



CHAPTER 13

Configuring Management Access

This chapter contains the following topics:

- [HTTPS/ASDM, page 13-1](#)
- [Command Line, page 13-2](#)
- [File Access, page 13-9](#)
- [ICMP, page 13-15](#)
- [Management Interface, page 13-18](#)
- [SNMP, page 13-19](#)
- [Management Access Rules, page 13-24](#)
- [Configuring AAA for System Administrators, page 13-27](#)

HTTPS/ASDM

The HTTPS/ASDM pane provides a table that specifies the addresses of all the hosts or networks that are allowed access to the ASDM using HTTPS. You can use this table to add or change the hosts or networks that are allowed access.

Fields

- **Interface**—Lists the interface on the security appliance from which the administrative access to the device manager is allowed.
- **IP Address**—Lists the IP address of the network or host that is allowed access.
- **Mask**—Lists the network mask associated with the network or host that is allowed access.
- **Add**—Displays the Add HTTP Configuration dialog box for adding a new host or network.
- **Edit**—Displays the Edit HTTP Configuration dialog box for editing the selected host or network.
- **Delete**—Deletes the selected host or network.

Modes

The following table shows the modes in which this feature is available:

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

Add/Edit HTTP Configuration

The Add/Edit HTTP Configuration dialog box lets you add a host or network that will be allowed administrative access to the security appliance device manager over HTTPS.

Fields

- Interface Name—Specifies the interface on the security appliance from which the administrative access to the security appliance device manager is allowed.
- IP Address—Specifies the IP address of the network or host that is allowed access.
- Mask—Specifies the network mask associated with the network or host that is allowed access.

Modes

The following table shows the modes in which this feature is available:

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

Command Line

This section includes command-line interface features, and includes the following topics:

- [Banner, page 13-2](#)
- [Console Timeout, page 13-4](#)
- [Secure Shell, page 13-4](#)
- [Telnet, page 13-6](#)

Banner

The Banner pane lets you configure message of the day, login, and session banners.

To create a banner, enter text into the appropriate box. Spaces in the text are preserved; however, tabs can be entered in the ASDM interface but cannot be entered through the command line interface. The tokens \$(domain) and \$(hostname) are replaced with the host name and domain name of the security appliance.

Use the \$(hostname) and \$(domain) tokens to echo the hostname and domain name specified in a particular context. Use the \$(system) token to echo a banner configured in the system space in a particular context.

Multiple lines in a banner are handled by entering a line of text for each line you wish to add. Each line is then appended to the end of the existing banner. If the text is empty, then a carriage return (CR) will be added to the banner. There is no limit on the length of a banner other than RAM and Flash memory limits. You can only use ASCII characters, including new line (the Enter key, which counts as two characters).

When accessing the security appliance through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs when attempting to display the banner messages.

To replace a banner, change the contents of the appropriate box and click **Apply**. To clear a banner, clear the contents of the appropriate box and click **Apply**.

Although the banner command is not available in the System Context through the ASDM pane, it can be configured with Tools > Command Line Interface.

Modes

The following table shows the modes in which this feature is available:

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

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 configure the CLI prompt, perform the following steps:

-
- Step 1** 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.
- Step 2** 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.
- Step 3** 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.

You can preview the command prompt at the bottom of the pane in the CLI Prompt Preview field.

Modes

The following table shows the modes in which this feature is available:

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

Console Timeout

The Console Timeout pane lets you specify a time period in minutes for the management console to remain active. When it reaches the time limit you specify here, the console automatically shuts down.

Type the time period in the Console Timeout field. To specify unlimited, enter 0. The default value is 0.

Modes

The following table shows the modes in which this feature is available:

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

Secure Shell

The Secure Shell pane lets you configure rules that permit only specific hosts or networks to connect to the security appliance for administrative access using the SSH protocol. The rules restrict SSH access to a specific IP address and netmask. SSH connection attempts that comply with the rules must then be authenticated by a AAA server or the Telnet password.

You can monitor SSH sessions using `Monitoring > Administration > Secure Shell Sessions`.

Fields

The Secure Shell pane displays the following fields:

- Allowed SSH Versions—Restricts the version of SSH accepted by the security appliance. By default, SSH Version 1 and SSH Version 2 connections are accepted.
- Timeout (minutes)—Displays the number of minutes, 1 to 60, the Secure Shell session can remain idle before the security appliance closes it. The default is 5 minutes.
- SSH Access Rule—Displays the hosts and networks that are allowed to access the security appliance using SSH. Double-clicking a row in this table opens the Edit SSH Configuration dialog box for the selected entry.
 - Interface—Displays the name of a security appliance interface that will permit SSH connections.
 - IP Address—Displays the IP address of each host or network permitted to connect to this security appliance through the specified interface.
 - Mask—Displays the netmask for the IP address of each host or network permitted to connect to this security appliance through the specified interface.
- Add—Opens the Add SSH Configuration dialog box.
- Edit—Opens the Edit SSH Configuration dialog box.
- Delete—Deletes the selected SSH access rule.

Modes

The following table shows the modes in which this feature is available:

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

Add/Edit SSH Configuration

The Add SSH Configuration dialog box lets you add a new SSH access rule to the rule table. The Edit SSH Configuration dialog box lets you change an existing rule.

Fields

- Interface—Specifies the name of the security appliance interface that permits SSH connections.
- IP Address—Specifies the IP address of the host or network that is permitted to establish an SSH connection with the security appliance.
- Mask—The netmask of the host or network that is permitted to establish an SSH connection with the security appliance.

Modes

The following table shows the modes in which this feature is available:

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

Telnet

The Telnet pane lets you configure rules that permit only specific hosts or networks running ASDM to connect to the security appliance using the Telnet protocol.

The rules restrict administrative Telnet access through a security appliance interface to a specific IP address and netmask. Connection attempts that comply with the rules must then be authenticated by a preconfigured AAA server or the Telnet password. You can monitor Telnet sessions using Monitoring > Telnet Sessions.



Note

Although a configuration file may contain more, there may be only five Telnet sessions active at the same time in single context mode. In multiple context mode, there may be only five Telnet sessions active per context.

Fields

The Telnet pane displays the following fields:

Telnet Rule Table:

- **Interface**—Displays the name of a security appliance interface which will permit Telnet connections, an interface on which is located a PC or workstation running ASDM.
- **IP Address**—Displays the IP address of each host or network permitted to connect to this security appliance through the specified interface.



Note This is not the IP address of the security appliance interface.

- **Netmask**—Displays the netmask for the IP address of each host or network permitted to connect to this security appliance through the specified interface.



Note This is not the IP address of the security appliance interface.

- **Timeout**—Displays the number of minutes, 1 to 60, the Telnet session can remain idle before the security appliance closes it. The default is 5 minutes.
- **Add**—Opens the Add Telnet Configuration dialog box.
- **Edit**—Opens the Edit Telnet Configuration dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in ASDM to the security appliance and applies them to the running configuration. Click Save to write a copy of the running configuration to Flash memory. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby unit.

- **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked **Refresh** or **Apply**. After Reset, use Refresh to make sure that information from the current running configuration is displayed.

Modes

The following table shows the modes in which this feature is available:

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

Add/Edit Telnet Configuration

Adding Telnet Rules

To add a rule to the Telnet rule table, perform the following steps:

1. Click the **Add** button to open the **Telnet > Add** dialog box.
2. Click **Interface** to add a security appliance interface to the rule table.
3. In the IP Address box, enter the IP address of the host running ASDM which will be permitted Telnet access through this security appliance interface.



Note This is not the IP address of the security appliance interface.

4. In the Mask list, select or enter a netmask for the IP address to be permitted Telnet access.



Note This is not a mask for the IP address of the security appliance interface.

5. To return to the previous pane click:
 - **OK**—Accepts changes and returns to the previous pane.
 - **Cancel**—Discards changes and returns to the previous pane.
 - **Help**—Provides more information.

Editing Telnet Rules

To edit a rule in the Telnet rule table, perform the following steps:

1. Click **Edit** to open the Telnet > Edit dialog box.
2. Click **Interface** to select a security appliance interface from the rule table.
3. In the IP Address field, enter the IP address of the host running ASDM which will be permitted Telnet access through this security appliance interface.



Note This is not the IP address of the security appliance interface.

4. In the Mask list, select or enter a netmask for the IP address to be permitted Telnet access.



Note This is not a mask for the IP address of the security appliance interface.

5. To return to the previous Window, click one of the following buttons:
 - **OK**—Accepts changes and returns to the previous pane.
 - **Cancel**—Discards changes and returns to the previous pane.
 - **Help**—Provides more information.

Deleting Telnet Rules

To delete a rule from the Telnet table, perform the following steps:

1. Select a rule from the Telnet rule table.
2. Click **Delete**.

Applying Changes

Changes to the table made by Add, Edit, or Delete are not immediately applied to the running configuration. To apply or discard changes, click one of the following buttons:

1. **Apply**—Sends changes made in ASDM to the security appliance and applies them to the running configuration. Click **Save** to write a copy of the running configuration to Flash memory. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby unit.
2. **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked **Refresh** or **Apply**. After Reset, use **Refresh** to make sure that information from the current running configuration is displayed.

Fields

- **Interface Name**—Select the interface to allow Telnet access to the security appliance.
- **IP Address**—Enter the IP address of the host or network permitted to Telnet to the security appliance.
- **Mask**—Enter the subnet mask of the host or network permitted to Telnet to the security appliance.
- **OK**—Accepts changes and returns to the previous pane.
- **Cancel**—Discards changes and returns to the previous pane.
- **Help**—Provides more information.

Modes

The following table shows the modes in which this feature is available:

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

File Access

This section includes file access features, and includes the following topics:

- [FTP Client, page 13-9](#)
- [Secure Copy, page 13-9](#)
- [TFTP Client, page 13-10](#)
- [Mount Points, page 13-11](#)

FTP Client

The FTP Mode pane configures FTP mode as active or passive. 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.

Fields

- Specify FTP mode as passive—Configures FTP mode as active or passive.

Modes

The following table shows the modes in which this feature is available:

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

Secure Copy

The Secure Copy pane lets you 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.

Limitations

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.

Fields

- Enable Secure Copy Server—Select this check box to enable the secure copy server on the security appliance.

Modes

The following table shows the modes in which this feature is available:

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

TFTP Client

This pane lets you configure the security appliance to act as a TFTP Client.

**Note**

This pane does not write the file to the server. Configure the security appliance for using a TFTP client in this pane, then click **File > Save Running Configuration to TFTP Server**.

TFTP Servers and the security appliance

TFTP is a simple client/server file transfer protocol described in RFC783 and RFC1350 Rev. 2. This pane lets you 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.

This pane uses the **configure net** command to specify the IP address of the TFTP client, and the **tftp-server** command to specify the interface and the path/filename on the server where the running configuration file will be written. Once this information is applied to the running configuration, ASDM File > Save Running Configuration to TFTP client uses the **copy** command to execute the file transfer.

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.

The **show tftp-client** command lists the **tftp-client** command statements in the current configuration. The **no tftp client** command disables access to the client.

Fields

The TFTP pane provides the following fields:

- Enable—Click to select and enable these TFTP client settings in the configuration.
- Interface Name—Select the name of the security appliance interface which will use these TFTP client settings.
- IP Address—Enter the IP address of the TFTP server.

- Path—Type in the TFTP client path, beginning with “/” (forward slash) and ending in the file name, to which the running configuration file will be written.

Example TFTP client path: **/tftpboot/security appliance/config3**



Note The path must begin with a forward slash (/).

For More Information

For more information about TFTP, refer to the security appliance Technical Documentation for your version of software.

Modes

The following table shows the modes in which this feature is available:

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

Mount Points

The Mount Points table displays those Common Internet File System (CIFS) and File Transfer Protocol (FTP) mount points currently configured for file access.



To add, change, or remove a mount point, do one of the following:

- To add a mount point, choose **Add > CIFS Mount Point** or **Add > FTP Mount Point**. For parameter details, see: [Fields in the Add or Edit FTP Mount Point Dialog Box, page 13-15](#) or [Fields in the Add or Edit FTP Mount Point Dialog Box, page 13-15](#).
- To change a mount point, select the entry in the table and click **Edit**. You can also double-click an entry to edit the entry. For parameter details, see: [Fields in the Add or Edit FTP Mount Point Dialog Box, page 13-15](#) or [Fields in the Add or Edit FTP Mount Point Dialog Box, page 13-15](#).
- To remove a mount point, select the entry you want removed and click **Delete**.

**Note**

The Delete button immediately removes the selected mount point from the table without further dialogue and renders the named file system inaccessible.

Apply/Reset. Although the addition and changes you make to the field values are reflected immediately on the screen, you must click Apply to save them to the configuration.



Fields in the Add or Edit CIFS Mount Point Dialog Box

The Add or Edit CIFS Mount Point dialog box displays the following fields:

- **Enable mount point**—Enables or disables access to the selected mount point. A check for this option attaches the CIFS file system on the security appliance to the UNIX file tree. Conversely, no check detaches the mount point.
- **Mount-Point Name** Enter or modify the name of an existing file system.
- **Server Name or IP Address**—Enter the predefined name (or the IP address in dotted decimal notation) of the CIFS server.
- **Share Name**—Enter the server share (a folder) by name to access file data within the CIFS server.
- **NT Domain Name**—Enter the predefined Windows NT domain name. A maximum of 63 characters is permitted.
- **User Name**—Enter the name of the user who is authorized for file-system mounting.
- **Password**—Enter the authorized password for file-system mounting.

- Confirm Password—Re-enter the authorized password.

Modes

The following table shows the modes in which this feature is available:

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



Fields in the Add or Edit FTP Mount Point Dialog Box

The Add or Edit FTP Mount Point dialog box displays the following fields:

- **Enable mount point**— Enables or disables access to the selected mount point. A check for this option attaches the FTP file system on the security appliance to the UNIX file tree. Conversely, clearing the checkbox detaches the mount point.
- **Mount-Point Name**— Enter or modify the name of an existing FTP file system.
- **Server Name or IP Address**— Enter the predefined name (or the IP address in dotted decimal notation) of the FTP file-system server.
- **Mode**— Select either Passive or Active FTP Transfer Mode for the FTP Mount option. For more information on FTP Transfer Mode, see [FTP Client](#).
- **Path To Mount**— Enter the directory pathname to the FTP file server. Spaces are not permitted
- **User Name**— Enter the name of the user who is authorized for file-system mounting.
- **Password**— Enter the authorized password for file-system mounting.
- **Confirm Password**— Re-enter the authorized password



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.

Modes

The following table shows the modes in which this feature is available:

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

ICMP

The ICMP Rules pane provides a table that lists the ICMP rules, which specify the addresses of all the hosts or networks that are allowed or denied ICMP access to the security appliance. You can use this table to add or change the hosts or networks that are allowed or prevented from sending ICMP messages to the security appliance.

The ICMP rule list controls ICMP traffic that terminates on any security appliance interface. If no ICMP control list is configured, then the security appliance accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the security appliance does not respond to ICMP echo requests directed to a broadcast address.



Note

Use the **Security Policy** pane to configure access rules for ICMP traffic that is routed *through* the security appliance for destinations on a protected interface.

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 an ICMP control list is configured, 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 control list is not configured; in that case, a **permit** statement is assumed.

Fields

- Interface—Lists the interface on the security appliance from which ICMP access is allowed.
- Action—Displays whether ICMP messages are permitted or not allowed from the specified network or host.
- IP Address—Lists the IP address of the network or host that is allowed or denied access.
- Mask—Lists the network mask associated with the network or host that is allowed access.
- ICMP Type—Lists the type of ICMP message to which the rule applies. [Table 13-1](#) lists the supported ICMP type values.
- Add—Displays the Add ICMP Rule dialog box for adding a new ICMP rule to the end of the table.
- Insert Before—Adds an ICMP rule before the currently selected rule.
- Insert After—Adds an ICMP rule after the currently selected rule.
- Edit—Displays the Edit ICMP Rule dialog box for editing the selected host or network.
- Delete—Deletes the selected host or network.

Table 13-1 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

Table 13-1 ICMP Type Literals (continued)

ICMP Type	Literal
31	conversion-error
32	mobile-redirect

Modes

The following table shows the modes in which this feature is available:

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

Add/Edit ICMP Rule

The Add/Edit ICMP Rule dialog box lets you add or modify an ICMP rule, which specifies the addresses of all the hosts or networks that are allowed or denied ICMP access to the security appliance.

Fields

- ICMP Type—Specifies the type of ICMP message to which the rule applies. [Table 13-2](#) lists the supported ICMP type values.
- Interface—Identifies the interface on the security appliance from which ICMP access is allowed.
- IP Address—Specifies the IP address of the network or host that is allowed or denied access.
- Any Address—Applies the action to all addresses received on the specified interface.
- Mask—Specifies the network mask associated with the network or host that is allowed access.
- Action—Specifies whether ICMP messages are permitted or not from the specified network or host.
 - Permit—Causes ICMP messages from the specified host or network and interface to be allowed.
 - Deny—Causes ICMP messages from the specified host or network and interface to be dropped.

Table 13-2 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

Table 13-2 ICMP Type Literals (continued)

ICMP Type	Literal
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

Modes

The following table shows the modes in which this feature is available:

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

Management Interface

The Management Interface pane lets you enable or disable management interface on a high-security interface and thus lets you perform management functions on the security appliance. With management interface enabled, you can run ASDM on an internal interface with a fixed IP address over an IPsec VPN tunnel. Use this feature if VPN is configured on the security appliance and the external interface is using a dynamically assigned IP address. For example, this feature is helpful for accessing and managing the security appliance securely from home using the VPN client.

Fields

- **Management Interface**—Lets you specify the interface to use for managing the security appliance. None disables management interface and is the default. To enable management interface, select the interface with the highest security, which will be an inside interface. You can enable management interface on only one interface at a time.

Modes

The following table shows the modes in which this feature is available:

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

SNMP

The SNMP pane lets you configure the security appliance for monitoring by Simple Network Management Protocol (SNMP) management stations.

SNMP defines a standard way for network management stations running on PCs or workstations to monitor the health and status of many types of devices, including switches, routers, and the security appliance.

SNMP Terminology

- Management stations—Network management stations running on PCs or workstations, use the SNMP protocol to administer standardized databases residing on the device being managed. Management stations can also receive messages about events, such as hardware failures, which require attention.
- Agent—In the context of SNMP, the management station is a client and an SNMP agent running on the security appliance is a server.
- OID—The SNMP standard assigns a system object ID (OID) so that a management station can uniquely identify network devices with SNMP agents and indicate to users the source of information monitored and displayed.
- MIB—The agent maintains standardized data structures called Management Information Databases, or MIBs which are compiled into management stations. MIBs collect information, such as packet, connection, and error counters, buffer usage, and failover status. MIBs are defined for specific products, in addition to MIBs for the common protocols and hardware standards used by most network devices. SNMP management stations can browse MIBs or request only specific fields. In some applications, MIB data can be modified for administrative purposes.
- Trap—The agent also monitors alarm conditions. When an alarm condition defined in a trap occurs, such as a link up, link down, or syslog event, the agent sends notification, also known as SNMP trap, to the designated management station immediately.

SNMP

For Cisco MIB files and OIDs, refer to:

<http://www.cisco.com/public/sw-center/netmgmt/ctmk/mibs.shtml>. OIDs may be downloaded at this URL: <ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz>.

MIB Support

The security appliance provides the following SNMP MIB support:



Note

The security appliance does not support browsing of the Cisco syslog MIB.

- You can browse the System and Interface groups of MIB-II. Browsing an MIB is different from sending traps. Browsing means doing an snmpget or snmpwalk of the MIB tree from the management station to determine values.
- The Cisco MIB and Cisco Memory Pool MIB are available.
- The security appliance does not support the following in the Cisco MIB:
 - cfwSecurityNotification NOTIFICATION-TYPE
 - cfwContentInspectNotification NOTIFICATION-TYPE
 - cfwConnNotification NOTIFICATION-TYPE
 - cfwAccessNotification NOTIFICATION-TYPE
 - cfwAuthNotification NOTIFICATION-TYPE
 - cfwGenericNotification NOTIFICATION-TYPE

SNMP CPU Utilization

The security appliance supports monitoring CPU utilization through SNMP. This feature allows network administrators to monitor security appliance CPU usage using SNMP management software, such as HP OpenView, for capacity planning.

This functionality is implemented through support for the cpmCPUTotalTable of the Cisco Process MIB (CISCO-PROCESS-MIB.my). The other two tables in the MIB, cpmProcessTable and cpmProcessExtTable, are not supported in this release.

Each row of the cpmCPUTotalTable includes the index of each CPU and the following objects:

MIB object name	Description
cpmCPUTotalPhysicalIndex	The value of this object will be zero because the entPhysicalTable of Entity MIB is not supported on the security appliance SNMP agent.
cpmCPUTotalIndex	The value of this object will be zero because the entPhysicalTable of Entity MIB is not supported on the security appliance SNMP agent.
cpmCPUTotal5sec	Overall CPU busy percentage in the last five-second period.
cpmCPUTotal1min	Overall CPU busy percentage in the last one-minute period.
cpmCPUTotal5min	Overall CPU busy percentage in the last five-minute period.



Note

Because all current security appliance hardware platforms support a single CPU, the security appliance returns only one row from cpmCPUTotalTable and the index is always 1.

The values of the last three elements are the same as the output from the **show cpu usage** command.

The security appliance does not support the following new MIB objects in the cpmCPUTotalTable:

- cpmCPUTotal5secRev
- cpmCPUTotal1minRev
- cpmCPUTotal5minRev

Fields

- Community string (default)—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.
- Contact—Enter 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.
- Security Appliance Location—Specify the security appliance location. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- Listening Port—Specify the port on which SNMP traffic is sent. The default is 161.
- Configure Traps—Lets you configure the events to notify through SNMP traps.
- SNMP Management Stations box:
 - Interface—Displays the security appliance interface name where the SNMP management stations reside.
 - IP Address—Displays the IP address of an SNMP management station to which the security appliance sends trap events and receive requests or polls.
 - Community string—If no community string is specified for a management station, the value set in Community String (default) field will be used.
 - SNMP Version—Displays the version of SNMP set on the management station.
 - Poll/Trap—Displays the method for communicating with this management station, poll only, trap only, or both trap and poll. Polling means that the security appliance waits for a periodic request from the management station. The trap setting sends syslog events when they occur.
 - UDP Port—SNMP host UDP port. The default is port 162.
- Add—Opens Add SNMP Host Access Entry with these fields:
- Interface Name—Select the interface on which the management station resides.
- IP Address—Specify the IP address of the management station.
- Server Poll/Trap Specification—Select Poll, Trap, or both.
- UDP Port—UDP port for the SNMP host. This field allows you to override the default value of 162 for the SNMP host UDP port.
- Help—Provides more information.
- Edit—Opens the Edit SNMP Host Access Entry dialog box with the same fields as Add.
- Delete—Deletes the selected item.

Modes

The following table shows the modes in which this feature is available:

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

Add/Edit SNMP Host Access Entry

Adding SNMP Management Stations

To add SNMP management stations, perform the following steps:

1. Click **Add** to open the SNMP Host Access Entry dialog box.
2. From Interface Name, select the interface on which the SNMP management station resides.
3. Enter the IP address of that management station in IP Address.
4. Enter the UDP port for the SNMP host. The default is 162.
5. Enter the Community String password for the SNMP host. If no community string is specified for a management station, the value set in Community String (default) field in the SNMP Configuration screen will be used.
6. Click to select **Poll**, **Trap**, or both.
7. To return to the previous pane click:
 - **OK**—Accepts changes and returns to the previous pane
 - **Cancel**—Discards changes and returns to the previous pane
 - **Help**—Provides more information

Editing SNMP Management Stations

To edit SNMP management stations, perform the following steps:

1. Select a list item from the SNMP management station table on the SNMP pane.
2. Click **Edit** to open Edit SNMP Host Access Entry.
3. From Interface Name, select the interface on which the SNMP management station resides.
4. Enter the IP address of that management station in IP Address.
5. Enter the Community String password for the SNMP host. If no community string is specified for a management station, the value set in Community String (default) field in the SNMP Configuration screen will be used.
6. Enter the UDP port for the SNMP host. The default is 162.
7. Click to select **Poll**, **Trap**, or both.
8. Select SNMP version.
9. To return to the previous pane click:
 - **OK**—Accepts changes and returns to the previous pane
 - **Cancel**—Discards changes and returns to the previous pane
 - **Help**—Provides more information

Deleting SNMP Management Stations

To delete an SNMP management station from the table, perform the following steps:

1. Select an item from the SNMP management station table on the SNMP pane.
2. Click **Delete**.

Fields

- Interface name—Select the interface where the SNMP host resides.
- IP Address—Enter the IP address of the SNMP host.
- UDP Port—Enter the UDP port on which to send SNMP updates. The default is 162.
- Community String—Enter the community string for the SNMP server.
- SNMP Version—Select the SNMP version.
- Server Port/Trap Specification
 - Poll—Select to send poll information. Polling means that the security appliance waits for a periodic request from the management station.
 - Trap—Select to send trap information. The trap setting sends syslog events when they occur.
- OK—Accepts changes and returns to the previous pane
- Cancel—Discards changes and returns to the previous pane
- Help—Provides more information

Modes

The following table shows the modes in which this feature is available:

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

SNMP Trap Configuration

Traps

Traps are different than browsing; they are unsolicited “comments” from the managed device to the management station for certain events, such as link up, link down, and syslog event generated.

An SNMP object ID (OID) for the security appliance displays in SNMP event traps sent from the security appliance. The security appliance provides system OID in SNMP event traps & SNMP mib-2.system.sysObjectID.

The SNMP service running on the security appliance performs two different functions:

- Replies to SNMP requests from management stations (also known as SNMP clients).
- Sends traps (event notifications) to management stations or other devices that are registered to receive them from the security appliance.

The security appliance supports 3 types of traps:

- firewall

- generic
- syslog

Configure Traps

Opens SNMP Trap Configuration with the following fields:

- Standard SNMP Traps—Select standard traps to send:
 - Authentication—Enables authentication standard trap.
 - Cold Start—Enables cold start standard trap.
 - Link Up—Enables link up standard trap.
 - Link Down—Enables link down standard trap.
- Entity MIB Notifications
 - FRU Insert—Enables a trap notification when a Field Replaceable Unit (FRU) has been inserted.
 - FRU Remove—Enables a trap notification when a Field Replaceable Unit (FRU) has been removed.
 - Configuration Change—Enables a trap notification when there has been a hardware change.
- IPsec Traps—Enables IPsec traps.
 - Start—Enables a trap when IPsec starts.
 - Stop—Enables a trap when IPsec stops.
- Remote Access Traps—Enables remote access traps.
 - Session threshold exceeded—Enables a trap when the number of remote access session attempts exceeds the threshold configured.
- Enable Syslog traps—Enables sending of syslog messages to SNMP management station.
- OK—Accepts changes and returns to the previous pane.
- Cancel—Discards changes and returns to the previous pane.
- Help—Provides more information.

Modes

The following table shows the modes in which this feature is available:

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

Management Access Rules

The Management Access Rules pane lets you define an access rule associated with an interface. 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 instance, in addition to detecting IKE Denial of Service attacks, you can block them using management access rules.

Fields

Note: You can adjust the table column widths by moving your cursor over a column line until it turns into a double arrow. Click and drag the column line to the desired size.

- Add—Adds a new management access rule.
- Edit—Edits a management access rule.
- Delete—Deletes a management access rule.
- Move Up—Moves a rule up. Rules are assessed in the order they appear in this table, so the order can matter if you have overlapping rules.
- Move Down—Moves a rule down.
- Cut—Cuts a rule.
- Copy—Copies the parameters of a rule so you can start a new rule with the same parameters using the Paste button.
- Paste—Opens an Add/Edit Rule dialog box with the copied or cut parameters of a rule prefilled. You can then make any modifications and add it to the table. The Paste button adds the rule above the selected rule. The Paste After item, available from the Paste drop-down list, adds the rule after the selected rule.

The following description summarizes the columns in the Management Access Rules table. You can edit the contents of these columns by double-clicking on a table row. Rules are displayed in the order of execution. If you right-click a rule, you see all of the options represented by the buttons above, as well as Insert and Insert After items. These items either insert a new rule before the selected rule (Insert) or after the selected rule (Insert After.)

- No—Indicates the order of evaluation for the rule.
- Enabled—Indicates whether the rule is enabled or disabled.
- Source—Specifies the IP address, network object group, interface IP, or any, from which traffic is permitted or denied to the destination specified in the Destination Type field. An address column might contain an interface name with the word any, such as inside:any. This means that any host on the inside interface is affected by the rule.
- Service—Shows the service or protocol specified by the rule.
- Action—The action that applies to the rule, either Permit or Deny.
- Logging—If you enable logging for the access list, this column shows the logging level and the interval in seconds between log messages.
- Time—Displays the time range during which the rule is applied.
- Description—Shows the description you entered when you added the rule. An implicit rule includes the following description: “Implicit outbound rule.”

Modes

The following table shows the modes in which this feature is available:

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

Add/Edit Management Access Rules

The Add/Edit Management Access Rule dialog box lets you create a new management rule, or modify an existing management rule.

- **Interface**—Specifies the interface to which the rule applies.
- **Action**—Determines the action type of the new rule. Select either permit or deny.
 - **Permit**—Permits all matching traffic.
 - **Deny**—Denies all matching traffic.
- **Source**—Specifies the IP address, network object group, interface IP, or any, from which traffic is permitted or denied to the destination specified in the Destination field.
 - ...—Lets you select, add, edit, delete, or find an existing IP address object, IP name, network object group, or all.
- **Destination**—Specifies the IP address, network object group, interface IP, or any, to which traffic is permitted or denied from the source specified in the Source Type field.
 - ...—Lets you select, add, edit, delete, or find an existing IP address object, IP name, network object group, or all.
- **Service**—Choose this option to specify a port number, a range of ports, or a well-known service name or group from a list of services.
 - ...—Lets you select, add, edit, delete, or find an existing service from a preconfigured list.
- **Description**—(Optional) Enter a description of the management access rule.
- **Enable Logging**—Enables logging for the access list.
 - **Logging Level**—Specifies default, emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
- **More Options**—Shows additional configuration options for the rule.
 - **Enable Rule**—Enables or disables the rule.
 - **Traffic Direction**—Determines which direction of traffic the rule is applied. Options are either incoming or outgoing.
 - **Source Service**—Specifies a source protocol and service (TCP or UDP service only).
 - ...—Lets you select, add, edit, delete or find a source service from a preconfigured list.
 - **Logging Interval**—Specifies the interval for logging in seconds if logging is configured.
 - **Time Range**—Specifies a time range defined for this rule from the drop-down list.
 - ...—Lets you select, add, edit, delete or find a time range from a preconfigured list.

Modes

The following table shows the modes in which this feature is available:

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

Modes

The following table shows the modes in which this feature is available:

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

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 “[Configuring the Local Database](#)” section on page 12-7 or the “[Identifying AAA Server Groups and Servers](#)” section on page 12-12.

This section includes the following topics:

- [Configuring Authentication for CLI, ASDM, and enable command Access](#), page 13-27
- [Limiting User CLI and ASDM Access with Management Authorization](#), page 13-28
- [Configuring Command Authorization](#), page 13-29
- [Configuring Management Access Accounting](#), page 13-37
- [Recovering from a Lockout](#), page 13-38

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 “[Secure Shell](#)” section on page 13-4, “[Telnet](#)” section on page 13-6, or “[HTTPS/ASDM](#)” section on page 13-1. 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 13-32 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.
 - admin—Allows full access to any services specified by the Authentication tab options.
 - 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.
 - 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).
- 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 the [“Add/Edit User Account > Identity”](#) section on page 12-9. 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 13-30](#)
- [Configuring Local Command Authorization, page 13-32](#)
- [Configuring TACACS+ Command Authorization, page 13-34](#)

Command Authorization Overview

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

- [Supported Command Authorization Methods, page 13-30](#)
- [About Preserving User Credentials, page 13-30](#)
- [Security Contexts and Command Authorization, page 13-31](#)

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 an LDAP Attribute Map”](#) section on page 12-21.)

This section includes the following topics:

- [Local Command Authorization Prerequisites](#), page 13-32
- [Default Command Privilege Levels](#), page 13-32
- [Assigning Privilege Levels to Commands and Enabling Authorization](#), page 13-33

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 13-27.)

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 [“Configuring the Local Database”](#) section on page 12-7.
 - 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 an LDAP Attribute Map”](#) section on page 12-21.

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 the **Enable authorization for command access > Enable** check box.
- 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 the **Configure Command Privileges** button.
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 the **Perform authorization for exec shell access > Enable** check box.

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 13-28 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 13-38.

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 13-29.

This section includes the following topics:

- [TACACS+ Command Authorization Prerequisites](#), page 13-34
- [Configuring Commands on the TACACS+ Server](#), page 13-34
- [Enabling TACACS+ Command Authorization](#), page 13-37

TACACS+ Command Authorization Prerequisites

Configure CLI and **enable** authentication (see the [“Configuring Authentication for CLI, ASDM, and enable command Access”](#) section on page 13-27).

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:

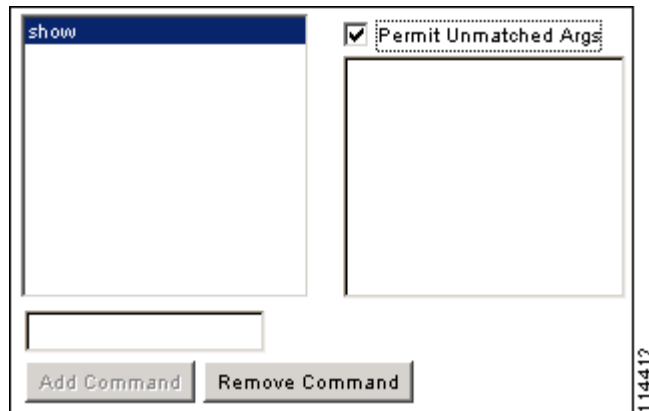
- The security appliance sends the commands to be authorized as “shell” commands, so configure the commands on the TACACS+ server as shell commands.



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

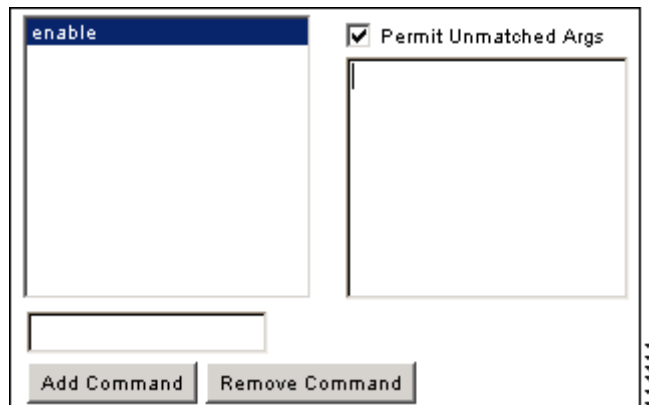
- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by **permit** or **deny**.
For example, to allow the **show running-configuration aaa-server** command, add **show running-configuration** to the command 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 13-1](#)).

Figure 13-1 Permitting All Related Commands



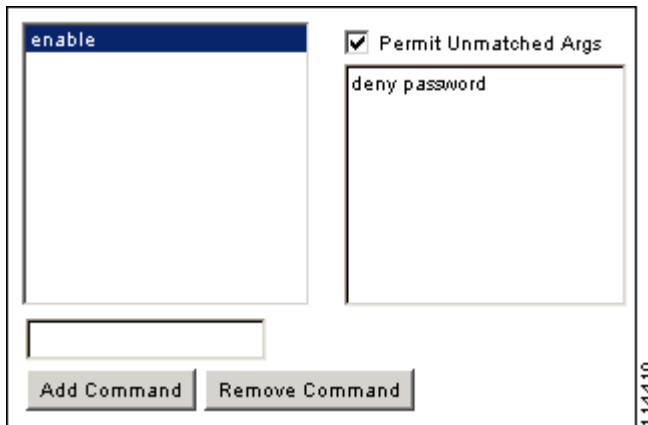
- For commands that are a single word, you *must* permit unmatched arguments, even if there are no arguments for the command, for example **enable** or **help** (see [Figure 13-2](#)).

Figure 13-2 Permitting Single Word Commands



- 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 13-3](#)).

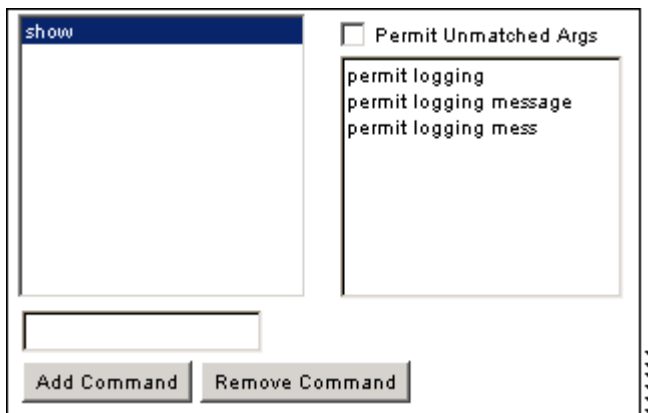
Figure 13-3 Disallowing Arguments



- 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 13-4](#)).

Figure 13-4 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 13-27](#).
 - 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 security appliance 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 13-33), 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 13-3](#) lists the common lockout conditions and how you might recover from them.

Table 13-3 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 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.

Table 13-3 *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 security appliance immediately, then log into the maintenance partition 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 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.