CHAPTER 34

Configuring Management Access

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

This chapter includes the following sections:

- Configuring Device Access for ASDM, Telnet, or SSH, page 34-1
- Configuring CLI Parameters, page 34-6
- Configuring ICMP Access, page 34-8
- Configuring Management Access Over a VPN Tunnel, page 34-10
- Configuring AAA for System Administrators, page 34-10

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

To configure the management IP address for transparent firewall mode, see the "Setting the Management IP Address for a Transparent Firewall" section on page 7-12.

Configuring Device Access for ASDM, Telnet, or SSH

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

- Configuring Telnet Access, page 34-2
- Configuring SSH Access, page 34-3
- Using an SSH Client, page 34-4
- Configuring HTTPS Access for ASDM, page 34-5

Configuring Telnet Access

The adaptive security appliance allows Telnet connections to the adaptive security appliance for management purposes. To gain access to the adaptive security appliance console using Telnet, enter the username **asa** and the login password set by the **password** command or log in by using the **aaa authentication telnet console** command.

Restrictions

You cannot use Telnet to the lowest security interface unless you use Telnet inside an IPsec tunnel.

The adaptive security appliance allows a maximum of 5 concurrent Telnet connections per context, if available, with a maximum of 100 connections divided between all contexts.

Management access to an interface other than the one from which you entered the adaptive security appliance 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, and entering the **management-access** command. For more information about the **management-access** command, see the *Cisco ASA 5500 Series Command Reference*.

Detailed Steps

To configure Telnet access, perform the following steps:

	Command	Purpose
Step 1	**telnet** *source_IP_address mask source_interface* **Example:** `hostname(config)# telnet 192.168.1.2 255.255.255.255 inside`	Identifies the IP addresses from which the adaptive security appliance accepts connections. Make sure that you perform this step for each address or subnet. If there is only one interface, you can configure Telnet to access that interface as long as the interface has a security level of 100.
Step 2	**telnet timeout** *minutes* **Example:** `hostname(config)# telnet timeout 30`	(Optional) Sets the duration for how long a Telnet session can be idle before the adaptive security appliance disconnects the session. Set the timeout from 1 to 1440 minutes. The default is 5 minutes. The default duration is too short in most cases, and should be increased until all pre-production testing and troubleshooting has been completed.

Examples

The following example allows a host on the inside interface with an address of 192.168.1.2 to access the adaptive security appliance:

```
hostname(config)# telnet 192.168.1.2 255.255.255.255 inside
hostname(config)# telnet timeout 30
```

The following example allows all users on the 192.168.3.0 network to access the adaptive security appliance on the inside interface:

```
hostname(config)# telnet 192.168.3.0 255.255.255.0 inside
```

Configuring SSH Access

The adaptive security appliance allows SSH connections to the adaptive security appliance for management purposes. To gain access to the adaptive security appliance console using SSH, at the SSH client prompt, enter the username **asa** and the login password set by the **password** command or log in by using the **aaa authentication telnet console** command.

Restrictions

The adaptive security appliance allows a maximum of 5 concurrent SSH connections per context, if available, with a maximum of 100 connections divided between all contexts.

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

Note XML management over SSL and SSH are not supported.

In addition, management access to an interface other than the one from which you entered the adaptive security appliance 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, and entering the **management-access** command. For more information about the **management-access** command, see the *Cisco ASA 5500 Series Command Reference*.

Detailed Steps

To configure SSH access, perform the following steps:

	Command	Purpose
Step 1	**crypto key generate rsa modulus** *modulus_size* **Example:** `hostname(config)# crypto key generate rsa modulus 1024`	Generates an RSA key pair, which is required for SSH. The modulus (in bits) is 512, 768, 1024, or 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA. We recommend a value of 1024.
Step 2	**write mem** **Example:** `hostname(config)# write mem`	Saves the RSA keys to persistent flash memory.

	Command	Purpose
Step 3	**ssh** *source_IP_address mask source_interface* **Example:** `hostname(config)# ssh 192.168.1.2 255.255.255.255 inside`	Identifies the IP addresses from which the adaptive security appliance accepts connections. Make sure that you perform this step for each address or subnet. The adaptive security appliance accepts SSH connections from all interfaces, including the one with the lowest security level.
Step 4	**ssh timeout** *minutes* **Example:** `hostname(config)# ssh timeout 30`	(Optional) Sets the duration for how long an SSH session can be idle before the adaptive security appliance disconnects the session. Sets the timeout from 1 to 60 minutes. The default is 5 minutes. The default duration is too short in most cases and should be increased until all preproduction testing and troubleshooting has been completed.

Examples

The following example generates RSA keys and allows a host on the inside interface with an address of 192.168.1.2 to access the adaptive security appliance:

```
hostname(config)# crypto key generate rsa modulus 1024
hostname(config)# write mem
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh timeout 30
```

The following example allows all users on the 192.168.3.0 network to access the adaptive security appliance on the inside interface:

```
hostname(config)# ssh 192.168.3.0 255.255.255.0 inside
```

By default, SSH allows both Versions 1 and 2. The following example specifies the version number:

```
hostname(config)# ssh version version_number
```

The *version_number* can be *1* or *2*.

Using an SSH Client

To gain access to the adaptive security appliance console using SSH, at the SSH client, enter the username **asa** and enter the login password set by the **password** command (see the "Configuring the Hostname, Domain Name, and Passwords" section on page 7-1).

When starting an SSH session, a dot (.) displays on the adaptive security appliance console before the SSH user authentication prompt appears, as follows:

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

The display of the dot does not affect the functionality of SSH. The dot appears 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 adaptive security appliance is busy and has not hung.

Configuring HTTPS Access for ASDM

To use ASDM, you need to enable the HTTPS server, and allow HTTPS connections to the adaptive security appliance. All of these tasks are completed if you use the **setup** command. This section describes how to manually configure ASDM access and how to log in to ASDM.

This section includes the following topics:

- Enabling HTTPS Access, page 34-5
- Accessing ASDM from Your PC, page 34-6

Enabling HTTPS Access

To configure ASDM access, perform the following steps:

Restrictions

The adaptive security appliance allows a maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 32 ASDM instances between all contexts.

Management access to an interface other than the one from which you entered the adaptive security appliance 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, and entering the **management-access** command. For more information about the **management-access** command, see the *Cisco ASA 5500 Series Command Reference*.

Detailed Steps

	Command	Purpose
Step 1	**http** *source_IP_address mask source_interface* **Example:** `hostname(config)# http 192.168.1.2 255.255.255.255 inside`	For each address or subnet, identifies the IP addresses from which the adaptive security appliance accepts HTTPS connections.
Step 2	**http server enable** [*port*] **Example:** `hostname(config)# http server enable 443`	Enables the HTTPS server. By default, the *port* is 443. If you change the port number, be sure to include it in the ASDM access URL. For example, if you change the port number to 444, enter the following: **https://10.1.1.1:444**
Step 3	**asdm image disk**{**0** | **1**}**:/**[*path/*]*filename* **Example:** `hostname(config)# asdm image disk{0 | 1}:/[path/]filename`	Specifies the location of the ASDM image.

Examples

The following example enables the HTTPS server and allows a host on the inside interface with an address of 192.168.1.2 to access ASDM:

```
hostname(config)# crypto key generate rsa modulus 1024
hostname(config)# write mem
hostname(config)# http server enable
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

The following example allows all users on the 192.168.3.0 network to access ASDM on the inside interface:

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

Accessing ASDM from Your PC

From a supported web browser on the adaptive security appliance network, enter the following URL:

https://*interface_ip_address*[**:***port*]

In transparent firewall mode, enter the management IP address.

Configuring CLI Parameters

This section includes the following topics:

- Configuring a Login Banner, page 34-6
- Customizing a CLI Prompt, page 34-7
- Changing the Console Timeout Period, page 34-8

Configuring a Login Banner

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

Restrictions

After a banner is added, Telnet or SSH sessions to adaptive security appliance may close if:

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

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.

Detailed Steps

Command	Purpose
banner {**exec** | **login** | **motd**} *text* **Example:** `hostname(config)# banner motd Welcome to $(hostname).`	Adds a banner to display at one of three times: when a user first connects (message-of-the-day (**motd**)), when a user logs in (**login**), and when a user accesses privileged EXEC mode (**exec**). When a user connects to the adaptive security appliance, the message-of-the-day banner appears first, followed by the login banner and prompts. After the user successfully logs in to the adaptive security appliance, the exec banner displays. To add more than one line, precede each line by the **banner** command. For the banner text: • Spaces are allowed but tabs cannot be entered using the CLI. • There is no length limit for banners other than those for RAM and flash memory. • You can dynamically add the hostname or domain name of the adaptive security appliance by including the strings **$(hostname)** and **$(domain)**. • If you configure a banner in the system configuration, you can use that banner text within a context by using the **$(system)** string in the context configuration.

Examples

For example, to add a message-of-the-day banner, enter:

```
hostname(config)# banner motd Welcome to $(hostname).
hostname(config)# banner motd Contact me at admin@example.com for any
hostname(config)# banner motd issues.
```

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 adaptive 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: • 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.

Detailed Steps

Command	Purpose
prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**]} **Example:** `hostname(config)# firewall transparent`	Customizes the CLI prompt.

Changing the Console Timeout Period

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

Detailed Steps

Command	Purpose
console timeout *number* **Example:** `hostname(config)# console timeout 0`	Specifies the idle time in minutes (0 through 60) after which the console session ends. The default timeout is 0, which means the console session will not time out.

Configuring ICMP Access

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

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

The adaptive security appliance 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.

Note For allowing ICMP traffic *through* the adaptive security appliance, see Chapter 32, "Configuring Access Rules."

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

To configure ICMP access rules, perform the following steps.

Detailed Steps

Command	Purpose
(For IPv4) **icmp** {**permit** | **deny**} {**host** *ip_address* | *ip_address mask* | **any**} [*icmp_type*] *interface_name* **Example:** `hostname(config)# icmp deny host 10.1.1.15 inside`	Creates an IPv4 ICMP access rule. If you do not specify an *icmp_type*, all types are identified. You can enter the number or the name. To control ping, specify echo-reply (0) (adaptive security appliance-to-host) or echo (8) (host-to-adaptive security appliance). See the"ICMP Types" section on page A-15 for a list of ICMP types.
(For IPv6) **ipv6 icmp** {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *interface_name* **Example:** `hostname(config)#`	Creates an IPv6 ICMP access rule. If you do not specify an *icmp_type*, all types are identified. You can enter the number or the name. To control ping, specify echo-reply (0) (adaptive security appliance-to-host) or echo (8) (host-to-adaptive security appliance). See the"ICMP Types" section on page A-15 for a list of ICMP types.

Examples

For example, to allow all hosts except the one at 10.1.1.15 to use ICMP to the inside interface, enter the following commands:

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

To allow the host at 10.1.1.15 to use only ping to the inside interface, enter the following commands:

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

The following example denies all ping requests and permits all Packet Too Big messages (to support Path MTU Discovery) at the outside interface:

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

The following example permits host 2000:0:0:4::2 or hosts on prefix 2001::/64 to ping the outside interface:

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

Configuring Management Access Over a VPN Tunnel

If your VPN tunnel terminates on one interface, but you want to manage the adaptive security appliance by accessing a different interface, you can identify that interface as a management-access interface. For example, if you enter the adaptive security appliance 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 LAN-to-LAN, and the AnyConnect SSL VPN client.

Restrictions

You can define only one management-access interface.

Detailed Steps

Command	Purpose
management access *management_interface* **Example:** `hostname(config)# management access inside`	The *management_interface* specifies the name of the management interface you want to access when entering the adaptive security appliance from another interface.

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 Chapter 33, "AAA Server and Local Database Support."

This section includes the following topics:

- Configuring Authentication for CLI and ASDM Access, page 34-11
- Configuring Authentication To Access Privileged EXEC Mode (the enable Command), page 34-12
- Limiting User CLI and ASDM Access with Management Authorization, page 34-13
- Configuring Command Authorization, page 34-14
- Configuring Management Access Accounting, page 34-25
- Viewing the Current Logged-In User, page 34-26

- Recovering from a Lockout, page 34-27

Configuring Authentication for CLI and ASDM Access

If you enable CLI authentication, the adaptive 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 (see the "Configuring Authentication for the enable Command" section on page 34-12), the adaptive 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 adaptive security appliance can authenticate a Telnet, SSH, or HTTP user, you must first configure access to the adaptive security appliance. See the "Configuring Device Access for ASDM, Telnet, or SSH" section on page 34-1. This configuration identifies the IP addresses that are allowed to communicate with the adaptive security appliance.

Detailed Steps

Command	Purpose
aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]} **Example:** `hostname(config)# aaa authentication telnet console LOCAL`	The **http** keyword authenticates the ASDM client that accesses the adaptive 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. If you use a AAA server group for authentication, you can configure the adaptive security appliance to use the local database as a fallback method if the AAA server is unavailable. Specify the server group name followed by **LOCAL** (**LOCAL** is case sensitive). We recommend that you use the same username and password in the local database as the AAA server because the adaptive security appliance prompt does not give any indication which method is being used. You can alternatively use the local database as your main method of authentication (with no fallback) by entering **LOCAL** alone.

Configuring Authentication To Access Privileged EXEC Mode (the enable Command)

You can configure the adaptive security appliance to authenticate users with a AAA server or the local database when they enter the **enable** command. Alternatively, users are automatically authenticated with the local database when they enter the **login** command, which also accesses privileged EXEC mode depending on the user level in the local database.

This section includes the following topics:

- Configuring Authentication for the enable Command, page 34-12
- Authenticating Users with the login Command, page 34-12

Configuring Authentication for the enable Command

You can configure the adaptive security appliance to authenticate users when they enter the **enable** command. If you do not authenticate the **enable** command, when you enter **enable**, the adaptive security appliance prompts for the system enable password (set by the **enable password** command), and you are no longer logged in as a particular user. Applying authentication to the **enable** command maintains the username. This feature is particularly useful when you perform command authorization, where usernames are important to determine the commands a user can enter.

Detailed Steps

Command	Purpose
aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]} **Example:** `hostname(config)# aaa authentication enable console LOCAL`	Authenticates users who enter the **enable** command. The user is prompted for the username and password. If you use a AAA server group for authentication, you can configure the adaptive security appliance to use the local database as a fallback method if the AAA server is unavailable. Specify the server group name followed by **LOCAL** (**LOCAL** is case sensitive). We recommend that you use the same username and password in the local database as the AAA server because the adaptive security appliance prompt does not give any indication which method is being used. You can alternatively use the local database as your main method of authentication (with no fallback) by entering **LOCAL** alone.

Authenticating Users with the login Command

From user EXEC mode, you can log in as any username in the local database using the **login** command.

This feature allows users to log in with their own username and password to access privileged EXEC mode, so you do not have to give out the system enable password to everyone. To allow users to access privileged EXEC mode (and all commands) when they log in, set the user privilege level to 2 (the default) through 15. If you configure local command authorization, then the user can only enter commands assigned to that privilege level or lower. See the "Configuring Local Command Authorization" section on page 34-16 for more information.

Caution If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged EXEC mode, you should configure command authorization. Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use a AAA server for authentication, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged EXEC mode.

To log in as a user from the local database, enter the following command:

```
hostname> login
```

The adaptive security appliance prompts for your username and password. After you enter your password, the adaptive security appliance places you in the privilege level that the local database specifies.

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 configure **aaa authentication serial console**, then any user who authenticates can access the console port.

Detailed Steps

To configure management authorization, perform the following steps:

Step 1 To enable management authorization, enter the following command:

```
hostname(config)# aaa authorization exec authentication-server
```

This command 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 34-16 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—Use the IETF RADIUS numeric Service-Type attribute which maps to one of the following values. (To map LDAP attributes, see the "LDAP Attribute Mapping for Authorization" section on page 33-18.)
  - Service-Type 6 (Administrative)—Allows full access to any services specified by the **aaa authentication console** commands.
  - Service-Type 7 (NAS prompt)—Allows access to the CLI when you configure the **aaa authentication {telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure **enable** authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.

  - Service-Type 5 (Outbound)—Denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed). Remote access (IPSec and SSL) users can still authenticate and terminate their remote access sessions.

- TACACS+ users—Authorization is requested with "service=shell," and the server responds with PASS or FAIL.
  - PASS, privilege level 1—Allows access to ASDM, with limited read-only access to the configuration and monitoring sections, and access for **show** commands that are privilege level 1 only.
  - PASS, privilege level 2 and higher—Allows access to the CLI when you configure the **aaa authentication {telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure **enable** authentication with the **aaa authentication enable console** command, 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 **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed).
- Local users—Set the **service-type** command. See the "Configuring the Local Database" section on page 33-8. By default, the **service-type** is **admin**, which allows full access to any services specified by the **aaa authentication console** commands.

Configuring Command Authorization

If you want to control the access to commands, the adaptive 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 34-14
- Configuring Local Command Authorization, page 34-16
- Configuring TACACS+ Command Authorization, page 34-21

Command Authorization Overview

This section describes command authorization and includes the following topics:

- Supported Command Authorization Methods, page 34-15
- About Preserving User Credentials, page 34-15
- Security Contexts and Command Authorization, page 34-16

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the adaptive security appliance. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the adaptive 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 adaptive 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 adaptive security appliance places you in level *n*. These levels are not used unless you turn on local command authorization (see "Configuring Local Command Authorization"). (See the *Cisco ASA 5500 Series 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 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 adaptive security appliance, they are required to provide a username and password for authentication. The adaptive 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 adaptive 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 adaptive 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 "LDAP Attribute Mapping for Authorization" section on page 33-18.)

This section includes the following topics:

- Local Command Authorization Prerequisites, page 34-17

- Default Command Privilege Levels, page 34-17
- Assigning Privilege Levels to Commands and Enabling Authorization, page 34-18
- Viewing Command Privilege Levels, page 34-20

Local Command Authorization Prerequisites

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

- Configure **enable** authentication. (See the "Configuring Authentication for CLI and ASDM Access" section on page 34-11.)

  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 33-8.
  - 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 "LDAP Attribute Mapping for Authorization" section on page 33-18.

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.

To view all privilege levels, see the "Viewing Command Privilege Levels" section on page 34-20.

Assigning Privilege Levels to Commands and Enabling Authorization

This section assigns a command to a new privilege level, and enables authorization.

Detailed Steps

	Command	Purpose
Step 1	**privilege** [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command* **Example:** `hostname(config)# privilege show level 5 command filter`	Assigns a command to a privilege level. Repeat this command for each command you want to reassign. See the following information about the options in this command: • **show | clear | cmd**—These optional keywords let you 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. If you do not use one of these keywords, all forms of the command are affected. • **level** *level*—A level between 0 and 15. • **mode** {**enable | configure**}—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: – **enable**—Specifies both user EXEC mode and privileged EXEC mode. – **configure**—Specifies configuration mode, accessed using the **configure terminal** command. • **command** *command*—The command you are configuring. 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.
Step 2	**aaa authorization exec authentication-server** **Example:** `hostname(config)# aaa authorization exec authentication-server`	Supports administrative user privilege levels from RADIUS. Without this command, the adaptive security appliance only supports privilege levels for local database users and defaults all other types of users to level 15. This command 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 34-13 for more information.
Step 3	**aaa authorization command LOCAL** **Example:** `hostname(config)# aaa authorization command LOCAL`	Enables the use of local command privilege levels, which can be checked against the privilege level of users in the local database, RADIUS server, or LDAP server (with mapped attributes). When you set command privilege levels, command authorization does not take place unless you configure command authorization with this command.

Examples

For example, the **filter** command has the following forms:

- **filter** (represented by the **configure** option)
- **show running-config filter**
- **clear configure filter**

You can set the privilege level separately for each form, or set the same privilege level for all forms by omitting this option. For example, set each form separately as follows.

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

Alternatively, you can set all filter commands to the same level:

```
hostname(config)# privilege level 5 command filter
```

The **show privilege** command separates the forms in the display.

The following example shows the use of the **mode** keyword. The **enable** command must be entered from user EXEC mode, while the **enable password** command, which is accessible in configuration mode, requires the highest privilege level.

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(config)# privilege show level 15 mode cmd command enable
```

This example shows an additional command, the **configure** command, that uses the **mode** keyword:

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

Note This last line is for the **configure terminal** command.

Viewing Command Privilege Levels

The following commands let you view privilege levels for commands.

Command	Purpose
show running-config all privilege all	Shows all commands.
show running-config privilege level *level*	Shows commands for a specific level. The *level* is an integer between 0 and 15.
show running-config privilege command *command*	Shows the level of a specific command.

Examples

For example, for the **show running-config all privilege all** command, the system displays the current assignment of each CLI command to a privilege level. The following is sample output from the command.

```
hostname(config)# show running-config all privilege all
privilege show level 15 command aaa
```

```
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
....
```

The following command displays the command assignments for privilege level 10:

```
hostname(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

The following command displays the command assignment for the **access-list** command:

```
hostname(config)# show running-config privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

Configuring TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the adaptive 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 adaptive security appliance. If you still get locked out, see the "Recovering from a Lockout" section on page 34-27.

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 adaptive 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 34-14.

This section includes the following topics:

- TACACS+ Command Authorization Prerequisites, page 34-21
- Configuring Commands on the TACACS+ Server, page 34-22
- Enabling TACACS+ Command Authorization, page 34-24

TACACS+ Command Authorization Prerequisites

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

- Configure CLI authentication (see the "Configuring Local Command Authorization" section on page 34-16).

- Configure **enable** authentication (see the "Configuring Authentication To Access Privileged EXEC Mode (the enable Command)" section on page 34-12).

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 adaptive 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 adaptive security appliance command authorization.

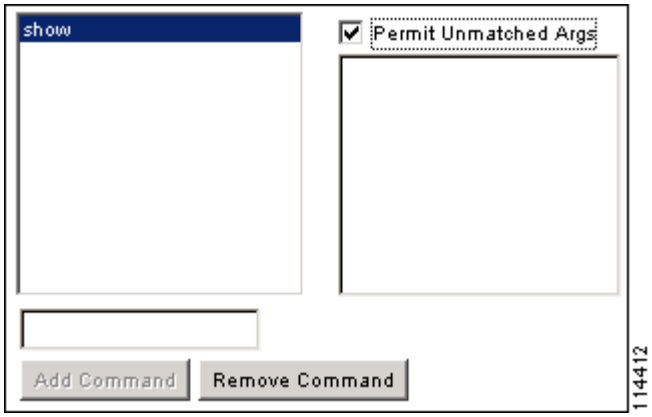
- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by **permit** or **deny**.

  For example, to allow the **show running-configuration aaa-server** command, add **show running-configuration** to the command 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.

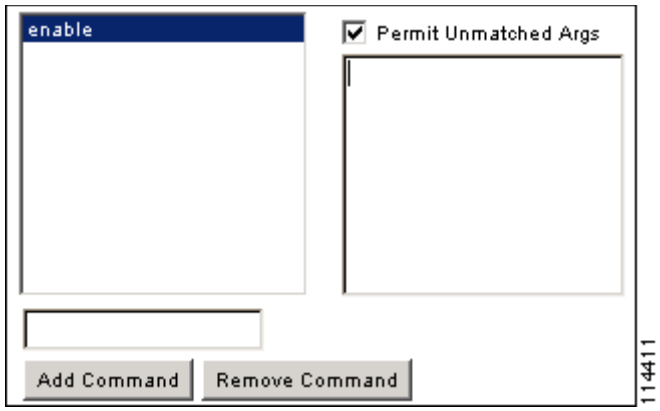
  For example, you can configure just the **show** command, and then all the **show** commands are allowed. We recommend using this method so that you do not have to anticipate every variant of a command, including abbreviations and **?**, which shows CLI usage (see Figure 34-1).

Figure 34-1 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 34-2).

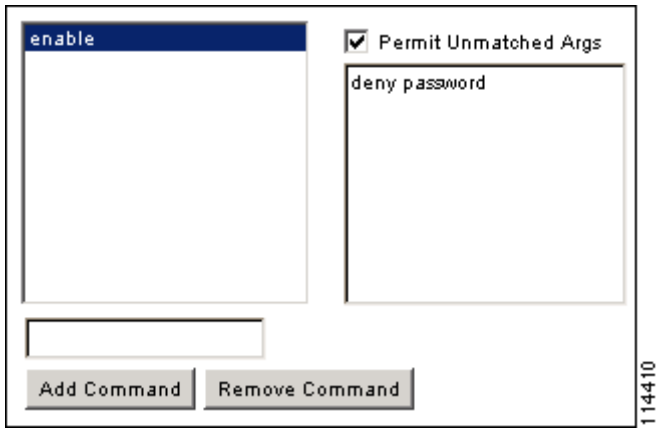
Figure 34-2 Permitting Single Word Commands



- 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 34-3).

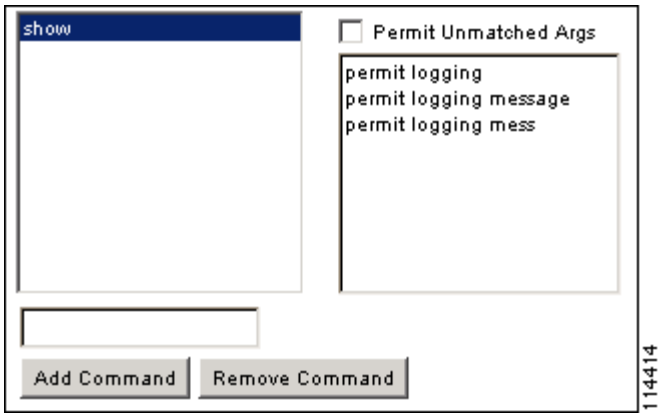
Figure 34-3 Disallowing Arguments



- When you abbreviate a command at the command line, the adaptive 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 adaptive security appliance sends the entire command to the TACACS+ server, **show logging**. However, if you enter **sh log mess**, then the adaptive 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 34-4).

Figure 34-4 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 adaptive security appliance as a user that is defined on the TACACS+ server, and that you have the necessary command authorization to continue configuring the adaptive security appliance. For example, you should log in as an admin user with all commands authorized. Otherwise, you could become unintentionally locked out.

Detailed Steps

Command	Purpose
aaa authorization command *tacacs+_server_group* [**LOCAL**] **Example:** `hostname(config)# aaa authorization command group_1 LOCAL`	Performs command authorization using a TACACS+ server. You can configure the adaptive security appliance to use the local database as a fallback method if the TACACS+ server is unavailable. To enable fallback, specify the server group name followed by **LOCAL** (**LOCAL** is case sensitive). We recommend that you use the same username and password in the local database as the TACACS+ server because the adaptive security appliance prompt does not give any indication which method is being used. Be sure to configure users in the local database (see the "Configuring the Local Database" section on page 33-8) and command privilege levels (see the "Configuring Local Command Authorization" section on page 34-16).

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.

Prerequisites

You can only account for users that first authenticate with the adaptive security appliance, so configure authentication using the "Configuring Authentication for CLI and ASDM Access" section on page 34-11.

For information about configuring a AAA server group, see the "Identifying AAA Server Groups and Servers" section on page 33-11. For CLI access, you can use TACACS+ or RADIUS servers. For command accounting, you can only use TACACS+ servers.

Detailed Steps

Command	Purpose
aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag* **Example:** `hostname(config)# aaa accounting telnet console group_1`	Enables support for AAA accounting for administrative access. Valid server group protocols are RADIUS and TACACS+.
aaa accounting command [**privilege** *level*] *server-tag* **Example:** `hostname(config)# aaa accounting command privilege 15 group_1`	Enables command accounting. Only TACACS+ servers support command accounting. Where *level* is the minimum privilege level and *server-tag* is the name of the TACACS+ server group that to which the adaptive security appliance should send command accounting messages.

Viewing the Current Logged-In User

To view the current logged-in user, enter the following command:

```
hostname# show curpriv
```

See the following sample **show curpriv** command output. A description of each field follows.

```
hostname# show curpriv
Username : admin
Current privilege level : 15
Current Mode/s : P_PRIV
```

Table 34-1 describes the **show curpriv** command output.

Table 34-1 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	Level 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 Mode/s	Shows the access modes: • P_UNPR—User EXEC mode (levels 0 and 1) • P_PRIV—Privileged EXEC mode (levels 2 to 15) • P_CONF—Configuration mode

Recovering from a Lockout

In some circumstances, when you turn on command authorization or CLI authentication, you can be locked out of the adaptive security appliance CLI. You can usually recover access by restarting the adaptive security appliance. However, if you already saved your configuration, you might be locked out. Table 34-2 lists the common lockout conditions and how you might recover from them.

Table 34-2 CLI Authentication and Command Authorization Lockout Scenarios

Feature	Lockout Condition	Description	Workaround: Single Mode	Workaround: Multiple Mode
Local CLI authentication	No users in the local database	If you have no users in the local database, you cannot log in, and you cannot add any users.	Log in and reset the passwords and **aaa** commands.	Session into the adaptive 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.	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 adaptive security appliance, session into the adaptive 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 34-2 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 adaptive security appliance immediately, then log into the maintenance partition and reset the passwords and **aaa** commands.	Session into the adaptive 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 adaptive security appliance from the switch. From the system execution space, you can change to the context and change the user level.