

# Management Access

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


- Configure Management Remote Access, on page 1
- Configure AAA for System Administrators, on page 15
- Monitoring Device Access, on page 32
- History for Management Access, on page 33


# Configure Management Remote Access

This section describes how to configure ASA access for ASDM, Telnet, or SSH, and other management parameters such as a login banner.

## Configure ASA Access for HTTPS, Telnet, or SSH

This section describes how to configure ASA access for HTTPS, including ASDM and CSM, Telnet, or SSH. See the following guidelines:

- 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. If, however, you configure HTTP redirect to redirect HTTP connections to HTTPS automatically, you must enable an access rule to allow HTTP; otherwise, the interface cannot listen to the HTTP port.
- 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 Configure Management Access Over a VPN Tunnel, on page 9.
- 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.

- In single context mode, a maximum 30 ASDM concurrent sessions. In multiple context mode, you can have a maximum of 5 concurrent ASDM sessions per context, with a maximum of 32 ASDM instances among all contexts.

  ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the multiple-context mode system limit of 32 ASDM sessions represents a limit of 64 HTTPS sessions.

- A maximum of 6 concurrent non-ASDM HTTPS sessions in single context mode or per context, if available, with a maximum or 100 HTTPS sessions among all contexts.

## Configure HTTPS Access for ASDM, Other Clients

This section describes how to configure ASA access for HTTPS, including ASDM and CSM.

### Before you begin

- 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.

### Procedure

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

The **Add Device Access Configuration** dialog box appears.

**Step 2** Choose **ASDM/HTTPS**.

**Step 3** Choose the management interface and set the host IP addresses allowed, and click **OK**.

Specify any named interface. For bridge groups, specify the bridge group member interface. For VPN management access only (see Configure Management Access Over a VPN Tunnel, on page 9), specify the named BVI interface.

**Step 4** To require certificate authentication, in the **Specify the interface requires client certificate to access ASDM** area, click **Add** to specify the interface and an optional certificate map that must be matched for successful authentication. See **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Advanced** > **IPSec** > **Certificate to Connection Map** > **Rules** to create the certificate map. For more information, see Configure ASDM Certificate Authentication, on page 18.

**Step 5** Configure **HTTP Settings**.

- **Enable HTTP Server**—Enable the HTTPS server.
- **Port Number**—Set the port number. The default is 443.
- **Idle Timeout**—Set the idle timeout for ASDM connections, from 1-1440 minutes. The default is 20 minutes. The ASA disconnects an ASDM connection that is idle for the set period of time.
- **Session Timeout**—Set the session timeout for ASDM sessions, from 1-1440 minutes. This timeout is disabled by default. The ASA disconnects an ASDM session that exceeds the set period of time.

**Step 6** Click **Apply**.

**Step 7** (Optional) Allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed.

Many specialty clients (for example, python libraries, curl, and wget) do not support Cross-site request forgery (CSRF) token-based authentication, so you need to specifically allow these clients to use the ASA basic authentication method. For security purposes, you should only allow required clients.

a) Choose **Configuration** > **Device Management** > **Management Access** > **HTTP Non-Browser Client Support**, and click **Add**.

b) In the **User-Agent String from the HTTP Header** field, specify the client's User-Agent string in the HTTP header of the HTTP request.

You can specify the complete string or a partial string; partial strings must match the start of the User-Agent string. We recommend complete strings for better security. Note that the string is case-sensitive.

For example, **curl** will match the following User-Agent string:

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

**curl** will *not* match the following User-Agent string:

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

**CURL** will *not* match the following User-Agent string:

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

## Configure SSH Access

This section describes how to configure ASA access for SSH. See the following guidelines:

- Only SSH Version 2 is 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 by choosing **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authentication**; then define a local user by choosing **Configuration** > **Device Management** > **Users/AAA**. 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.

### Before you begin

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.

### Procedure

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

The **Add Device Access Configuration** dialog box appears.

**Step 2** Choose **SSH**.

**Step 3** Choose the management interface and set the host IP addresses allowed, and click **OK**.

Specify any named interface. For bridge groups, specify the bridge group member interface. For VPN management access only (see Configure Management Access Over a VPN Tunnel, on page 9), specify the named BVI interface.

**Step 4** (Optional) Configure **SSH Settings**.

- **Allowed SSH Versions**—Only version 2 is supported.
- **SSH Timeout**—Set 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 pre-production testing and troubleshooting have been completed.
- **DH Key Exchange** (Admin context only)—Click the applicable radio button to choose the Diffie-Hellman (DH) Key Exchange Group. If no DH group key-exchange method is specified, the DH group 14 SHA256 key-exchange method is used. For more information about using DH key-exchange methods, see RFC 4253. You can only set the key exchange in the Admin context; this value is used by all contexts.

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

**Step 6** Configure SSH user authentication.

a) (For password access) Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authentication**.

AAA authentication does not affect local public key authentication for usernames with the **Public Key Using PKF** option. The ASA implicitly uses the local database for public key authentication. SSH authentication only affects usernames with passwords. If you want to allow either public key authentication or password use by a local user, then you need to explicitly configure local authentication with this procedure to allow password access.

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

c) Choose the **LOCAL** database (or AAA server) from the **Server Group** drop-down list.

d) Click **Apply**.

e) Add a local user. You can alternatively use a AAA server for user access, but a local username is recommended. Choose **Configuration** > **Device Management** > **Users/AAA** > **User Accounts**, then click **Add**.

The **Add User Account-Identity** dialog box appears.

f) Enter a username and password, then confirm the password. You might want to create a user without a password if you want to force the user to use public key authentication instead of password authentication. If you configure public key authentication as well as a password, then the user can log in with either method if you explicitly configure AAA authentication in this procedure.

g) (Optional) To enable public key authentication on a per-user basis instead of/as well as password authentication, choose one of the following panes:

- **Public Key Authentication**—Paste in a Base64-encoded public key. You can generate the key using any SSH key generation software (such as ssh keygen) that can generate ssh-rsa raw keys (with no certificates).When you view an existing key, the key is encrypted using a SHA-256 hash. If you need to copy and paste a hashed key, check the **Key is hashed** check box.
- To remove an authentication key, click **Delete Key** to display a confirmation dialog box. Click **Yes** to remove the authentication key, or click **No** to retain it.
- **Public Key Using PKF**—Check the **Specify a new PKF** key check box, and paste or import a public key file (PKF) formatted key, up to 4096 bits. Use this format for keys that are too large to paste in Base64 format. For example, you can generate a 4096-bit key using ssh keygen, then convert it to PKF, and import on this pane. When you view an existing key, the key is encrypted using a SHA-256 hash. If you need to copy and paste a hashed key, copy it from the **Public Key Authentication** pane, and paste it in that pane on the new ASA with the **Key is hashed** check box checked.

  To remove an authentication key, click **Delete Key** to display a confirmation dialog box. Click **Yes** to remove the authentication key, or click **No** to retain it.

h) Click **OK**, then click **Apply**.

**Step 7** Generate a key pair (for physical ASAs only).

For the ASAv, the key pairs are automatically created after deployment. The ASAv only supports the RSA key.

a) Choose **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificates**.
b) Click **Add** and click the **Add a new identity certificate** radio button.
c) Click **New**.
d) In the **Add Key Pair** dialog box, specify the type and size, and click **Generate Now**.

The default key pair used is RSA.

You can then **Cancel** out of the certificate dialog box, because you only wanted to generate the key pair.

**Step 8** (Optional) Configure SSH cipher encryption and integrity algorithms:

a) Choose **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**.
b) Select **Encryption**, and click **Edit**.
c) From the SSH cipher security level drop-down list, choose one of the following levels.

Ciphers are used in the order they are listed. For pre-defined lists, they are listed from lowest to highest security.

- **All**—Specifies using all ciphers: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **Custom**—Specifies a custom cipher encryption configuration string that you enter in the **Cipher algorithms/custom string** field, separated by colons.
- **Fips**—Specifies only FIPS-compliant ciphers: aes128-cbc aes256-cbc
- **High**—Specifies only high-strength ciphers: aes256-cbc aes256-ctr
- **Low**—Specifies low, medium, and high strength ciphers: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **Medium**—Specifies the medium and high strength ciphers (the default): 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

d) Select **Integrity**, and click **Edit**.
e) From the SSH cipher security level drop-down list, choose one of the following levels:

- **All**—Specifies using all ciphers: hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- **Custom**—Specifies a custom cipher encryption configuration string that you enter in the **Cipher algorithms/custom string** field, separated by colons.
- **Fips**—Specifies only FIPS-compliant ciphers: hmac-sha1 hmac-sha2-256
- **High**—Specifies only high-strength ciphers (the default): hmac-sha2-256
- **Low**—Specifies low, medium, and high strength ciphers: hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96
- **Medium**—Specifies the medium and high strength ciphers: hmac-sha1 hmac-sha1-96

## Examples

The following example generates a shared key for SSH on a Linux or Macintosh system, and imports it to the ASA:

1. Generate the RSA public and private keys for 4096 bits on your computer:

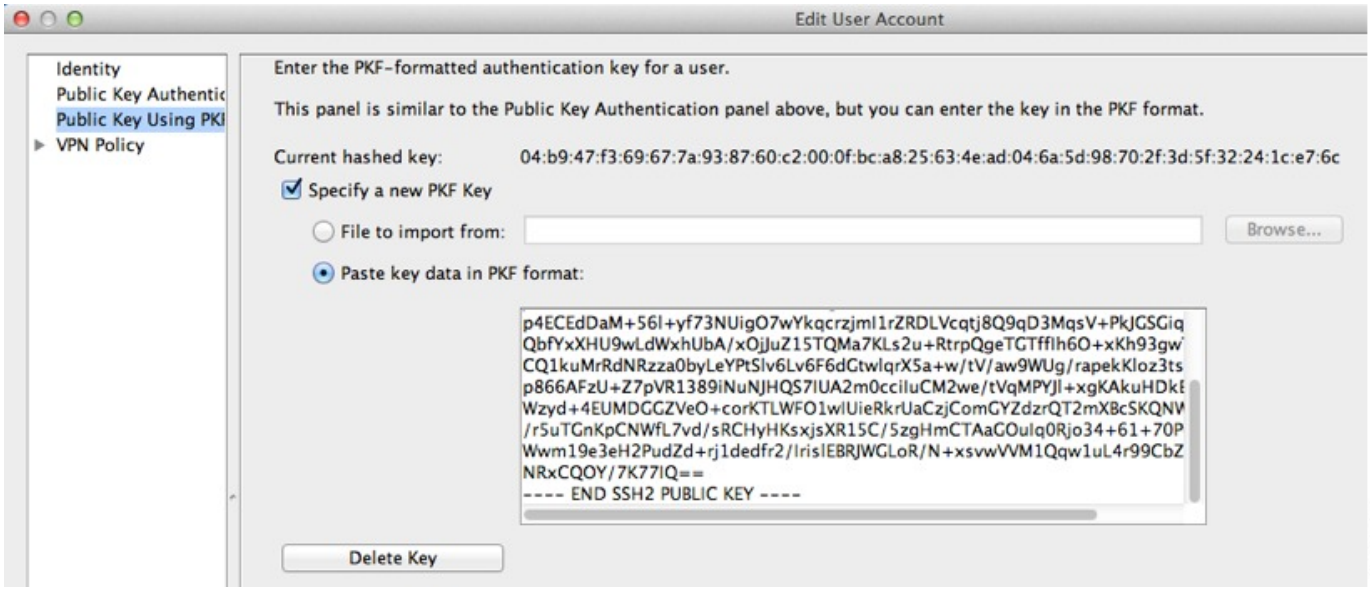
```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. Convert the key to PKF format:

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
```

```
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. Copy the key to your clipboard.
4. In ASDM, choose **Configuration** > **Device Management** > **Users/AAA** > **User Accounts**, select the username and then click **Edit**. Click **Public Key Using PKF** and paste the key into the window:




5. Verify the user can SSH to the ASA. For the password, enter the SSH key password you specified when you created the key pair.

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

The following dialog box appears for you to enter your passphrase:




Meanwhile, in the terminal session:

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

## Configure Telnet Access

This section describes how to configure ASA access for Telnet. You cannot use Telnet to the lowest security interface unless you use Telnet inside a VPN tunnel.

### Before you begin

- 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.
- To gain access to the ASA CLI using Telnet, enter the login password. You must manually set the password before using Telnet.

### Procedure

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

The **Add Device Access Configuration** dialog box appears.

**Step 2** Choose **Telnet**.

**Step 3** Choose the management interface and set the host IP addresses allowed, and click **OK**.

Specify any named interface. For bridge groups, specify the bridge group member interface. For VPN management access only (see Configure Management Access Over a VPN Tunnel, on page 9), specify the named BVI interface.

**Step 4** (Optional) Set the **Telnet Timeout**. The default timeout value is 5 minutes.

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

**Step 6** Set a login password before you can connect with Telnet; there is no default password.

a) Choose **Configuration** > **Device Setup** > **Device Name/Password**.
b) Check the **Change the password to access the console of the security appliance** check box in the **Telnet Password** area.
c) Enter the old password (leave this field blank for a new ASA), new password, then confirm the new password.
d) Click **Apply**.

# Configure HTTP Redirect for ASDM Access or Clientless SSL VPN

You must use HTTPS to connect to the ASA using ASDM or clientless SSL VPN. For your convenience, you can redirect HTTP management connections to HTTPS. For example, by redirecting HTTP, you can enter either **http://10.1.8.4/admin/** or **https://10.1.8.4/admin/** and still arrive at the ASDM launch page at the HTTPS address.

You can redirect both IPv4 and IPv6 traffic.

### Before you begin

Normally, you do not need an access rule allowing the host IP address. However, for HTTP redirect, you must enable an access rule to allow HTTP; otherwise, the interface cannot listen to the HTTP port.

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **HTTP Redirect**.

The table shows the currently configured interfaces and whether redirection is enabled on an interface.

**Step 2** Select the interface that you use for ASDM, and click **Edit**.

**Step 3** Configure the following options in the **Edit HTTP/HTTPS Settings** dialog box:

- **Redirect HTTP to HTTPS**—Redirects HTTP requests to HTTPS.
- **HTTP Port**—Identifies the port from which the interface redirects HTTP connections. The default is 80.

**Step 4** Click **OK**.

# Configure 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 must 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.

**Note** For secure SNMP polling over a site-to-site VPN, include the IP address of the outside interface in the crypto map access-list as part of the VPN configuration.

VPN access to an interface other than the one from which you entered the ASA is not supported. For example, if your VPN access is located on the outside interface, you can only initiate a connection directly to the outside interface. You should enable VPN on the directly-accessible interface of the ASA and use name resolution so that you don't have to remember multiple addresses.

Management access is available via the following VPN tunnel types: IPsec clients, IPsec Site-to-Site, Easy VPN, and the AnyConnect SSL VPN client.

### Before you begin

Due to routing considerations with the separate management and data routing tables, the VPN termination interface and the management access interface need to be the same type: both need to be management-only interfaces or regular data interfaces.

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Management Access** > **Management Interface**.

**Step 2** Choose the interface with the highest security (the inside interface) from the **Management Access Interface** drop-down list.

For Easy VPN and Site-to-Site tunnels, you can specify a named BVI (in routed mode).

**Step 3** Click **Apply**.

The management interface is assigned, and the change is saved to the running configuration.

# Configure Management Access for FXOS on Firepower 2100 Data Interfaces

If you want to manage FXOS on the Firepower 2100 from a data interface, you can configure SSH, HTTPS, and SNMP access. This feature is useful if you want to manage the device remotely, but you want to keep Management 1/1, which is the native way to access FXOS, on an isolated network. If you enable this feature, you can continue to use Management 1/1 for local access only. However, you cannot allow *remote* access to or from Management 1/1 for FXOS at the same time as using this feature. This feature requires forwarding traffic to the ASA data interfaces using an internal path (the default), and you can only specify one FXOS management gateway.

The ASA uses non-standard ports for FXOS access; the standard port is reserved for use by the ASA on the same interface. When the ASA forwards traffic to FXOS, it translates the non-standard destination port to the FXOS port for each protocol (do not change the HTTPS port in FXOS). The packet destination IP address (which is the ASA interface IP address) is also translated to an internal address for use by FXOS. The source address remains unchanged. For returning traffic, the ASA uses its data routing table to determine the correct egress interface. When you access the ASA data IP address for the management application, you must log in using an FXOS username; ASA usernames only apply for ASA management access.

You can also enable FXOS management traffic *initiation* on ASA data interfaces, which is required for SNMP traps, or NTP and DNS server access, for example. By default, FXOS management traffic initiation is enabled for the ASA outside interface for DNS and NTP server communication (required for Smart Software Licensing communication).

### Before you begin

- Single context mode only.
- Excludes ASA management-only interfaces.
- You cannot use a VPN tunnel to an ASA data interface and access FXOS directly. As a workaround for SSH, you can VPN to the ASA, access the *ASA* CLI, and then use the **connect fxos** command to access the FXOS CLI. Note that SSH, HTTPS, and SNMPv3 are/can be encrypted, so direct connection to the data interface is safe.
- Ensure that the FXOS gateway is set to forward traffic to the ASA data interfaces (the default). See the getting started guide for more information about setting the gateway.

### Procedure

**Step 1** In ASDM, choose **Configuration** > **Firewall** > **Advanced** > **FXOS Remote Management**.

**Step 2** Enable FXOS remote management.

a) Choose **HTTPS**, **SNMP**, or **SSH** from the navigation pane.

b) Click **Add**, and set the **Interface** where you want to allow management, set the **IP Address** allowed to connect, and then click **OK**.

You can create multiple entries for each protocol type. Set the **Port** if you do not want to use the following defaults:

- HTTPS default port—3443
- SNMP default port—3061
- SSH default port—3022

**Step 3** Allow FXOS to initiate management connections from an ASA interface.

a) Choose **FXOS Traffic Initiation** from the navigation pane.

b) Click **Add**, and enable the ASA interfaces where you need to send FXOS management traffic. By default, the outside interface is enabled.

**Step 4** Click **Apply**.

**Step 5** Connect to the Firepower Chassis Manager on Management 1/1 (by default https://192.168.45.45, with the username: **admin** and password: **Admin123**).

**Step 6** Click the **Platform Settings** tab, and enable **SSH**, **HTTPS**, or **SNMP**.

SSH and HTTPS are enabled by default.

**Step 7** Configure an **Access List** on the **Platform Settings** tab to allow your management addresses. SSH and HTTPS only allow the Management 1/1 192.168.45.0 network by default. You need to allow any addresses that you specified in the **FXOS Remote Management** configuration on the ASA.

# Change 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.

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Management Access** > **Command Line (CLI)** > **Console Timeout**.

**Step 2** Define a new timeout value in minutes, To specify an unlimited amount of time, enter **0**. The default value is 0.

**Step 3** Click **Apply**.

The timeout value change is saved to the running configuration.

# Customize a CLI Prompt

The ability to add information to a prompt allows you to see at-a-glance which ASA you are logged into when you have multiple modules. During a failover, this feature is useful when both ASAs have the same hostname.

In multiple context mode, you can view the extended prompt when you log in to the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name.

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** | 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 or role of the unit.<br>For failover, the following values are displayed for the state keyword:<br>• **act**—Failover is enabled, and the unit is actively passing traffic.<br>• **stby**— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state.<br>• **actNoFailover**—Failover is not enabled, and the unit is actively passing traffic.<br>• **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.<br>For clustering, the values for control and data are shown. |

**Procedure**

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

**Step 2** Do any of the following to customize the prompt:

- Click the attribute in the **Available Prompts** list, 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.
- Click the attribute in the **Selected Prompts** list, then click **Delete**. The attribute is moved from the **Selected Prompts** list to the **Available Prompts** list.
- Click the attribute in the **Selected Prompts** list and click **Move Up** or **Move Down** to change the order in which the attributes appear.

The prompt is changed and appears in the **CLI Prompt Preview** field.

**Step 3** Click **Apply**.

The new prompt is saved to the running configuration.

# Configure 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.

### Before you begin

- 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.
```

- After a banner has been added, Telnet or SSH sessions to the 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).
- See RFC 2196 for guidelines about banner messages.

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Management Access** > **Command Line (CLI)** > **Banner**.

**Step 2** 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 3** Click **Apply**.

The new banner is saved to the running configuration.

## Set a Management Session Quota

You can establish a maximum number of simultaneous ASDM, SSH, and Telnet sessions that are allowed on the ASA. 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.

**Note** In multiple context mode, you cannot configure the number of ASDM sessions, where the maximum is fixed at 5 sessions.

**Note** If you also set a resource limit per context for the maximum administrative sessions (SSH, etc.), then the lower value will be used.

#### Before you begin

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.

#### Procedure

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

**Step 2** Enter the maximum number of simultaneous sessions.

- **Aggregate**—Sets the aggregate number of sessions between 1 and 15. The default is 15.
- **HTTP Sessions**—Sets the maximum HTTPS (ASDM) sessions, between 1 and 5. The default is 5.
- **SSH Sessions**—Sets the maximum SSH sessions, between 1 and 5. The default is 5.
- **Telnet Sessions**—Sets the maximum Telnet sessions, between 1 and 5. The default is 5.
- **User Sessions**—Sets the maximum sessions per user, between 1 and 5. The default is 5.

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

# Configure AAA for System Administrators

This section describes how to configure authentication, management authorization, and command authorization for system administrators.

## Configure Management Authentication

Configure authentication for CLI and ASDM access.

# About Management Authentication

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

## About SSH Authentication

See the following behavior for SSH access with and without authentication:

- No Authentication—SSH is not available without authentication.
- Authentication—When you enable SSH authentication, you enter the username and password as defined on the AAA server or local user database. For public key authentication, the ASA only supports the local database. If you configure SSH public key authentication, then the ASA uses the local database implicitly. You only need to explicitly configure SSH authentication when you use a username and password to log in. You access user EXEC mode.

## About Telnet Authentication

See the following behavior for Telnet access with and without authentication:

- No Authentication—If you do not enable any authentication for Telnet, you do not enter a username; you enter the login password. There is no default password, so you must set one before you can Telnet to the ASA. You access user EXEC mode.
- Authentication—If you enable Telnet authentication, you enter the username and password as defined on the AAA server or local user database. You access user EXEC mode.

## About ASDM Authentication

See the following behavior for ASDM access with and without authentication. You can also configure certificate authentication, with or without AAA authentication.

- No Authentication—By default, you can log into ASDM with a blank username and the enable password, which is blank by default. We suggest that you change the enable password as soon as possible so that it does not remain blank; see Set the Hostname, Domain Name, and the Enable and Telnet Passwords. When you enter the **enable** command at the CLI for the first time, you are prompted to change the password; this behavior is not enforced when you log into ASDM. 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.
- Certificate Authentication—(Single, routed mode only) You can require that the user have a valid certificate. Enter the certificate username and password, and the ASA validates the certificate against the PKI trustpoint.
- AAA Authentication—When you enable ASDM (HTTPS) authentication, you enter the username and password as defined on the AAA server or local user database. You can no longer use ASDM with a blank username and the enable password.
- AAA Authentication plus Certificate Authentication—(Single, routed mode only) When you enable ASDM (HTTPS) authentication, you enter the username and password as defined on the AAA server or local user database. If the username and password are different for the certificate authentication, you are prompted to enter them as well. You can opt to pre-fill the username derived from your certificate.

### About Serial Authentication

See the following behavior for access to the serial console port with and without authentication:

- No Authentication—If you do not enable any authentication for serial access, you do not enter a username or password. You access user EXEC mode.
- Authentication—If you enable authentication for serial access, you enter the username and password as defined on the AAA server or local user database. You access user EXEC mode.

### About Enable Authentication

To enter privileged EXEC mode after logging in, enter the **enable** command. How this command works depends on whether or not you enable authentication:

- No Authentication—If you do not configure enable authentication, enter the system enable password when you enter the **enable** command, which is blank by default. The first time you enter the **enable** command, you are prompted to change it. However, if you do not use enable authentication, after you enter the **enable** command, you are no longer logged in as a particular user, which can affect user-based features such as command authorization. To maintain your username, use enable authentication.
- Authentication—If you configure enable authentication, the ASA prompts you for your username and password as defined on the AAA server or local user database. 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. The **login** command maintains the username, but requires no configuration to turn on authentication.



**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 discourage the login command by using a AAA server for authentication instead of the local database, 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.

### Sessions from the Host Operating System to the ASA

Some platforms support running the ASA as a separate application: for example, the ASASM on the Catalyst 6500, or the ASA on the Firepower 4100/9300. For sessions from the host operating system to the ASA, you can configure serial and Telnet authentication, depending on the type of connection. For example, the **connect asa** command in FXOS on the Firepower 2100 uses a serial connection.

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 these sessions. The admin context AAA server or local user database is used in this instance.

## Configure Authentication for CLI, ASDM, and enable command Access

#### Before you begin

- Configure Telnet, SSH, or HTTP access.

- For external authentication, configure a AAA server group. For local authentication, add users to the local database.
- HTTP management authentication does not support the SDI protocol for a AAA server group.
- This feature does not affect SSH public key authentication for local usernames with the **ssh authentication** command. The ASA implicitly uses the local database for public key authentication. This feature only affects usernames with passwords. If you want to allow either public key authentication or password use by a local user, then you need to explicitly configure local authentication with this procedure to allow password access.

**Procedure**

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

a) Check the **Enable** check box.
b) 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. 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 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**, then 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.
   - **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 the Firepower 2100, this keyword affects the virtual console accessed from FXOS using the **connect asa** command.
   - **SSH**—Authenticates users who access the ASA using SSH (password only; public key authentication implicitly uses the local database).
   - **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.
b) For each service that you checked, 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. 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 of which method is being used.

**Step 3** Click **Apply**.

## Configure ASDM Certificate Authentication

You can require certificate authentication, with or without AAA authentication. The ASA validates the certificate against the PKI trustpoint.

### Before you begin

This feature is supported in single, routed mode only.

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**.

**Step 2** In the **Specify the interface requires client certificate to access ASDM** area, click **Add** to specify the interface and an optional certificate map that must be matched for successful authentication.

You configure certificate authentication for each interface, so that connections on a trusted/inside interface do not have to provide a certificate. See **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPSec** > **Certificate to Connection Map** > **Rules** to create the certificate map.

**Step 3** (Optional) To set the attribute used by ASDM to derive the username from the certificate, choose **Configuration** > **Device Management** > **Management Access** > **HTTP Certificate Rule**.

Choose one of the following methods:

- **Specify the Certificate Fields to be used**—Select a value from the **Primary Field** and the **Secondary Field** drop-down lists.
- **Use the entire DN as the username**
- **Use script to select username**—Click **Add** to add the script content.

Check the **Prefill Username** check box to pre-fill the username when prompted for authentication. If the username is different from the one you initially typed in, a new dialog box appears with the username pre-filled. You can then enter the password for authentication.

By default, ASDM uses CN OU attributes.

**Step 4** Click **Apply**.

# Control CLI and ASDM Access with Management Authorization

The ASA lets you distinguish between administrative and remote-access users when they authenticate. User role differentiation can prevent remote access VPN and network access users from establishing an administrative connection to the ASA.

### Before you begin

**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.

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

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.

**TACACS+ users**

Authorization is requested with "service=shell," and the server responds with PASS or FAIL.

**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.

**Management Authorization Attributes**

See the following table for AAA server types and valid values for management authorization. The ASA uses these values to determine the level of management access.

| Management Level | RADIUS/LDAP (Mapped) Attributes | TACACS+ Attributes | Local Database Attributes |
|---|---|---|---|
| Full Access—Allows full access to any services specified by the **Authentication** tab options | Service-Type 6 (Administrative), Privilege-Level 1 | PASS, privilege level 1 | admin |
| Partial Access—Allows access to the CLI or ASDM when you configure the **Authentication** tab options. However, if you configure **enable** authentication with the **Enable** option, then the CLI user cannot access privileged EXEC mode using the **enable** command. | Service-Type 7 (NAS prompt), Privilege-Level 2 and higher<br>The Framed (2) and Login (1) service types are treated the same way. | PASS, privilege level 2 and higher | nas-prompt |
| No Access—Denies management access. The user cannot use any services specified by the **Authentication** tab options (excluding the **Serial** option; serial access is allowed). Remote access (IPsec and SSL) users can still authenticate and terminate their remote access sessions. All other service types (Voice, FAX, and so on) are treated the same way. | Service-Type 5 (Outbound) | FAIL | remote-access |

**Additional Guidelines**

- Serial console access is not included in management authorization.
- You must also configure AAA authentication for management access to use this feature. See Configure Authentication for CLI, ASDM, and enable command Access, on page 17.
- If you use external authentication, you must pre-configure a AAA server group before you enable this feature.
- HTTP authorization is supported in single, routed mode only.

**Procedure**

**Step 1** To enable management authorization for HTTP sessions, choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authorization**, and check the **HTTP** check box in the **Enable Authorization for ASA Command Access** Area.

**Note** To configure ASA Command Access, see Configure Local Command Authorization, on page 23.

**Step 2** To enable management authorization for Telnet and SSH sessions, choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authorization**, and check the **Enable** check box in the **Perform authorization for exec shell access** Area.

**Step 3** Select either the **Remote** or **Local** radio buttons to specify the server to be used for authorization of exec shell access.

**Step 4** To enable management authorization, check the **Allow privileged users to enter into EXEC mode on login** check box.

The **auto-enable** option allows users Full Access to be placed directly in privileged EXEC mode. Otherwise, users are placed in user EXEC mode.

# Configure 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

## About Command Authorization

You can enable command authorization so only authorized users can enter commands.

### 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.

- 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.

### Security Contexts and Command Authorization

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.

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

### 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 cannot enter configuration mode.

## Configure 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).

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authorization**.

**Step 2** Check the **Enable authorization for ASA command access** > **Enable** check box.

**Step 3** Choose **LOCAL** from the **Server Group** drop-down list.

**Step 4** 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.

- Click **Set ASDM Defined User Roles** to use predefined user account privileges.

  The **ASDM Defined User Roles Setup** dialog box appears. 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).

- Click **Configure Command Privileges** to manually configure command levels.

  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**, then **Edit**.

  Click **OK** to accept your changes.

**Step 5** (Optional) Check the **Perform authorization for exec shell access** > **Enable** check box to enable AAA users for command authorization. Without this option, the ASA only supports privilege levels for local database users and defaults all other types of users to level 15.

This command also enables management authorization. See Control CLI and ASDM Access with Management Authorization, on page 19.

**Step 6** Click **Apply**.

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

## Configure 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.

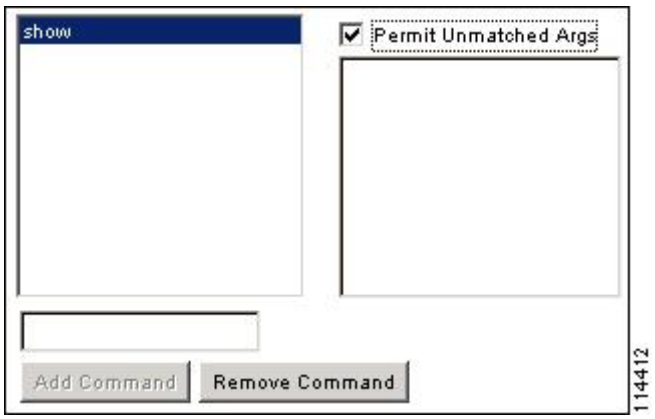
- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by **permit** or **deny**.

  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.

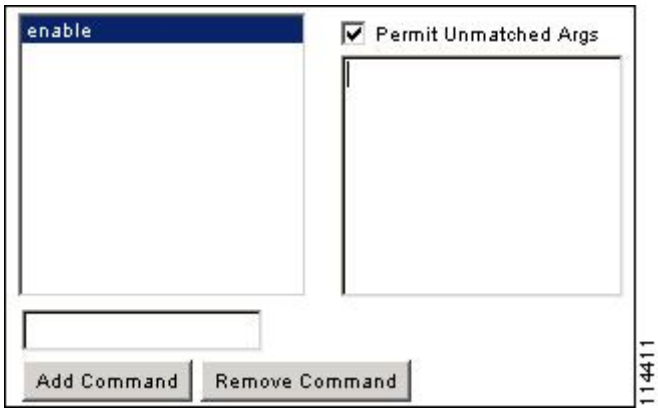
  For example, you can configure just the **show** command, then all the **show** commands are allowed. We recommend using this method so that you do not have to anticipate every variant of a command, including abbreviations and a question mark, which shows CLI usage (see the following figure).

*Figure 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 the following figure).

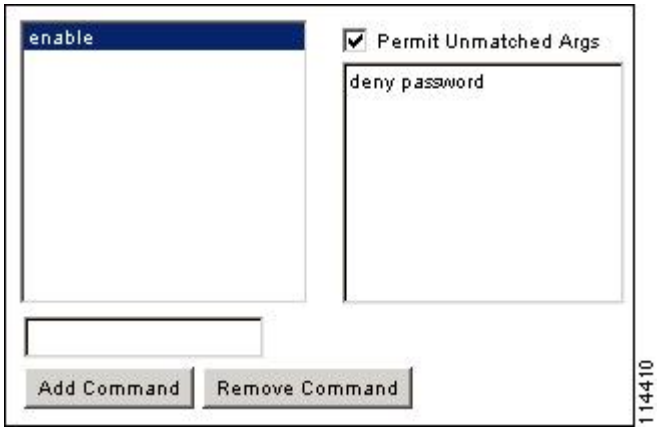
*Figure 2: Permitting Single Word Commands*




- 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 the following figure).

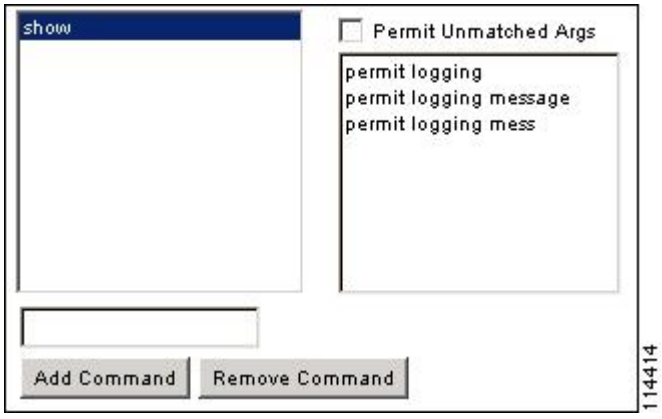
*Figure 3: Disallowing Arguments*




- 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 the following figure).

*Figure 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**

## Configure 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.

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.

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

**Procedure**

**Step 1** Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authorization**.

**Step 2** Check the **Enable authorization for command access** > **Enable** check box.

**Step 3** Choose a AAA server group name from the **Server Group** drop-down list.

**Step 4** (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 and command privilege levels.

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

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

# Configure 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.

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.

### Before you begin

- Configure AAA authentication for CLI or ASDM access using the local database.
- Specify usernames in the local database.

### Procedure

**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.

- **Enable Reuse Interval**—You can prohibit the reuse of a password that matches previously used passwords, between 2 and 7 previous passwords. The previous passwords are stored in the configuration under each username in encrypted form using the **password-history** command; this command is not user-configurable.
- **Prevent Passwords from Matching Usernames**—Prohibit a password that matches a username.

**Step 3** (Optional) Check the **Enable Password and Account Protection** 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 and 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** Click **Apply** to save the configuration settings.

## Change 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.

To change your username password, perform the following steps:

### Procedure

**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.

# Enable and View the Login History

By default, the login history is saved for 90 days. You can disable this feature or change the duration, up to 365 days.

### Before you begin

- The login history is only saved per unit; in failover and clustering environments, each unit maintains its own login history only.

- Login history data is not maintained over reloads.
- This feature applies to usernames in the local database or from a AAA server when you enable local AAA authentication for one or more of the CLI management methods (SSH, Telnet, serial console). ASDM logins are not saved in the history.

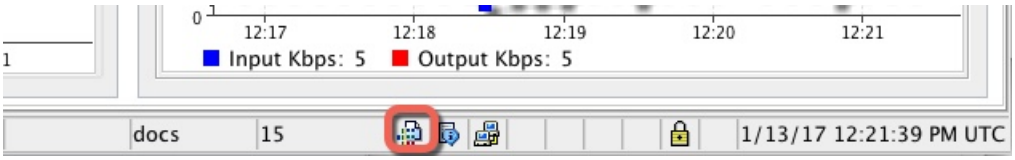
**Procedure**

**Step 1** Choose **Configuration** > **Device Management** > **Users/AAA** > **Login History**.

**Step 2** Check the **Configure login history reporting for administrators** check box. This feature is enabled by default.

**Step 3** Set the **Duration** between 1 and 365 days. The default is 90.

**Step 4** To view the login history, from any ASDM screen you can click on the **Login History** icon in the bottom **Status** bar:




The login history for all users displays in a dialog box.

# Configure 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:

**Procedure**

**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** , then check the **Require accounting to allow accounting of user activity** > **Enable** check box.

b) 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) Check the **Serial**, **SSH**, and/or **Telnet** check boxes in the **Require accounting for the following types of connections** area.

b) Choose a RADIUS or TACACS+ server group name for each connection type.

**Step 3** To configure command accounting, perform the following steps:

a) Check the **Enable** check box in the **Require accounting for the following types of connections** area.
b) 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.

# Recover 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.

The following table lists the common lockout conditions and how you might recover from them.

***Table 1: 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<br>TACACS+ CLI authentication<br>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.<br>**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.<br>**2.** Configure the local database as a fallback method so that you do not get locked out when the server is down. |

| 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.<br>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

- **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**

  This pane 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 Locked Out Users**

  This pane 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**.

- **Tools > Command Line Interface**

  This pane allows you to issue various non-interactive commands and view results.

# History for Management Access

*Table 2: History for Management Access*

| Feature Name | Platform Releases | Description |
|---|---|---|
| Setting the SSH key exchange mode is restricted to the Admin context | 9.12(2) | You must set the SSH key exchange in the Admin context; this setting is inherited by all other contexts.<br>New/Modified screen: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** > **SSH Settings** > **DH Key Exchange** |
| **enable** password change now required on login | 9.12(1) | The default **enable** password is blank. When you try to access privileged EXEC mode on the ASA, you are now required to change the password to a value of 3 characters or longer. You cannot keep it blank. The **no enable password** command is no longer supported.<br>At the CLI, you can access privileged EXEC mode using the **enable** command, the **login** command (with a user at privilege level 2+), or an SSH or Telnet session when you enable **aaa authorization exec auto-enable**. All of these methods require you to set the enable password.<br>This password change requirement is not enforced for ASDM logins. In ASDM, by default you can log in without a username and with the **enable** password.<br>No modified screens. |
| Configurable limitation of admin sessions | 9.12(1) | You can configure the maximum number of aggregate, per user, and per-protocol administrative sessions. Formerly, you could configure only the aggregate number of sessions. This feature does not affect console sessions. Note that in multiple context mode, you cannot configure the number of HTTPS sessions, where the maximum is fixed at 5 sessions. The **quota management-session** command is also no longer accepted in the system configuration, and is instead available in the context configuration. The maximum aggregate sessions is now 15; if you configured 0 (unlimited) or 16+, then when you upgrade, the value is changed to 15.<br>New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **Management Session Quota** |
| Notifications for administrative privilege level changes | 9.12(1) | When you authenticate for enable access (**aaa authentication enable console**) or allow privileged EXEC access directly (**aaa authorization exec auto-enable**), then the ASA now notifies users if their assigned access level has changed since their last login.<br>New/Modified screens:<br>**Status** bar > **Login History** icon |

| Feature Name | Platform Releases | Description |
|---|---|---|
| SSH stronger security | 9.12(1) | See the following SSH security improvements:<br>• Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default. The former default was Group 1 SHA1.<br>• HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha2-256 only). The former default was the medium set.<br>New/Modified screens:<br>• **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**<br>• **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** |
| Allow non-browser-based HTTPS clients to access the ASA | 9.12(1) | You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed.<br>New/Modified screens.<br>**Configuration** > **Device Management** > **Management Access** > **HTTP Non-Browser Client Support** |
| RSA key pair supports 3072-bit keys | 9.9(2) | You can now set the modulus size to 3072.<br>New or modified screen: **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificates** |
| VPN management access on Bridged Virtual Interfaces (BVIs) | 9.9(2) | You can now enable management services, such as **telnet**, **http**, and **ssh**, on a BVI if VPN **management-access** has been enabled on that BVI. For non-VPN management access, you should continue to configure these services on the bridge group member interfaces.<br>New or Modified commands: **https**, **telnet**, **ssh**, **management-access** |
| SSH version 1 has been deprecated | 9.9(1) | SSH version 1 has been deprecated, and will be removed in a future release. The default setting has changed from both SSH v1 and v2 to just SSH v2.<br>New/Modified screens:<br>• **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** |

| Feature Name | Platform Releases | Description |
|---|---|---|
| Separate authentication for users with SSH public key authentication and users with passwords | 9.6(3)/9.8(1) | In releases prior to 9.6(2), you could enable SSH public key authentication (**ssh authentication**) without also explicitly enabling AAA SSH authentication with the Local user database (**aaa authentication ssh console LOCAL**). In 9.6(2), the ASA required you to explicitly enable AAA SSH authentication. In this release, you no longer have to explicitly enable AAA SSH authentication; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for for usernames with *passwords*, and you can use any AAA server type (**aaa authentication ssh console radius_1**, for example). For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS.<br><br>We did not modify any screens. |
| Login history | 9.8(1) | By default, the login history is saved for 90 days. You can disable this feature or change the duration, up to 365 days. This feature only applies to usernames in the local database when you enable local AAA authentication for one or more of the management methods (SSH, ASDM, Telnet, and so on).<br><br>We introduced the following screen: **Configuration** > **Device Management** > **Users/AAA** > **Login History** |
| Password policy enforcement to prohibit the reuse of passwords, and prohibit use of a password matching a username | 9.8(1) | You can now prohibit the reuse of previous passwords for up to 7 generations, and you can also prohibit the use of a password that matches a username.<br><br>We modified the following screen: **Configuration** > **Device Management** > **Users/AAA** > **Password Policy** |
| ASA SSL Server mode matching for ASDM | 9.6(2) | For an ASDM user who authenticates with a certificate, you can now require the certificate to match a certificate map.<br><br>We modified the following screen: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** |
| SSH public key authentication improvements | 9.6(2) | In earlier releases, you could enable SSH public key authentication without also enabling AAA SSH authentication with the Local user database . The configuration is now fixed so that you must explicitly enable AAA SSH authentication. To disallow users from using a password instead of the private key, you can now create a username without any password defined.<br><br>We modifed the following screens:<br><br>**Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**<br><br>**Configuration** > **Device Management** > **Users/AAA** > **User Accounts** > **Add/Edit User Account** |

| Feature Name | Platform Releases | Description |
|---|---|---|
| ASDM management authorization | 9.4(1) | You can now configure management authorization separately for HTTP access vs. Telnet and SSH access.<br><br>We modified the following screen: **Configuration > Device Management > Users/AAA > AAA Access > Authorization** |
| ASDM username from certificate configuration | 9.4(1) | When you enable ASDM certificate authentication, you can configure how ASDM extracts the username from the certificate; you can also enable pre-filling the username at the login prompt.<br><br>We introduced the following screen: **Configuration > Device Management > Management Access > HTTP Certificate Rule.** |
| 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.<br><br>We modified the following screen: Configuration > Device Management > Users/AAA > AAA Access > Authorization. |
| HTTP redirect support for IPV6 | 9.1(7)/9.6(1) | When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address.<br><br>We added functionality to the following screen: **Configuration** > **Device Management** > **HTTP Redirect** |
| Configurable SSH encryption and integrity ciphers | 9.1(7.4)/9.3(3.6)(1) | Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. You might want to change the ciphers to be more or less strict, depending on your application. Note that the performance of secure copy depends partly on the encryption cipher used. By default, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use **ssh cipher encryption custom aes128-cbc**, for example.<br><br>We introduced the following screen: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** |
| 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 | 9.1(2) | An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic.<br><br>. |
| 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. |

| Feature Name | Platform Releases | Description |
|---|---|---|
| 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.<br><br>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).<br><br>We introduced the following screens:<br><br>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.<br><br>*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.<br><br>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.<br><br>We introduced the following screen: Configuration > Device Management > Management Access > Management Session Quota. |
| 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. |

| Feature Name | Platform Releases | Description |
|---|---|---|
| Management Access | 7.0(1) | We introduced this feature.<br>We introduced the following screens:<br>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. |