16-5](#)
- [Configuring the Security Appliance as a TFTP Client, page 16-5](#)
- [Adding Mount Points, page 16-6](#)

Configuring the FTP Client Mode

The security appliance can use FTP to upload or download image files or configuration files to or from an FTP server. In passive FTP, the client initiates both the control connection and the data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

To configure the FTP client to be in passive mode, perform the following steps:

Step 1 From the Configuration > Device Management > Management Access > File Access > FTP Client pane, check **Specify FTP mode as passive**.

Step 2 Click **Apply**.

The FTP client configuration is changed and the change is saved to the running configuration.

Configuring the Security Appliance as a Secure Copy Server

You can enable the secure copy server on the security appliance. Only clients that are allowed to access the security appliance using SSH can establish a secure copy connection.

This implementation of the secure copy server has the following limitations:

- The server can accept and terminate connections for secure copy, but cannot initiate them.
- The server does not have directory support. The lack of directory support limits remote client access to the security appliance internal files.
- The server does not support banners.
- The server does not support wildcards.
- The security appliance license must have the VPN-3DES-AES feature to support SSH version 2 connections.

To configure the security appliance as a Secure Copy (SCP) server, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > File Access > **Secure Copy (SCP) Server** pane, check **Enable secure copy server**.
- Step 2** Click **Apply**.

The changes are saved to the running configuration. The security appliance can function as an SCP server for transferring files from/to the device.

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 security appliance 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 security appliances.

The security appliance 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 security appliance to the TFTP client is done apart from this function.

To configure the security appliance 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 security appliance configuration files. For more information, see [Save Running Configuration to TFTP Server, page 3-4](#).

Adding Mount Points

Common Internet File System (CIFS) and File Transfer Protocol (FTP) mount points

This section includes the following topics:

- [Adding a CIFS Mount Point, page 16-6](#)
- [Adding an FTP Mount Point, page 16-6](#)

Adding a CIFS Mount Point

To define a CIFS mount point, perform the following steps:

- Step 1** From the Configuration > Device Management > Management Access > File Access > Mount-Points pane, click **Add > CIFS Mount Point**.
- The Add CIFS Mount Point dialog box appears.
- Step 2** Check **Enable mount point**.
- This option attaches the CIFS file system on the security appliance to the UNIX file tree.
- Step 3** In the Mount Point Name field, add the name of an existing CIFS location.
- Step 4** In the Server Name or IP Address field, add the name or IP address of the server where the mount point is located.
- Step 5** In the Share Name field, add the name of the folder on the CIFS server.
- Step 6** In the NT Domain Name field, add the name of the NT Domain where the server resides.
- Step 7** In the User Name field, add the name of the user authorized for file system mounting on the server.
- Step 8** In the Password field, add the password for the user authorized for file system mounting on the server.
- Step 9** In the Confirm Password field, add the password again.
- Step 10** Click **OK**.
- The Add CIFS Mount Point dialog box closes.
- Step 11** Click **Apply**.
- The mount point is added to the security appliance and the change is saved to the running configuration.
-

Adding an FTP Mount Point



Note

For an FTP mount point, the FTP Server must have a UNIX directory listing style. Microsoft FTP servers have a default of MS-DOS directory listing style.

To define an FTP mount point, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Management Access > File Access > Mount-Points pane, click **Add > FTP Mount Point**.
The Add FTP Mount Point dialog box appears.
- Step 2** Check the **Enable** check box.
This option attaches the FTP file system on the security appliance to the UNIX file tree.
- Step 3** In the Mount Point Name field, add the name of an existing FTP location.
- Step 4** In the Server Name or IP Address field, add the name or IP address of the server where the mount point is located.
- Step 5** In the Mode field, click the radio button for the FTP mode (Active or Passive). When you choose Passive mode, the client initiates both the FTP control connection and data connection. The server responds with the number of its listening port for this connection.
- Step 6** In the Path to Mount field, add the directory path name to the FTP file server.
- Step 7** In the User Name field, add the name of the user authorized for file system mounting on the server.
- Step 8** In the Password field, add the password for the user authorized for file system mounting on the server.
- Step 9** In the Confirm Password field, add the password again.
- Step 10** Click **OK**.
The dialog box closes.
- Step 11** Click **Apply**.
The mount point is added to the security appliance and the change is saved to the running configuration.
-

Configuring Configuring ICMP Access

By default, you can send ICMP packets to any security appliance interface. However, by default, the security appliance does not respond to ICMP echo requests directed to a broadcast address. You can protect the security appliance from attacks by limiting the addresses of hosts and networks that are allowed to have ICMP access to the security appliance.



Note

For allowing ICMP traffic *through* the security appliance, see the [“Configuring Access Rules” section on page 20-7](#).

It is recommended 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 security appliance 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 security appliance discards the ICMP packet and generates a syslog message. An exception is when an ICMP rule is not configured; in that case, a **permit** statement is assumed.

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 16-1](#) lists the types of ICMP messages.

Table 16-1 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 security appliance interface the rule is to be applied to.
- Step 4** In the IP Address field, do one of the following:
- Add a specific IP address for the host or network.
 - Click **Any Address** and go to [Step 7](#).
- Step 5** From the Mask drop-down list, choose the network mask.
- Step 6** Click **OK**.

The dialog box closes.

- Step 7** (Optional) To set ICMP unreachable message limits, set the following options. Increasing the rate limit, along with enabling the “Decrement time to live for a connection” option on the Configuration > Firewall > Service Policy Rules > Rule Actions > Connection Settings dialog box, is required to allow a traceroute through the security appliance that shows the security appliance as one of the hops.
- **Rate Limit**—Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
 - **Burst Size**—Sets the burst rate, between 1 and 10. This keyword is not currently used by the system, so you can choose any value.
- Step 8** Click **Apply**.
- The ICMP rule is added to the end of the ICMP table and the change is saved to the running configuration.
-

Configuring a Management Interface

A high-security interface can be identified to manage the security appliance. When a management interface is assigned, ASDM can run on it with a fixed IP address over an IPSec VPN tunnel. This is possible if VPN is configured on the security appliance and the external interface is using a dynamically assigned IP address. The management interface is also used when accessing and managing the security appliance securely from home using the VPN client.

To configure a management interface, perform the following steps:

- Step 1** From the **Configuration > Device Management > Management Access > Management Interface** pane, choose the interface with the highest security (the inside interface) from the **Management Access Interface** drop-down list.
- Step 2** Click **Apply**.
- The management interface is assigned 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 16-9](#)
- [Configuring the SNMP Agent, page 16-18](#)
- [Configuring SNMP Traps, page 16-19](#)

Information About SNMP

The Simple Network Management Protocol (SNMP) enables the monitoring of network devices from a central location. The security appliance 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 security appliance 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 security appliance 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 security appliance SNMP agent also replies when a management station asks for information.

This section includes the following topics:

- [Information About SNMP Terminology, page 16-10](#)
- [Information About the Management Information Base and Traps, page 16-10](#)

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 security appliance.
SNMP Agent	The SNMP server running on the security appliance. 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, etc. 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 security appliance 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 location:

<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>.

The following table describes the SNMP MIB support that the security appliance provides:

MIB or Trap Support	Description of Security Appliance Support
SNMP core traps	<p>The security appliance 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 adaptive security appliance is running after a reload.
IF-MIB	<p>Browsing of the following tables:</p> <ul style="list-style-type: none"> • ifXTable <p>The following objects are supported:</p> <pre> IF-MIB::ifName.1 = Ge7/0 IF-MIB::ifInMulticastPkts.1 = Counter32: 0 IF-MIB::ifInBroadcastPkts.1 = Counter32: 0 IF-MIB::ifOutMulticastPkts.1 = Counter32: 0 IF-MIB::ifOutBroadcastPkts.1 = Counter32: 0 IF-MIB::ifHCInOctets.1 = Counter64: 231678 IF-MIB::ifHCInUcastPkts.1 = Counter64: 963 IF-MIB::ifHCInMulticastPkts.1 = Counter64: 0 IF-MIB::ifHCInBroadcastPkts.1 = Counter64: 0 IF-MIB::ifHCOutOctets.1 = Counter64: 27251 IF-MIB::ifHCOutUcastPkts.1 = Counter64: 325 IF-MIB::ifHCOutMulticastPkts.1 = Counter64: 0 IF-MIB::ifHCOutBroadcastPkts.1 = Counter64: 0 IF-MIB::ifLinkUpDownTrapEnable.1 = enabled(1) IF-MIB::ifHighSpeed.1 = Gauge32: 10000 (supports 10GE interfaces) IF-MIB::ifPromiscuousMode.1 = false(2) IF-MIB::ifConnectorPresent.1 = true(1) IF-MIB::ifAlias.1 = IF-MIB::ifCounterDiscontinuityTime.1 = Timeticks: (0) 0:00:00.00 </pre>

MIB or Trap Support	Description of Security Appliance Support
RFC1213-MIB	<p>Browsing of the following table:</p> <ul style="list-style-type: none"> • ipAddrTable • ifTable <p>The following objects are supported:</p> <pre> RFC1213-MIB::ifNumber.0 = 1 RFC1213-MIB::ifIndex.1 = 1 RFC1213-MIB::ifDescr.1 = "Adaptive Security Appliance 'mgmt' interface" RFC1213-MIB::ifType.1 = ethernet-csmacd(6) RFC1213-MIB::ifMtu.1 = 1500 RFC1213-MIB::ifSpeed.1 = Gauge32: 4294967295 RFC1213-MIB::ifPhysAddress.1 = Hex: 00 15 17 15 AB 08 RFC1213-MIB::ifAdminStatus.1 = up(1) RFC1213-MIB::ifOperStatus.1 = up(1) RFC1213-MIB::ifLastChange.1 = Timeticks: (200) 0:00:02.00 RFC1213-MIB::ifInOctets.1 = Counter32: 231678 RFC1213-MIB::ifInUcastPkts.1 = Counter32: 963 RFC1213-MIB::ifInNUcastPkts.1 = Counter32: 0 RFC1213-MIB::ifInDiscards.1 = Counter32: 630 RFC1213-MIB::ifInErrors.1 = Counter32: 0 RFC1213-MIB::ifOutOctets.1 = Counter32: 27251 RFC1213-MIB::ifOutUcastPkts.1 = Counter32: 325 RFC1213-MIB::ifOutNUcastPkts.1 = Counter32: 0 RFC1213-MIB::ifOutDiscards.1 = Counter32: 0 RFC1213-MIB::ifOutErrors.1 = Counter32: 0 RFC1213-MIB::ifOutQLen.1 = Gauge32: 6 RFC1213-MIB::ifSpecific.1 = OID: SNMPv2-SMI::zeroDotZero </pre> <ul style="list-style-type: none"> • system <p>The following objects are supported:</p> <pre> RFC1213-MIB::sysDescr.0 = "Cisco Adaptive Security Appliance Version 8.1(0)15" RFC1213-MIB::sysObjectID.0 = OID: CISCO-PRODUCTS-MIB::ciscoASA5580 RFC1213-MIB::sysUpTime.0 = Timeticks: (390500) 1:05:05.00 RFC1213-MIB::sysContact.0 = "yourname@yourcompany.com" RFC1213-MIB::sysName.0 = "sw8-5580" RFC1213-MIB::sysLocation.0 = "YourCity, YourState" RFC1213-MIB::sysServices.0 = 4 </pre>
SNMPv2-MIB	SNMP browsing

MIB or Trap Support	Description of Security Appliance Support
ENTITY-MIB	<p>Browsing of the following groups and tables:</p> <ul style="list-style-type: none"> • entPhysicalTable • entLogicalTable <p>The following objects are supported:</p> <pre> ENTITY-MIB::entPhysicalDescr.1 = ASA 5580 Series SPE40 or SPE20 ENTITY-MIB::entPhysicalDescr.2 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.3 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.4 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.5 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.6 = ASA 5580 4 port GE Fiber If Card ENTITY-MIB::entPhysicalDescr.7 = ASA 5580 4 port GE Copper If Card ENTITY-MIB::entPhysicalDescr.8 = ASA 5580 2 port 10GE SR Fiber If Card ENTITY-MIB::entPhysicalVendorType.1 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevChassisASA5580 ENTITY-MIB::entPhysicalVendorType.2 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.3 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.4 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.5 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.6 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB:: cevModuleASA5580Pm4x1geFi ENTITY-MIB::entPhysicalVendorType.7 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB:: cevModuleASA5580Pm4x1geCu ENTITY-MIB::entPhysicalVendorType.8 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB:: cevModuleASA5580Pm2x10geFi ENTITY-MIB::entPhysicalContainedIn.1 = 0 ENTITY-MIB::entPhysicalContainedIn.2 = 1 ENTITY-MIB::entPhysicalContainedIn.3 = 1 ENTITY-MIB::entPhysicalContainedIn.4 = 1 ENTITY-MIB::entPhysicalContainedIn.5 = 1 ENTITY-MIB::entPhysicalContainedIn.6 = 1 ENTITY-MIB::entPhysicalContainedIn.7 = 1 ENTITY-MIB::entPhysicalContainedIn.8 = 1 ENTITY-MIB::entPhysicalClass.1 = chassis(3) ENTITY-MIB::entPhysicalClass.2 = cpu(12) ENTITY-MIB::entPhysicalClass.3 = cpu(12) ENTITY-MIB::entPhysicalClass.4 = cpu(12) ENTITY-MIB::entPhysicalClass.5 = cpu(12) ENTITY-MIB::entPhysicalClass.6 = module(9) ENTITY-MIB::entPhysicalClass.7 = module(9) ENTITY-MIB::entPhysicalClass.8 = module(9) ENTITY-MIB::entPhysicalParentRelPos.1 = 0 ENTITY-MIB::entPhysicalParentRelPos.2 = 0 ENTITY-MIB::entPhysicalParentRelPos.3 = 1 ENTITY-MIB::entPhysicalParentRelPos.4 = 2 ENTITY-MIB::entPhysicalParentRelPos.5 = 3 ENTITY-MIB::entPhysicalParentRelPos.6 = 0 ENTITY-MIB::entPhysicalParentRelPos.7 = 0 ENTITY-MIB::entPhysicalParentRelPos.8 = 0 ENTITY-MIB::entPhysicalName.1 = Chassis ENTITY-MIB::entPhysicalName.2 = 0 ENTITY-MIB::entPhysicalName.3 = 1 ENTITY-MIB::entPhysicalName.4 = 2 </pre>

MIB or Trap Support	Description of Security Appliance Support
ENTITY-MIB (continued)	ENTITY-MIB::entPhysicalName.5 = 3 ENTITY-MIB::entPhysicalName.6 = slot 4 ENTITY-MIB::entPhysicalName.7 = slot 5 ENTITY-MIB::entPhysicalName.8 = slot 7 ENTITY-MIB::entPhysicalHardwareRev.1 = V01 ENTITY-MIB::entPhysicalHardwareRev.2 = ENTITY-MIB::entPhysicalHardwareRev.3 = ENTITY-MIB::entPhysicalHardwareRev.4 = ENTITY-MIB::entPhysicalHardwareRev.5 = ENTITY-MIB::entPhysicalHardwareRev.6 = D5618404 ENTITY-MIB::entPhysicalHardwareRev.7 = D4577407 ENTITY-MIB::entPhysicalHardwareRev.8 = D7555203 ENTITY-MIB::entPhysicalFirmwareRev.1 = 1.1(0)4 ENTITY-MIB::entPhysicalFirmwareRev.2 = ENTITY-MIB::entPhysicalFirmwareRev.3 = ENTITY-MIB::entPhysicalFirmwareRev.4 = ENTITY-MIB::entPhysicalFirmwareRev.5 = ENTITY-MIB::entPhysicalFirmwareRev.6 = ENTITY-MIB::entPhysicalFirmwareRev.7 = ENTITY-MIB::entPhysicalFirmwareRev.8 = ENTITY-MIB::entPhysicalSoftwareRev.1 = 8.1(0)1 ENTITY-MIB::entPhysicalSoftwareRev.2 = ENTITY-MIB::entPhysicalSoftwareRev.3 = ENTITY-MIB::entPhysicalSoftwareRev.4 = ENTITY-MIB::entPhysicalSoftwareRev.5 = ENTITY-MIB::entPhysicalSoftwareRev.6 = ENTITY-MIB::entPhysicalSoftwareRev.7 = ENTITY-MIB::entPhysicalSoftwareRev.8 = ENTITY-MIB::entPhysicalSerialNum.1 = JAB12345678 ENTITY-MIB::entPhysicalSerialNum.2 = ENTITY-MIB::entPhysicalSerialNum.3 = ENTITY-MIB::entPhysicalSerialNum.4 = ENTITY-MIB::entPhysicalSoftwareRev.5 = ENTITY-MIB::entPhysicalSerialNum.6 = 001517154451 ENTITY-MIB::entPhysicalSerialNum.7 = 0015171559DC ENTITY-MIB::entPhysicalSerialNum.8 = 0015171D9752 ENTITY-MIB::entPhysicalMfgName.1 = Cisco Systems Inc. ENTITY-MIB::entPhysicalMfgName.2 = ENTITY-MIB::entPhysicalMfgName.3 = ENTITY-MIB::entPhysicalMfgName.4 = ENTITY-MIB::entPhysicalMfgName.5 = ENTITY-MIB::entPhysicalMfgName.6 = ENTITY-MIB::entPhysicalMfgName.7 = ENTITY-MIB::entPhysicalMfgName.8 = ENTITY-MIB::entPhysicalMfgName.9 = ENTITY-MIB::entPhysicalModelName.1 = ASA5580-SPE40 or SPE20 ENTITY-MIB::entPhysicalModelName.2 = ENTITY-MIB::entPhysicalModelName.3 = ENTITY-MIB::entPhysicalModelName.4 = ENTITY-MIB::entPhysicalModelName.5 = ENTITY-MIB::entPhysicalModelName.6 = ASA5580-4GE-FI ENTITY-MIB::entPhysicalModelName.7 = ASA5580-4GE-CU ENTITY-MIB::entPhysicalModelName.8 = ASA5580-2X10GE-SR ENTITY-MIB::entPhysicalAlias.1 = ENTITY-MIB::entPhysicalAlias.2 = ENTITY-MIB::entPhysicalAlias.3 = ENTITY-MIB::entPhysicalAlias.4 = ENTITY-MIB::entPhysicalAlias.5 = ENTITY-MIB::entPhysicalAlias.6 = ENTITY-MIB::entPhysicalAlias.7 =

MIB or Trap Support	Description of Security Appliance Support
ENTITY-MIB (continued)	<p>ENTITY-MIB::entPhysicalAlias.8 = ENTITY-MIB::entPhysicalAssetID.1 = ENTITY-MIB::entPhysicalAssetID.2 = ENTITY-MIB::entPhysicalAssetID.3 = ENTITY-MIB::entPhysicalAssetID.8 = ENTITY-MIB::entPhysicalIsFRU.1 = false(2) ENTITY-MIB::entPhysicalIsFRU.2 = false(2) ENTITY-MIB::entPhysicalIsFRU.4 = false(2) ENTITY-MIB::entPhysicalIsFRU.5 = false(2) ENTITY-MIB::entPhysicalIsFRU.6 = true(1) ENTITY-MIB::entPhysicalIsFRU.7 = true(1) ENTITY-MIB::entPhysicalIsFRU.8 = true(1)</p> <p>Browsing of the following traps:</p> <ul style="list-style-type: none"> • config-change • fru-insert • fru-remove
CISCO-IPSEC-FLOW-MONITOR-MIB	<p>Browsing of the MIB.</p> <p>Browsing of the following traps:</p> <ul style="list-style-type: none"> • start • stop
CISCO-REMOTE-ACCESS-MONITOR-MIB	<p>Browsing of the MIB.</p> <p>Browsing of the following traps:</p> <ul style="list-style-type: none"> • session-threshold-exceeded
CISCO-CRYPTO-ACCELERATOR-MIB	Browsing of the MIB.
ALTIGA-GLOBAL-REG	Browsing of the MIB.
CISCO-FIREWALL-MIB	<p>Browsing of the following groups:</p> <ul style="list-style-type: none"> • cfwSystem <p>The information in cfwSystem.cfwStatus, which relates to failover status, applies to the entire device and not just a single context.</p>

MIB or Trap Support	Description of Security Appliance Support
CISCO-MEMORY-POOL-MIB	<p>Browsing of the following table:</p> <ul style="list-style-type: none"> • <code>ciscoMemoryPoolTable</code>—The memory usage described in this table applies only to the security appliance general-purpose processor, and not to the network processors. <p>The following objects are supported:</p> <pre> CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.1 = System memory CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.6 = DMA ALT1 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.7 = DMA CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.8 = Global Shared CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.1 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.6 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.7 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.8 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.1 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.6 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.7 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.8 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.1 = Gauge32: 102805792 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.6 = Gauge32: 32012672 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.7 = Gauge32: 32012672 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.8 = Gauge32: 38752248 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.1 = Gauge32: 1432686304 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.6 = Gauge32: 198862416 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.7 = Gauge32: 198862416 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.8 = Gauge32: 229683208 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.1 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.6 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.7 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.8 = Gauge32: 0 bytes </pre>

MIB or Trap Support	Description of Security Appliance Support
CISCO-PROCESS- MIB	<p>Browsing of the following table:</p> <ul style="list-style-type: none"> • <code>cpmCPUTotalTable</code> <p>The following objects are supported:</p> <pre> CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.1 = 1 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.2 = 2 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.3 = 3 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.4 = 4 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.5 = 5 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.6 = 1 CISCO-PROCESS-MIB::cpmCPUTotal15sec.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal15sec.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal15sec.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal15sec.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal15sec.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal15sec.6 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal1min.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal1min.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.6 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal5min.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal5min.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.6 = Gauge32: 50 </pre> <p>The first row in the <code>cpmCPUTotalTable</code> reflects either the CPU load for the system in single security context mode or the CPU load for the context in multiple context mode.</p> <p>The last row in <code>cpmCPUTotalTable</code> always reflects the system CPU load. This row is identical to the first row in single context mode and is only available through the admin context in multiple context mode. The row represents the load for all CPUs, and is equivalent to the output from the <code>show cpu</code> command.</p> <p>All rows in-between the first and last reflect the per-CPU load. They are only present for multi-CPU systems and only available in either single mode or the admin context in multiple mode.</p>
CISCO-SYSLOG-MIB	<p>The following trap:</p> <ul style="list-style-type: none"> • <code>clogMessageGenerated</code> <p>You cannot browse this MIB.</p>
CISCO-UNIFIED-FIREWALL-MIB	<p>Browsing of the following tables:</p> <ul style="list-style-type: none"> • <code>cuFwConnectionGlobals</code> • <code>cufwUrlFilterGlobals</code> • <code>cufwUrlFilterServers</code>

Configuring an SNMP Agent and Management Station

This section includes the following topics:

- [Configuring the SNMP Agent, page 16-18](#)

- [Adding an SNMP Management Station, page 16-18](#)

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.
- Enter the password used by the SNMP management stations when sending requests to the security appliance. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The security appliance 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 2** In the Contact field, add the name of the security appliance 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 3** In the Location field, add the location of the security appliance 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 4** In the Listening Port field, add the number of the security appliance port that listens for SNMP requests from management stations; or keep the default, port number 161.
- Step 5** 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 19-15](#).
- 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 [“AAA Server and Local Database Support”](#) section on page 14-3 or the [“Configuring AAA Server Groups”](#) section on page 14-9.

This section includes the following topics:

- [Configuring Authentication for CLI, ASDM, and enable command Access, page 16-20](#)
- [Limiting User CLI and ASDM Access with Management Authorization, page 16-22](#)
- [Configuring Command Authorization, page 16-23](#)
- [Configuring Management Access Accounting, page 16-31](#)
- [Recovering from a Lockout, page 16-32](#)

Configuring Authentication for CLI, ASDM, and enable command Access

If you enable CLI authentication, the security appliance 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 security appliance 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 security appliance can authenticate a Telnet, SSH, or HTTP user, you must first configure access to the security appliance according to the “[Configuring Device Access for ASDM, Telnet, or SSH](#)” section on page 16-1. These panes identify the IP addresses that are allowed to communicate with the security appliance.

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:
- Check the **Enable** check box.
 - From the Server Group drop-down list, choose a server group name or the LOCAL database.
 - (Optional) If you chose a AAA server, you can configure the security appliance 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 security appliance 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:
- Check one or more of the following check boxes:
 - HTTP/ASDM**—Authenticates the ASDM client that accesses the security appliance 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.
 - Serial**—Authenticates users who access the security appliance using the console port.
 - SSH**—Authenticates users who access the security appliance using SSH.
 - Telnet**—Authenticates users who access the security appliance using Telnet.
 - For each service that you checked, from the Server Group drop-down list, choose a server group name or the LOCAL database.
 - (Optional) If you chose a AAA server, you can configure the security appliance 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 security appliance prompt does not give any indication which method is being used.
- Step 3** Click **Apply**.
-

Limiting User CLI and ASDM Access with Management Authorization

If you configure CLI or **enable** authentication, you can limit a local user, RADIUS, TACACS+, or LDAP user (if you map LDAP attributes to RADIUS attributes) from accessing the CLI, ASDM, or the **enable** command.



Note

Serial access is not included in management authorization, so if you enable the Authentication > Serial option, then any user who authenticates can access the console port.

To configure management authorization, perform the following steps:

- Step 1** To enable management authorization, go to Configuration > Device Management > Users/AAA > AAA Access > Authorization, and check the **Perform authorization for exec shell access > Enable** check box.

This option also enables support of administrative user privilege levels from RADIUS, which can be used in conjunction with local command privilege levels for command authorization. See the [“Configuring Local Command Authorization”](#) section on page 16-25 for more information.

- Step 2** To configure the user for management authorization, see the following requirements for each AAA server type or local user:
- RADIUS or LDAP (mapped) users—Configure the Service-Type attribute for one of the following values.
 - RADIUS or LDAP (mapped) users—Use the IETF RADIUS numeric Service-Type attribute which maps to one of the following values.
 - Service-Type 6 (admin)—Allows full access to any services specified by the Authentication tab options
 - Service-Type 7 (nas-prompt)—Allows access to the CLI when you configure the Telnet or SSH authentication options, but denies ASDM configuration access if you configure the HTTP option. ASDM monitoring access is allowed. If you configure **enable** authentication with the Enable option, the user cannot access privileged EXEC mode using the **enable** command.
 - Service-Type 5 (remote-access)—Denies management access. The user cannot use any services specified by the Authentication tab options (excluding the Serial option; serial access is allowed). Remote-access (IPSec and SSL) users can still authenticate and terminate their remote-access sessions.
 - TACACS+ users—Authorization is requested with the “service=shell” and the server responds with PASS or FAIL.
 - PASS, privilege level 1—Allows full access to any services specified by the Authentication tab options.
 - PASS, privilege level 2 and higher—Allows access to the CLI when you configure the Telnet or SSH authentication options, but denies ASDM configuration access if you configure the HTTP option. ASDM monitoring access is allowed. If you configure **enable** authentication with the Enable option, the user cannot access privileged EXEC mode using the **enable** command.
 - FAIL—Denies management access. The user cannot use any services specified by the Authentication tab options (excluding the Serial option; serial access is allowed).

- Local users—Configure the Access Restriction option. See “[Add/Edit User Account > Identity](#)”. By default, the access restriction is Full Access, which allows full access to any services specified by the Authentication tab options.
-

Configuring Command Authorization

If you want to control the access to commands, the security appliance 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 16-23](#)
- [Configuring Local Command Authorization, page 16-25](#)
- [Configuring TACACS+ Command Authorization, page 16-27](#)

Command Authorization Overview

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

- [Supported Command Authorization Methods, page 16-23](#)
- [About Preserving User Credentials, page 16-24](#)
- [Security Contexts and Command Authorization, page 16-24](#)

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the security appliance. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the security appliance 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 security appliance 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 security appliance 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 *Cisco Security Appliance 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 security appliance, they are required to provide a username and password for authentication. The security appliance 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 security appliance.

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 security appliance 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 14-22.)

This section includes the following topics:

- [Local Command Authorization Prerequisites](#), page 16-25
- [Default Command Privilege Levels](#), page 16-26
- [Assigning Privilege Levels to Commands and Enabling Authorization](#), page 16-26

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 16-20.)

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 “[AAA Server and Local Database Support](#)” section on page 14-3.
 - 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 14-22.

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 security appliance 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. See the [“Limiting User CLI and ASDM Access with Management Authorization”](#) section on page 16-22 for more information.

- Step 5** Click **Apply**.
-

Configuring TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the security appliance 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 security appliance. If you still get locked out, see the [“Recovering from a Lockout”](#) section on page 16-32.

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 security appliance. 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 16-23.

This section includes the following topics:

- [TACACS+ Command Authorization Prerequisites](#), page 16-28
- [Configuring Commands on the TACACS+ Server](#), page 16-28
- [Enabling TACACS+ Command Authorization](#), page 16-30

TACACS+ Command Authorization Prerequisites

Configure CLI and **enable** authentication (see the [“Configuring Authentication for CLI, ASDM, and enable command Access”](#) section on page 16-20).

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 security appliance 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 security appliance command authorization.

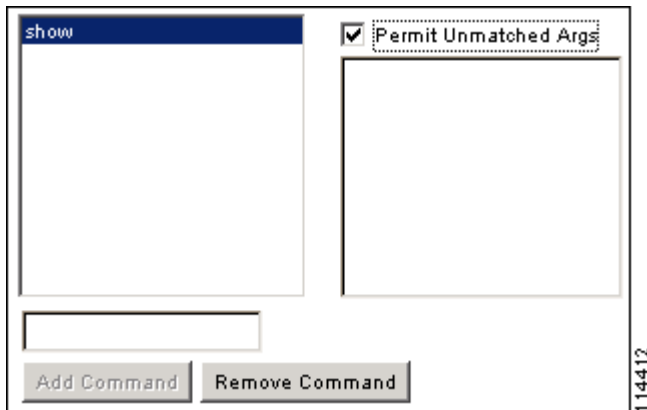
- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by **permit** or **deny**.

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 16-1](#)).

Figure 16-1 Permitting All Related Commands



- 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 16-2](#)).

Figure 16-2 Permitting Single Word Commands

The screenshot shows a configuration window with two main text areas. The left area, labeled 'enable', contains a list of permitted commands. The right area, labeled 'Arguments', is currently empty. A checkbox labeled 'Permit Unmatched Args' is checked. At the bottom of the window are two buttons: 'Add Command' and 'Remove Command'. A vertical label '114411' is 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 16-3).

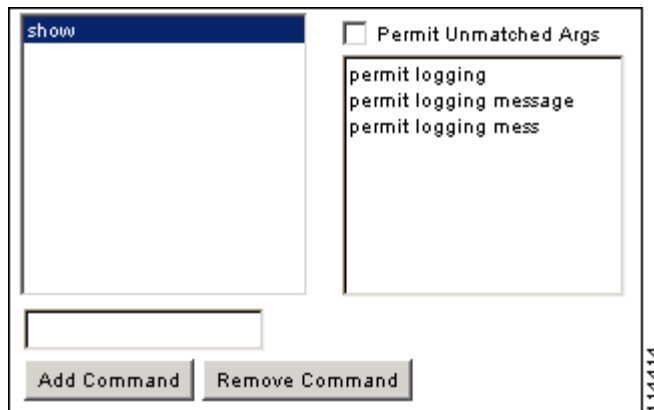
Figure 16-3 Disallowing Arguments

This screenshot is similar to Figure 16-2, but the 'Arguments' box now contains the text 'deny password'. The 'enable' command remains in the 'Commands' box, and the 'Permit Unmatched Args' checkbox is still checked. The 'Add Command' and 'Remove Command' buttons are at the bottom. A vertical label '114410' is on the right side of the window.

- When you abbreviate a command at the command line, the security appliance 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 security appliance sends the entire command to the TACACS+ server, **show logging**. However, if you enter **sh log mess**, then the security appliance 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 16-4).

Figure 16-4 Specifying Abbreviations



- 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 security appliance as a user that is defined on the TACACS+ server, and that you have the necessary command authorization to continue configuring the security appliance. 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 security appliance 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 security appliance 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 security appliance, so configure authentication using the [“Configuring Authentication for CLI, ASDM, and enable command Access” section on page 16-20](#).
- Step 2** To enable accounting of users when they enter the **enable** command:
- Go to Configuration > Device Management > Users/AAA > AAA Access > Accounting, and check the **Require accounting to allow accounting of user activity > Enable** check box.
 - 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 security appliance using Telnet, SSH, or the serial console:
- Under the Require accounting for the following types of connections area, check the check boxes for Serial, SSH, and/or Telnet.
 - 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:
- Under the Require command accounting area, check **Enable**.
 - 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.
 - 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 16-26](#)), you can limit which commands the security appliance accounts for by specifying a minimum privilege level in the Privilege level drop-down list. The security appliance 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 security appliance CLI. You can usually recover access by restarting the security appliance. However, if you already saved your configuration, you might be locked out. Table 16-2 lists the common lockout conditions and how you might recover from them.

Table 16-2 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 security appliance 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 security appliance, session into the security appliance 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.
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.	<p>Fix the TACACS+ server user account.</p> <p>If you do not have access to the TACACS+ server and you need to configure the security appliance immediately, then log into the maintenance partition and reset the passwords and aaa commands.</p>	Session into the security appliance 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 security appliance from the switch. From the system execution space, you can change to the context and change the user level.

