

Management Access

This chapter describes how to access the ASA for system management through Telnet, SSH, and HTTPS (using ASDM), how to authenticate and authorize users, and how to create login banners.

This chapter includes the following sections:

- Configuring ASA Access for ASDM, Telnet, or SSH, page 42-1
- Configuring CLI Parameters, page 42-5
- Configuring ICMP Access, page 42-8
- Configuring Management Access Over a VPN Tunnel, page 42-11
- Configuring AAA for System Administrators, page 42-12
- Monitoring Device Access, page 42-32
- Feature History for Management Access, page 42-33

Note To access the ASA interface for management access, you do not also need an access rule allowing the host IP address. You only need to configure management access according to the sections in this chapter.

Configuring ASA Access for ASDM, Telnet, or SSH

This section describes how to allow clients to access the ASA using ASDM, Telnet, or SSH and includes the following topics:

- Licensing Requirements for ASA Access for ASDM, Telnet, or SSH, page 42-1
- Guidelines and Limitations, page 42-2
- Configuring Management Access, page 42-3
- Using a Telnet Client, page 42-4
- Using an SSH Client, page 42-5

Licensing Requirements for ASA Access for ASDM, Telnet, or SSH

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6.

Model Guidelines

For the ASASM, a session from the switch to the ASASM is a Telnet session, but Telnet access configuration according to this section is not required.

Additional Guidelines

- You cannot use Telnet to the lowest security interface unless you use Telnet inside a VPN tunnel.
- Management access to an interface other than the one from which you entered the ASA is not supported. For example, if your management host is located on the outside interface, you can only initiate a management connection directly to the outside interface. The only exception to this rule is through a VPN connection. See Configuring Management Access Over a VPN Tunnel, page 42-11.
- The ASA allows:
  - A maximum of 5 concurrent Telnet connections per context, if available, with a maximum of 100 connections divided among all contexts.
  - A maximum of 5 concurrent SSH connections per context, if available, with a maximum of 100 connections divided among all contexts.
  - A maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 32 ASDM instances among all contexts.
- The ASA supports the SSH remote shell functionality provided in SSH Versions 1 and 2 and supports DES and 3DES ciphers.
- XML management over SSL and SSH is not supported.
- (8.4 and later) The SSH default username is no longer supported. You can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using Configuration > Device Management > Users/AAA > AAA Access > Authentication; then define a local user by choosing Configuration > Device Management > Users/AAA > User Accounts. If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.

- (9.1(2) and later) The default Telnet login password was removed; you must manually set the password before using Telnet. See Configuring the Hostname, Domain Name, and Passwords, page 17-1.
- If you cannot make a Telnet or SSH connection to the ASA interface, make sure that you enabled Telnet or SSH to the ASA according to the instructions in the Configuring ASA Access for ASDM, Telnet, or SSH, page 42-1.
- The AES-CTR encryption for SSH supports only AES-128 on single-core platforms, which includes the ASA 5505.

Configuring Management Access

To identify the client IP addresses allowed to connect to the ASA using Telnet, SSH, or ASDM, perform the following steps.

Prerequisites

In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, in the Configuration > Device List pane, double-click the context name under the active device IP address.

Detailed Steps

Step 1 In ASDM, choose **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**, and click **Add**.

The Add Device Access Configuration dialog box appears.

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, enter 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 Click **OK**.

Step 7 Configure HTTP Settings.

a. Enable HTTP Server—Enable the HTTP server for ASDM access. This is enabled by default.

b. (Optional) Port Number—The default port is 443.

c. (Optional) Idle Timeout—The default idle timeout is 20 minutes.

d. (Optional) Session Timeout—By default, the session timeout is disabled. ASDM connections have no session time limit.

e. (Optional) Require client certificate to access ASDM on the following interfaces—Specify the interface from the drop-down list.

Step 8 (Optional) Configure Telnet Settings.

a. Telnet Timeout—The default timeout value is 5 minutes.

Step 9 (Optional) Configure SSH Settings.

a. Allowed SSH Version(s)—The default value is 1 & 2.

b. SSH Timeout—The default timeout value is 5 minutes.

c. DH Key Exchange—Click the applicable radio button to choose Diffie-Hellman (DH) Key Exchange Group 1 or Group 14. Both the DH Group 1 and Group 14 key-exchange methods for key exchange are supported on the ASA. If no DH group key-exchange method is specified, the DH group 1 key-exchange method is used. For more information about using DH key-exchange methods, see RFC 4253.

Step 10 Click **Apply**.

The changes are saved to the running configuration.

Step 11 (Required for Telnet) Set a login password before you can connect with Telnet; there is no default password.

a. Choose **Configuration > Device Setup > Device Name/Password**.

b. In the Telnet Password area, check the **Change the password to access the console of the security appliance** checkbox.

c. Enter the old password (for a new ASA, leave this field blank), new password, and then confirm the new password.

d. Click **Apply**.

Step 12 (Required for SSH) Configure SSH user authentication.

a. Choose **Configuration > Device Management > Users/AAA > AAA Access > Authentication**.

b. Check the **SSH** check box.

c. From the Server Group drop-down list, choose the **LOCAL** database. You can alternatively configure authentication using a AAA server.

d. Click **Apply**.

e. Add a local user. Choose **Configuration > Device Management > Users/AAA > User Accounts**, and then click **Add**.

The Add User Account-Identity dialog box appears.

f. Enter a username and password, and then confirm the password.

g. Click **OK,** then click **Apply**.

Using a Telnet Client

To gain access to the ASA CLI using Telnet, enter the login password. You must manually set the password before using Telnet. See Configuring the Hostname, Domain Name, and Passwords, page 17-1.

If you configure Telnet authentication (see Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18), then enter the username and password defined by the AAA server or local database.

Using an SSH Client

In the SSH client on your management host, enter the username and password. When starting an SSH session, a dot (.) displays on the ASA console before the following SSH user authentication prompt appears:

```
ciscoasa(config)#.
```

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

You can alternatively configure a public key instead of using a password. See Adding a User Account to the Local Database, page 34-3.

Configuring CLI Parameters

This section includes the following topics:

- Licensing Requirements for CLI Parameters, page 42-5
- Guidelines and Limitations, page 42-5
- Configuring a Login Banner, page 42-6
- Customizing a CLI Prompt, page 42-7
- Changing the Console Timeout, page 42-8

Licensing Requirements for CLI Parameters

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

Configuring a Login Banner

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

Restrictions

After a banner is added, Telnet or SSH sessions to ASA may close if:

- There is not enough system memory available to process the banner message(s).
- A TCP write error occurs when trying to display banner message(s).

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.

To configure a login banner, perform the following steps:

Detailed Steps

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

- The session (exec) banner appears when a user accesses privileged EXEC mode at the CLI.
- The login banner appears when a user logs in to the CLI.
- The message-of-the-day (motd) banner appears when a user first connects to the CLI.
- The ASDM banner appears when a user connects to ASDM, after user authentication. The user is given two options for dismissing the banner:
  - Continue—Dismiss the banner and complete login.
  - Disconnect—Dismiss the banner and terminate the connection.
- Only ASCII characters are allowed, including a 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 ASA 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.

Step 2 Click **Apply**.

The new banner is 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 ASA. In multiple context mode, the prompt also displays the context name. You can display the following items in the CLI prompt:

cluster-unit	(Single and multiple mode) Displays the cluster unit name. Each unit in a cluster can have a unique name.
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 appear for the state: • 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 another inactive 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 condition might occur when there is an interface failure above the threshold on the standby unit. Shows the role (master or slave) of a unit in a cluster. For example, in the prompt ciscoasa/cl2/slave, the hostname is ciscoasa, the unit name is cl2, and the state name is slave.

Detailed Steps

To customize the CLI prompt, perform the following steps:

Step 1 Choose **Configuration > Device Management > Management Access > Command Line (CLI) > CLI Prompt**, then 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

The console timeout sets how long a connection can remain in privileged EXEC mode or configuration mode; when the timeout is reached, the session drops into user EXEC mode. By default, the session does not time out. This setting does not affect how long you can remain connected to the console port, which never times out.

To change the console timeout, perform the following steps:

Detailed Steps

Step 1 To define a new timeout value in minutes, choose **Configuration > Device Management > Management Access > Command Line (CLI) > Console Timeout**.

Step 2 To specify an unlimited amount of time, enter **0**. The default value is 0.

Step 3 Click **Apply**.

The timeout value is changed and the change is saved to the running configuration.

Configuring ICMP Access

By default, you can send ICMP packets to any ASA interface using either IPv4 or IPv6. This section tells how to limit ICMP management access to the ASA. You can protect the ASA from attacks by limiting the addresses of hosts and networks that are allowed to have ICMP access to the ASA.

Note For allowing ICMP traffic through the ASA, seethe firewall configuration guide.

This section includes the following topics:

- Information About ICMP Access, page 42-9
- Licensing Requirements for ICMP Access, page 42-9
- Guidelines and Limitations, page 42-9
- Default Settings, page 42-10
- Configuring ICMP Access, page 42-10

Information About ICMP Access

ICMP in IPv6 functions the same as ICMP in IPv4. ICMPv6 generates error messages, such as ICMP destination unreachable messages and informational messages like ICMP echo request and reply messages. Additionally ICMP packets in IPv6 are used in the IPv6 neighbor discovery process and path MTU discovery.

We recommend that you always grant permission 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 ASA uses a first match to the ICMP traffic followed by an implicit deny all entry. 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 ASA 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.

Licensing Requirements for ICMP Access

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines

- The ASA does not respond to ICMP echo requests directed to a broadcast address.
- The ASA only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.
- If you cannot ping the ASA interface, make sure that you enable ICMP to the ASA for your IP address using the **icmp** command.

Default Settings

By default, you can send ICMP packets to any ASA interface using either IPv4 or IPv6.

Configuring ICMP Access

To configure ICMP access rules, perform the following steps:

Detailed Steps

Step 1 Choose **Configuration > Device Management > Management Access > ICMP**, and click **Add**.

Step 2 Choose which version of IP traffic to filter by clicking the applicable radio button:

- **Both** (filters IPv4 and IPv6 traffic)
- **IPv4** only
- **IPv6** only

Step 3 If you want to insert a rule into the ICMP table, select the rule that the new rule will precede, and click **Insert**.

The Create ICMP Rule dialog box appears in the right-hand pane.

Step 4 From the ICMP Type drop-down list, choose the type of ICMP message for this rule.

Step 5 From the Interface list, choose the destination ASA interface to which the rule is to be applied.

Step 6 In the IP Address field, do one of the following:

- Add a specific IP address for the host or network.
- Click **Any Address,** then go to Step 9.

Step 7 From the Mask drop-down list, choose the network mask.

Step 8 Click **OK**.

The Create ICMP Rule dialog box closes.

Step 9 (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 ASA that shows the ASA 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 10 Click **Apply**.

The ICMP rule is added to the ASA, and the change is saved to the running configuration.

Configuring Management Access Over a VPN Tunnel

If your VPN tunnel terminates on one interface, but you want to manage the ASA by accessing a different interface, you can identify that interface as a management-access interface. For example, if you enter the ASA from the outside interface, this feature lets you connect to the inside interface using ASDM, SSH, Telnet, or SNMP; or you can ping the inside interface when entering from the outside interface. Management access is available via the following VPN tunnel types: IPsec clients, IPsec site-to-site, and the AnyConnect SSL VPN client.

This section includes the following topics:

- Licensing Requirements for a Management Interface, page 42-11
- Guidelines and Limitations, page 42-2
- Configuring a Management Interface, page 42-12

Licensing Requirements for a Management Interface

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single mode.

Firewall Mode Guidelines

Supported in routed mode.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines

You can define only one management access interface.

Note For the configurations that follow, 192.168.10.0/24 is the VPN pool for AnyConnect or IPsec VPN clients. Each configuration allows VPN client users to connect to ASDM or SSH to the ASA using the management interface IP address.

To allow only VPN client users access to ASDM or HTTP (and deny access to all other users), enter the following commands:

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.10.0 255.255.255.0 management_interface
```

To allow only VPN client users access to the ASA using SSH (and deny access to all other users), enter the following command:

```
ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface
```

Configuring a Management Interface

To configure the management interface, perform the following steps.

Detailed 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 AAA for System Administrators

This section describes how to enable authentication and command authorization for system administrators.

- Information About AAA for System Administrators, page 42-12
- Licensing Requirements for AAA for System Administrators, page 42-16
- Prerequisites, page 42-16
- Guidelines and Limitations, page 42-17
- Default Settings, page 42-17
- Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18
- Limiting User CLI and ASDM Access with Management Authorization, page 42-19
- Configuring a Password Policy for Local Database Users, page 42-21
- Configuring Command Authorization, page 42-24
- Configuring Management Access Accounting, page 42-29
- Viewing the Currently Logged-In User, page 42-29
- Setting a Management Session Quota, page 42-30
- Recovering from a Lockout, page 42-31

Information About AAA for System Administrators

This section describes AAA for system administrators and includes the following topics:

- Information About Management Authentication, page 42-13

- Information About Command Authorization, page 42-14

Information About Management Authentication

This section describes authentication for management access and includes the following topics:

- Comparing CLI Access with and without Authentication, page 42-13
- Comparing ASDM Access with and without Authentication, page 42-13
- Authenticating Sessions from the Switch to the ASA Services Module, page 42-13

Comparing CLI Access with and without Authentication

How you log into the ASA depends on whether or not you enable authentication:

- No Authentication—If you do not enable any authentication for Telnet, you do not enter a username; you enter the login password. (SSH is not available without authentication). You access user EXEC mode.
- Authentication—If you enable Telnet or SSH authentication according to this section, you enter the username and password as defined on the AAA server or local user database. You access user EXEC mode.

To enter privileged EXEC mode after logging in, enter the **enable** command. How **enable** works depends on whether you enable authentication:

- No Authentication—If you do not configure enable authentication, enter the system enable password when you enter the **enable** 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.
- Authentication—If you configure enable authentication, the ASA prompts you for your username and password again. This feature is particularly useful when you perform command authorization, in which usernames are important in determining the commands that a user can enter.

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

Comparing ASDM Access with and without Authentication

By default, you can log into ASDM with a blank username and the enable password. Note that if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

If you configure HTTP authentication, you can no longer use ASDM with a blank username and the enable password.

Authenticating Sessions from the Switch to the ASA Services Module

For sessions from the switch to the ASASM (using the **session** command), you can configure Telnet authentication. For virtual console connections from the switch to the ASASM (using the **service-module session** command), you can configure serial port authentication.

In multiple context mode, you cannot configure any AAA commands in the system configuration. However, if you configure Telnet or serial authentication in the admin context, then authentication also applies to sessions from the switch to the ASASM. The admin context AAA server or local user database is used in this instance.

Information About Command Authorization

This section describes command authorization and includes the following topics:

- Supported Command Authorization Methods, page 42-14
- About Preserving User Credentials, page 42-14
- Security Contexts and Command Authorization, page 42-15

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the ASA. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the ASA 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 assigned 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 ASA 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 ASA places you in level *n*. These levels are not used unless you enable local command authorization (see Configuring Local Command Authorization, page 42-24). (See the command reference for more information about the **enable** command.)

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

About Preserving User Credentials

When a user logs into the ASA, that user is required to provide a username and password for authentication. The ASA 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 for 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.

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

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

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 among contexts.

  When configuring command authorization, you must configure each security context separately. This configuration 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 which 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 that they need.

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

Licensing Requirements for AAA for System Administrators

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Prerequisites

Prerequisites for the AAA Server or Local Database

You must configure users in a AAA server or the local database. For a AAA server, you then need to configure the ASA to communicate with it. See the following chapters:

- AAA server—See theapplicable AAA server-type chapter.
- Local Database—SeeAdding a User Account to the Local Database, page 34-3.

Prerequisites for Management Authentication

Before the ASA can authenticate a Telnet, SSH, or HTTP user, you must identify the IP addresses that are allowed to communicate with the ASA. For the ASASM, the exception is for access to the system in multiple context mode; a session from the switch to the ASASM is a Telnet session, but Telnet access configuration is not required. For more information, see Configuring ASA Access for ASDM, Telnet, or SSH, page 42-1.

Prerequisites for Local Command Authorization

- Configure **enable** authentication. (See Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18.)

  enable authentication is essential for maintaining 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.
  - 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 VSA CVPN3000-Privilege-Level according to theConfiguring LDAP Attribute Maps, page 37-5.

Prerequisites for TACACS+ Command Authorization

- Configure CLI and **enable** authentication (see Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18).

Prerequisites for Management Accounting

- Configure CLI and **enable** authentication (see Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18).

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6.

Default Settings

Default Command Privilege Levels

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

To view all privilege levels, see Viewing Local Command Privilege Levels, page 42-25.

Configuring Authentication for CLI, ASDM, and enable command Access

You can require authentication for CLI, ASDM, and enable command access.

Prerequisites

- Configure Telnet, SSH, or HTTP access according to the Configuring ASA Access for ASDM, Telnet, or SSH, page 42-1.
- For SSH access, you must configure SSH authentication; there is no default username.

Detailed Steps

Step 1 To authenticate users who use the **enable** command, choose **Configuration > Device Management > Users/AAA > AAA Access > Authentication**, and configure the following settings:

a. Check the **Enable** check box.

b. From the Server Group drop-down list, choose a server group name or the LOCAL database.

c. (Optional) If you chose a AAA server, you can configure the ASA 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 ASA prompt does not give any indication of which method is being used.

Step 2 To authenticate users who access the CLI or ASDM, choose **Configuration > Device Management > Users/AAA > AAA Access > Authentication**, and configure the following settings:

a. Check one or more of the following check boxes:

- **HTTP/ASDM**—Authenticates the ASDM client that accesses the ASA using HTTPS. HTTP management authentication does not support the SDI protocol for a AAA server group.
- **Serial**—Authenticates users who access the ASA using the console port. For the ASASM, this parameter affects the virtual console accessed from the switch using the **service-module session** command. For multiple mode access, see Authenticating Sessions from the Switch to the ASA Services Module, page 42-13.
- **SSH**—Authenticates users who access the ASA using SSH.
- **Telnet**—Authenticates users who access the ASA using Telnet. For the ASASM, this parameter also affects the session from the switch using the **session** command. For multiple mode access, see Authenticating Sessions from the Switch to the ASA Services Module, page 42-13.

b. For each service that you checked, from the Server Group drop-down list, choose a server group name or the LOCAL database.

c. (Optional) If you chose a AAA server, you can configure the ASA 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 ASA prompt does not give any indication of which method is being used.

Step 3 Click **Apply**.

Limiting User CLI and ASDM Access with Management Authorization

The ASA enables you to distinguish between administrative and remote-access users when they authenticate using RADIUS, LDAP, TACACS+, or the local user database. User role differentiation can prevent remote access VPN and network access users from establishing an administrative connection to the ASA.

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.

Detailed Steps

Step 1 Choose one of the following options:

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

  When the **LOCAL** option is configured, the local user database is the source for the username entered and the Service-Type and Privilege-Level attributes assigned.

  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 Configuring Local Command Authorization, page 42-24 for more information.

  When the **authentication-server** option is configured, the same server is used for both authentication and authorization.

- To enable management authorization, choose **Configuration > Device Management > Users/AAA > AAA Access > Authorization**, and check the **Allow privileged users to enter into EXEC mode on login** check box.

  The **auto-enable** option allows users with sufficient privileges from the login authentication server to be placed directly in privileged EXEC mode. Otherwise, users are placed in user EXEC mode. These privileges are determined by the Service-Type and Privilege-Level attributes that are required to enter each EXEC mode. To enter privileged EXEC mode, users must have a Service-Type attribute of Administrative and a Privilege Level attribute of greater than 1 assigned to them.

  This option is not supported in the system context. However, if you configure Telnet or serial authentication in the admin context, then authentication also applies to sessions from the switch to the ASASM.

  There is no effect if you enter the **aaa authorization exec** command alone.

  The **auto-enable** option is not included when you use serial authentication in management authorization.

  The **aaa authentication http** command is not affected by the **auto-enable** option.

  Before you configure the **auto-enable** option, we recommend that you configure both protocol login and enable authentication, and that all authentication requests go to the same AAA server group, as shown in the following example:

```
ciscoasa (config)# aaa authentication ssh console RADIUS
ciscoasa (config)# aaa authentication enable console RADIUS
ciscoasa (config)# aaa authorization exec authentication-server auto-enable
```

  We do *not* recommend that you use other types of configurations.

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

When users are authenticated through LDAP, the native LDAP attributes and their values can be mapped to Cisco ASA attributes to provide specific authorization features. Configure Cisco VSA CVPN3000-Privilege-Level with a value between 0 and 15. and then map the LDAP attributes to Cisco VAS CVPN3000-Privilege-Level. For more information, see Configuring LDAP Attribute Maps, page 37-5.

The RADIUS IETF **service-type** attribute, when sent in an access-accept message as the result of a RADIUS authentication and authorization request, is used to designate which type of service is granted to the authenticated user:

- Service-Type 6 (Administrative)—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. The Framed (2) and Login (1) service types are treated the same way.
- Service-Type 5 (Outbound)—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. All other service types (Voice, FAX, and so on) are treated the same way.

The RADIUS Cisco VSA **privilege-level** attribute (Vendor ID 3076, sub-ID 220), when sent in an access-accept message, is used to designate the level of privilege for the user.

When an authenticated user tries administrative access to the ASA through ASDM, SSH, or Telnet, but does not have the appropriate privilege level to do so, the ASA generates syslog message 113021. This message informs the user that the attempted login failed because of inappropriate administrative privileges.

TACACS+ users

Authorization is requested with “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. You are not allowed to access privileged EXEC mode using the **enable** command if your enable privilege level is set to 14 or less.
- FAIL—Denies management access. You 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 for a given username. By default, the access restriction is Full Access, which allows full access to any services specified by the Authentication tab options. For more information, see Adding a User Account to the Local Database, page 34-3.

Configuring a Password Policy for Local Database Users

When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters.

The password policy only applies to administrative users using the local database, and not to other types of traffic that can use the local database, such as VPN or AAA for network access, and not to users authenticated by a AAA server.

This section includes the following topics:

- Configuring the Password Policy, page 42-21
- Changing Your Password, page 42-23

Configuring the Password Policy

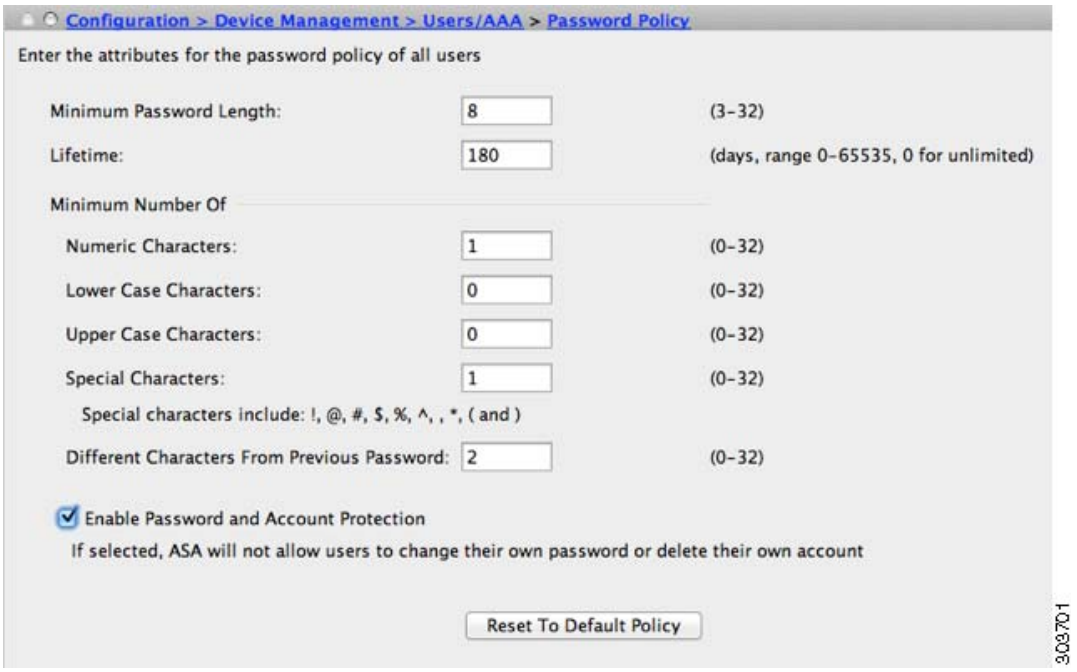
After you configure the password policy, when you change a password (either your own or another user's), the password policy applies to the new password. Any existing passwords are grandfathered in. The new policy applies to changing the password with the User Accounts pane as well as the Change My Password pane.

Prerequisites

- Configure both CLI/ASDM and enable authentication according to the Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18. Be sure to specify the local database.

Detailed Steps

Step 1 Choose **Configuration > Device Management > Users/AAA > Password Policy**.



Step 2 Configure any mix of the following options:

- Minimum Password Length—Enter the minimum length for passwords. Valid values range from 3 to 64 characters. The recommended minimum password length is 8 characters.
- Lifetime—Enter the interval in days after which passwords expire for remote users (SSH, Telnet, HTTP); users at the console port are never locked out due to password expiration. Valid values are between 0 and 65536 days. The default value is 0 days, a value indicating that passwords will never expire.

  7 days before the password expires, a warning message appears. After the password expires, system access is denied to remote users. To gain access after expiration, do one of the following:

  - Have another administrator change your password.
  - Log in to the physical console port to change your password.
- Minimum Number Of—Specify the minimum of characters from the following types:
  - Numeric Characters—Enter the minimum number of numeric characters that passwords must have. Valid values are between 0 and 64 characters. The default value is 0.
  - Lower Case Characters—Enter the minimum number of lower case characters that passwords must have. Valid values range from 0 to 64 characters. The default value is 0.
  - Upper Case Characters—Enter the minimum number of upper case characters that passwords must have. Valid values range from 0 to 64 characters. The default value is 0.
  - Special Characters—Enter the minimum number of special characters that passwords must have. Valid values range from 0 to 64 characters. Special characters include the following: !, @, #, $, %, ^, &, *, '(‘ and ‘)’.The default value is 0.
  - Different Characters from Previous Password—Enter the minimum number of characters that you must change between new and old passwords. Valid values are between 0 and 64 characters. The default value is 0. Character matching is position independent, meaning that new password characters are considered changed only if they do not appear anywhere in the current password.

Step 3 (Optional) Check the **Authentication Enable** check box to require users to change their password on the Change My Password pane instead of the User Accounts pane. The default setting is disabled: a user can use either method to change their password.

If you enable this feature, if you try to change your password on the User Accounts pane, the following error message is generated:

```
ERROR: Changing your own password is prohibited
```

Step 4 To reset the password policy to the default, click **Reset to Default**.

Step 5 Click **Apply** to apply the configuration settings.

Changing Your Password

If you configure a password lifetime in the password policy, you need to change your password to a new one when the old password expires. This password change method is required if you enable password policy authentication. If password policy authentication is not enabled, then you can use this method, or you can change your user account directly with the User Accounts pane.

Detailed Steps

Step 1 Choose **Configuration > Device Management > Users/AAA > Change Password**.



Step 2 Enter your old password.

Step 3 Enter your new password.

Step 4 Confirm your new password.

Step 5 Click **Make Change**.

Step 6 Click the **Save** icon to save your changes to the running configuration.

Configuring Command Authorization

If you want to control access to commands, the ASA 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.

You can use one of two command authorization methods:

- Local privilege levels
- TACACS+ server privilege levels

For more information about command authorization, see Information About Command Authorization, page 42-14.

This section includes the following topics:

- Configuring Local Command Authorization, page 42-24
- Viewing Local Command Privilege Levels, page 42-25
- Configuring Commands on the TACACS+ Server, page 42-25
- Configuring TACACS+ Command Authorization, page 42-28

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 the assigned privilege level or below. The ASA 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 following sections for more information:

- Adding a User Account to the Local Database, page 34-3
- Supported Authentication Methods, page 35-2
- Configuring LDAP Attribute Maps, page 37-5

To configure local command authorization, perform the following steps:

Detailed Steps

Step 1 To enable command authorization, choose **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 **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 or 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 commands that appear, 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 ASA 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, mapped LDAP, and TACACS+ users. See Limiting User CLI and ASDM Access with Management Authorization, page 42-19 for more information.

Step 5 Click **Apply**.

The authorization settings are assigned, and the changes are saved to the running configuration.

Viewing Local Command Privilege Levels

The following commands when entered in the Tools > Command Line Interface tool, let you view privilege levels for commands.

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 ASA 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 ASA command authorization.

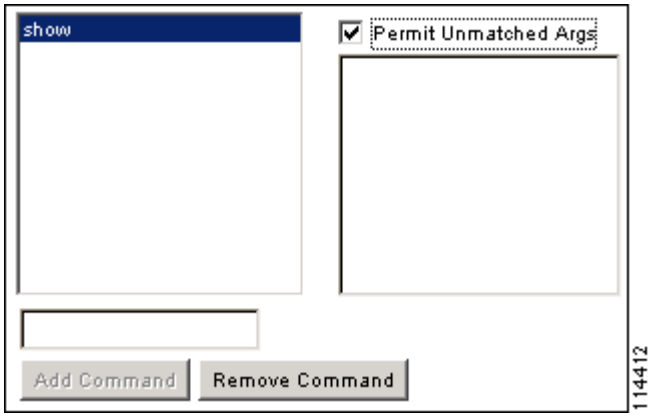
- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by **permit** or **deny**.

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

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

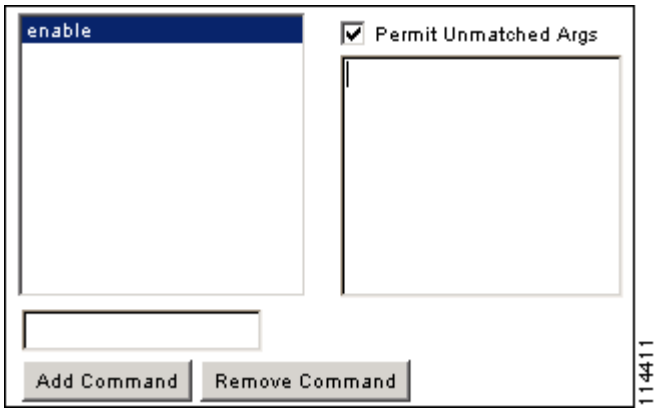
  For example, you can configure just the **show** command, then all the **show** commands are allowed. We recommend using this method so that you do not have to anticipate every variant of a command, including abbreviations and a question mark, which shows CLI usage (see Figure 42-1).

Figure 42-1 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 42-2).

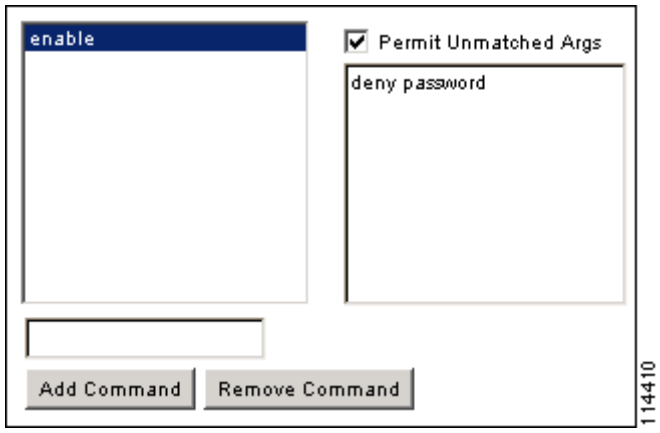
Figure 42-2 Permitting Single Word Commands



- To disallow some arguments, enter the arguments preceded by **deny**.

For example, to allow **enable**, but not **enable password**, enter **enable** in the commands field, and **deny password** in the arguments field. Be sure to check the **Permit Unmatched Args** check box so that **enable** alone is still allowed (see Figure 42-3).

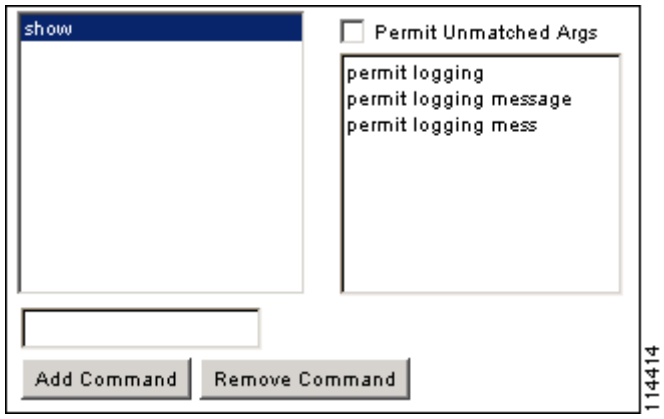
Figure 42-3 Disallowing Arguments



- When you abbreviate a command at the command line, the ASA 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 ASA sends the entire command to the TACACS+ server, **show logging**. However, if you enter **sh log mess**, then the ASA 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 42-4).

Figure 42-4 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**

Configuring TACACS+ Command Authorization

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

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

Do not save your configuration until you are sure that it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the ASA. If you still get locked out, see Recovering from a Lockout, page 42-31.

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 ASA. 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 procedures listed in the Configuring Command Authorization, page 42-24.

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

Detailed Steps

Step 1 To perform command authorization using a TACACS+ server, choose **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 ASA to use the local database as a fallback method if the AAA server is unavailable. To do so, check 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 ASA prompt does not give any indication which method is being used. Be sure to configure users in the local database (see Adding a User Account to the Local Database, page 34-3) and command privilege levels (see Configuring Local Command Authorization, page 42-24).

Step 4 Click **Apply**.

The command authorization settings are assigned, and the changes are saved to the running configuration.

Configuring Management Access Accounting

You can send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI. You can configure accounting when users log in, when they enter the **enable** command, or when they issue commands.

For command accounting, you can only use TACACS+ servers.

To configure management access and enable command accounting, perform the following steps:

Detailed Steps

Step 1 To enable accounting of users when they enter the **enable** command, perform the following steps:

a. Choose **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 2 To enable accounting of users when they access the ASA using Telnet, SSH, or the serial console, perform the following steps:

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 3 To configure command accounting, perform the following steps:

a. Under the Require command accounting area, check the **Enable** check box.

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, you can limit which commands the ASA accounts for by specifying a minimum privilege level in the Privilege level drop-down list. The ASA does not account for commands that are below the minimum privilege level.

Step 4 Click **Apply**.

The accounting settings are assigned, and the changes are saved to the running configuration.

Viewing the Currently Logged-In User

To view the current logged-in user, in the Tools > Command Line Interface tool:

```
ciscoasa# show curpriv
```

Examples

The following is sample output from the **show curpriv** command:

```
ciscoasa# show curpriv
```

```
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

Table 42-1 describes the **show curpriv** command output.

Table 42-1 show curpriv Command Output Description

Field	Description
Username	Username. If you are logged in as the default user, the name is enable_1 (user EXEC) or enable_15 (privileged EXEC).
Current privilege level	Levels range from 0 to 15. Unless you configure local command authorization and assign commands to intermediate privilege levels, levels 0 and 15 are the only levels that are used.
Current Modes	The available access modes are the following: • P_UNPR—User EXEC mode (levels 0 and 1) • P_PRIV—Privileged EXEC mode (levels 2 to 15) • P_CONF—Configuration mode

Setting a Management Session Quota

You can establish a maximum number of simultaneous management sessions. If the maximum is reached, no additional sessions are allowed and a syslog message is generated. To prevent a system lockout, the management session quota mechanism cannot block a console session.

To set a management session quota, perform the following steps:

Step 1 Choose **Configuration > Device Management > Management Access > Management Session Quota**.

Step 2 Enter the maximum number of simultaneous ASDM, SSH, and Telnet sessions that are allowed on the ASA. Valid values range from 0 to 10000.

Note If the management quota session number is exceeded, an error message appears, and ASDM closes.

Step 3 Click **Apply** to save the configuration changes.

Recovering from a Lockout

In some circumstances, when you turn on command authorization or CLI authentication, you can be locked out of the ASA CLI. You can usually recover access by restarting the ASA. However, if you already saved your configuration, you might be locked out. Table 42-2 lists the common lockout conditions and how you might recover from them.

Table 42-2 CLI Authentication and Command Authorization Lockout Scenarios

Feature	Lockout Condition	Description	Workaround: Single Mode	Workaround: Multiple Mode
Local CLI authentication	No users have been configured 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 ASA 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	The server is 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.	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.	1. If the server is unreachable because the network configuration is incorrect on the ASA, session into the ASA 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 that 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.	Fix the TACACS+ server user account. If you do not have access to the TACACS+ server and you need to configure the ASA immediately, then log into the maintenance partition and reset the passwords and **aaa** commands.	Session into the ASA 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 ASA from the switch. From the system execution space, you can change to the context and change the user level.

Monitoring Device Access

To monitor device access, see the following panes:

Path	Purpose
Monitoring > Properties > Device Access > ASDM/HTTPS/Telnet/SSH Sessions	The top pane lists the connection types, session IDs, and IP addresses for users connected through ASDM, HTTPS, and Telnet sessions. To disconnect a specific session, click **Disconnect**. The bottom pane lists the clients, usernames, connection states, software versions, incoming encryption types, outgoing encryption types, incoming HMACs, outgoing HMACs, SSH session IDs, remaining rekey data, remaining rekey time, data-based rekeys, time-based rekeys, and the last rekey time. To disconnect a specific session, click **Disconnect**.
Monitoring > Properties > Device Access > Authenticated Users	Lists the usernames, IP addresses, dynamic ACLs, inactivity timeouts (if any), and absolute timeouts for users who were authenticated by AAA servers.
Monitoring > Properties > Device Access > AAA Local Locked Out Users	Lists the usernames of locked-out AAA local users, the number of failed attempts to authenticate, and the times that users were locked out. To clear a specific user who has been locked out, click **Clear Selected Lockout**. To clear all users who have been locked out, click **Clear All Lockouts**.

Feature History for Management Access

Table 42-3 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 42-3 Feature History for Management Access

Feature Name	Platform Releases	Feature Information
Management Access	7.0(1)	We introduced this feature. We introduced the following screens: Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH Configuration > Device Management > Management Access > Command Line (CLI) > Banner Configuration > Device Management > Management Access > CLI Prompt Configuration > Device Management > Management Access > ICMP Configuration > Device Management > Management Access > File Access > FTP Client Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server Configuration > Device Management > Management Access > File Access > Mount-Points Configuration > Device Management > Users/AAA > AAA Access > Authentication Configuration > Device Management > Users/AAA > AAA Access > Authorization Configuration > Device Management > Users/AAA > AAA Access > > Accounting.
Increased SSH security; the SSH default username is no longer supported.	8.4(2)	Starting in 8.4(2), you can no longer connect to the ASA using SSH with the pix or asa username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or Configuration > Device Management > Users/AAA > AAA Access > Authentication (ASDM); then define a local user by entering the **username** command (CLI) or choosing Configuration > Device Management > Users/AAA > User Accounts (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.

Table 42-3 Feature History for Management Access (continued)

Feature Name	Platform Releases	Feature Information
Support for administrator password policy when using the local database	8.4(4.1), 9.1(2)	When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters. We introduced the following screen: Configuration > Device Management > Users/AAA > Password Policy.
Support for SSH public key authentication	8.4(4.1), 9.1(2)	You can enable public key authentication for SSH connections to the ASA on a per-user basis. You can specify a public key file (PKF) formatted key or a Base64 key. The PKF key can be up to 4096 bits. Use PKF format for keys that are too large to for the ASA support of the Base64 format (up to 2048 bits). We introduced the following screens: Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Using PKF. *PKF key format support is only in 9.1(2) and later.*
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	8.4(4.1), 9.1(2)	Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported. We modified the following screen: Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH.
Support for a maximum number of management sessions	8.4(4.1), 9.1(2)	You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions. We introduced the following screen: Configuration > Device Management > Management Access > Management Session Quota.
For the ASASM in multiple context mode, support for Telnet and virtual console authentication from the switch.	8.5(1)	Although connecting to the ASASM from the switch in multiple context mode connects to the system execution space, you can configure authentication in the admin context to govern those connections.
AES-CTR encryption for SSH	9.1(2)	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
Improved SSH rekey interval		An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic. .

Table 42-3 Feature History for Management Access (continued)

Feature Name	Platform Releases	Feature Information
Improved one-time password authentication	9.2(1)	Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once. The **auto-enable** option was added to the **aaa authorization exec** command. We modified the following screen: Configuration > Device Management > Users/AAA > AAA Access > Authorization.