Platform Settings for Classic Devices

The following topics explain Firepower platform settings and how to configure them on Classic devices:

About Platform Settings for Classic Devices

Platform settings for managed devices are policy-based so that you can apply the same configuration to multiple devices. Use a *Firepower* platform settings policy with Classic devices:

- 7000/8000 series devices
- ASA FirePOWER modules
- NGIPSv

Note that for the FMC, many of these settings are handled in the *system configuration;* see System Configuration.

Table 1: Firepower Platform Settings for Classic Devices

Platform Setting	Description	See
Access List	Control which computers can access the system on specific ports.	Configure Access Lists for Classic Devices, on page 3
Audit Log	Configure the system to send an audit log to an external host.	Stream Audit Logs from Classic Devices, on page 3
Audit Log Certificate	As part of audit log secure streaming, require mutual authentication between Classic devices and the audit log server.	Require Valid Audit Log Server Certificates for Classic Devices, on page 5

Platform Setting	Description	See
External Authentication	Set the default user role for any 7000/8000 series device user who is authenticated by an external RADIUS, LDAP or Microsoft Active Directory repository.	Enable External Authentication to 7000/8000 Series Devices, on page 6
Language	Specify a different language for the web interface on a 7000/8000 series device.	Set the Language for the 7000/8000 Series Web Interface, on page 8
Login Banner	Create a custom login banner that appears when users log in.	Customize the Login Banner for Classic Devices , on page 9
Shell Timeout	Configure the amount of idle time, in minutes, before a user's login session times out due to inactivity.	Configure Session Timeouts for Classic Devices, on page 10
SNMP	Enable Simple Network Management Protocol (SNMP) polling.	Configure SNMP Polling on Classic Devices, on page 11
Time Synchronization	Manage time synchronization on the system.	Synchronize Time on Classic Devices with an NTP Server, on page 9
UCAPL/CC Compliance	Enable compliance with specific requirements set out by the United States Department of Defense.	Enable Security Certifications Compliance

Requirements for Platform Settings for Classic Devices

License Requirements

None.

Model Requirements

You can apply a Firepower platform settings policy to any Classic device.

Some platform settings apply only to 7000/8000 series devices because those devcies have a web interface: external authentication settings, display language, session timeouts, and so on. Applying these settings to ASA FirePOWER or NGIPSv has no effect.

You can also log into the local web interface on 7000/8000 series devices for non-policy based system configurations. See Local System Configuration for 7000/8000 Series Devices, on page 12.

Domain Requirements

None.

You can apply a Firepower platform setting policy at any Domain level.

Configure Platform Settings for Classic Devices

Platform settings for managed devices are policy-based so that you can apply the same configuration to multiple devices. Use a Firepower platform settings policy with Classic devices.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

See About Platform Settings for Classic Devices, on page 1 and Create a Platform Settings Policy.

Step 2 Choose the **Available Devices** where you want to deploy the policy by clicking **Policy Assignment**.

Step 3 Click **Add to Policy** (or drag and drop) to add the selected devices.

Step 4 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Configure Access Lists for Classic Devices

By default, access to Firepower devices is not restricted. Port 22 (SSH) is open for CLI access. For 7000/8000 series devices, port 443 (HTTPS) is also open for web interface access.

To operate in a more secure environment, consider adding access for specific IP addresses. You can also add access to poll for SNMP information over port 161.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **Access List**.

Step 3 To add access for one or more IP addresses, click **Add Rules**.

Step 4 In the **IP Address** field, enter an IP address or address range, or `any`.

Step 5 Choose **SSH**, **HTTPS**, **SNMP**, or a combination of these options to specify which ports you want to enable for these IP addresses.

Step 6 Click **Add**.

Step 7 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Stream Audit Logs from Classic Devices

Firepower appliances generate records (or *audit logs*) of user interactions. You can stream these audit logs to a syslog or HTTP server. Note that sending audit information to an external URL may affect system performance.

Tip On 7000/8000 series devices, you can also review audit logs on the device's web interface: Auditing the System.

Optionally, you can use Transport Layer Security (TLS) certificates to secure communications between Firepower devices and a trusted audit log server. For *each device* (client certificates are unique), you must generate a certificate signing request (CSR), submit it to a Certificate Authority (CA) for signing, then import the signed certificate onto the device. You cannot use the FMC to import audit log certificates onto its managed devices. These certificates are unique to each device, and you must log into *each device* to import them.

To ensure security, use a globally recognized and trusted CA. The same CA must sign:

- Both the client certificate and the server certificate, if you plan to require mutual authentication between the device and the audit log server.
- Any intermediate certificates in the certificate chain. If the signing CA requires you to trust an intermediate CA, you must provide the necessary certificate chain (or certificate path).

Audit logs have the following format:

```
timestamp host [tag] appliance_name: username@ip_address, subsystem, action
```

For example:

```
Mar 01 14:45:24 localhost [FIREPOWER] MyFirepowerAppliance: admin@10.1.1.2, System >
Configuration, Page View
```

Note that the tag is optional and user-configurable. Syslog events also have an optional facility and severity..

Before you begin

Make sure your devices can communicate with the server or servers where you plan to stream audit logs. For syslog streaming, the system uses port 7/UDP to verify that the syslog server is reachable when you save the configuration. Then, the system uses port 514/UDP to stream audit logs. If you secure the channel, you must manually configure port 1470 for TCP.

Step 1 (Optional) Set up secure communications with the audit log server.

For ASA FirePOWER and NGIPSv, you can generate a CSR with a tool like OpenSSL, then use the CLI to import the signed certificate: **configure audit_cert import**. For 7000/8000 series devices, use the system configuration (**System** > **Configuration**) on the device's web interface: Obtain a Signed Client Certificate for Secure Audit Log Streaming on a 7000/8000 Series Device, on page 13.

To verify that the certificate imported correctly, use the 7000/8000 series device's web interface, or the CLI: **show audit_cert**.

Step 2 On the FMC, choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 3 Click **Audit Log** to configure audit log streaming.

Syslog streaming:

a) Set **Send Audit Log to Syslog** to **Enabled**.
b) Provide **Host** information for the syslog server: IP address or fully qualified name.
c) Choose a **Facility** (Syslog Alert Facilities) and **Severity** (Syslog Severity Levels).

Attention When you enable **Send Audit Log to Syslog** and provide **Host** information, syslog messages are also sent to the configured host in addition to the audit logs; see Filter Syslogs from Audit Logs, on page 6.

HTTP streaming:

a) Set **Send Audit Log to HTTP Server** to **Enabled**.

b) Provide a **URL to Post Audit** where you want to send audit logs. HTTPS is supported.

The URL must correspond to a Listener program that expects the following HTTP POST variables: `subsystem`, `actor`, `event_type`, `message`, `action_source_ip`, `action_destination_ip`, `result`, `time`, `tag` (if provided).

Step 4 (Optional) Enter a **Tag** in include in each message. For example, you might want to tag Firepower audit logs with **`FIREPOWER`**.

Step 5 Click **Save**.
If you configured syslog streaming, the system verifies that the syslog server is reachable.

What to do next

- (Optional) If you configured secure communications, we recommend you also require mutual authentication between the device and the audit log server: Require Valid Audit Log Server Certificates for Classic Devices, on page 5.
- (Optional) If you enabled streaming the audit logs to a syslog server and want to filter the syslog messages from the audit logs: Filter Syslogs from Audit Logs, on page 6.
- Deploy configuration changes; see Deploy Configuration Changes.

Require Valid Audit Log Server Certificates for Classic Devices

For additional security, we recommend you require mutual authentication between Firepower appliances and the audit log server. To accomplish this, load one or more certificate revocation lists (CRLs). You cannot stream audit logs to servers with revoked certificates listed in those CRLs.

Firepower supports CRLs encoded in Distinguished Encoding Rules (DER) format. Note that these are the same CRLs that the system uses to validate HTTPS client certificates for the FMC web interface.

Before you begin

Obtain and import a signed client certificate onto each device.

- For ASA FirePOWER and NGIPSv, you can generate a CSR with a tool like OpenSSL, then use the CLI to import the signed certificate: **configure audit_cert import**.
- For 7000/8000 series devices, use the system configuration (**System** > **Configuration**) on the device's web interface: Obtain a Signed Client Certificate for Secure Audit Log Streaming on a 7000/8000 Series Device, on page 13.

Use a globally recognized and trusted CA. The same CA must sign the client certificates you imported *and* the server certificate you will require with this procedure.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **Audit Log Certificate**.

Step 3 Select **Enable TLS**, then **Enable Mutual Authentication**.

We recommend you enable mutual authentication. If you do not, the device will accept server certificates without verification.

Step 4 Select **Enable Fetching of CRL**, provide the URL to a CRL file, and click **Add CRL**.

You can add up to 25 CRLs. When you deploy, the system will schedule CRL updates. To set the update frequency, see Configuring Certificate Revocation List Downloads.

Step 5 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Filter Syslogs from Audit Logs

When you enable **Send Audit Log to Syslog** and provide **Host** information, syslog messages are also sent to the configured host in addition to the audit logs. This behavior is caused by the fact that the `/etc/syslog-ng.d/syslog-tls.conf` is created when you deploy the Firepower platform settings policy, which results in syslog messages being forwarded/sent to the configured host, instead of only sending the audit logs.

If your auditing policy does not want or require these syslog records, you can prevent those syslogs from being streamed to the configured host. To filter syslogs from audit logs, you must have access to an appliance's **admin** user account, and you must be able to either access the appliance's console or open a secure shell.

⚠ **Caution** Make sure that only authorized personnel have access to the appliance and to its **admin** account.

Step 1 In the `/etc/syslog-ng.conf` file, comment out the `@include "/etc/syslog-ng.d/*.conf"` line.

Example:

```
#@include "/etc/syslog-ng.d/*.conf"
```

Step 2 Reload the syslog configuration file. Use the `syslog-ng-ctl reload` command to reload the configuration file without having to restart the application.

Example:

```
syslog-ng-ctl reload
```

Enable External Authentication to 7000/8000 Series Devices

Use device platform settings to allow users of 7000/8000 series devices to authenticate to an LDAP or RADIUS server, rather than using the local database.

Before you begin

Configure external authentication objects. See Configure External Authentication.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **External Authentication**.

Step 3 From the **Status** drop-down list, choose **Enabled**.

Step 4 From the **Default User Role** drop-down list, choose user roles to define the default permissions you want to grant to externally authenticated users.

Step 5 If you want to use the external server to authenticate CLI or shell access accounts, choose **Enabled** from the **Shell Authentication** drop-down list.

Step 6 If you want to enable CAC authentication and authorization, choose an available CAC authentication object from the **CAC Authentication** drop-down list.

For more information, see Configure Common Access Card Authentication with LDAP.

Step 7 Check the check boxes next to the each external authentication object that you want to use. If you enable more than 1 object, then users are checked against servers in the order specified. See the next step to reorder servers.

If you enable shell authentication, you must enable an external authentication object that includes a **Shell Access Filter**. CLI/shell access users can only authenticate against the server whose authentication object is highest in the list.

If you need both CLI and CAC authentication, you must use separate authentication objects for each purpose.

Step 8 (Optional) Use the up and down arrows to change the order in which authentication servers are accessed when an authentication request occurs.

Step 9 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

About External Authentication for 7000/8000 Series Devices

If you create an authentication object referencing an external authentication server, you can enable external authentication to let users logging into the managed device authenticate to that server, rather than using the local database.

When you enable external authentication, the system verifies the user credentials against users on an LDAP or RADIUS server. In addition, if a user has local, internal authentication enabled and the user credentials are not found in the internal database, the system then checks the external server for a set of matching credentials. If a user has the same username on multiple systems, all passwords across all servers work. Note, however, that if authentication fails on the available external authentication servers, the system does not revert to checking the local database.

When you enable external authentication, you can set the default user role for any user whose account is externally authenticated. You can select multiple roles, as long as those roles can be combined. For example, if you enable external authentication that retrieves only users in the Network Security group in your company, you may set the default user role to include the Security Analyst role so users can access collected event data without any additional user configuration on your part. However, if your external authentication retrieves records for other personnel in addition to the security group, you would probably want to leave the default role unselected.

If no access role is selected, users can log in but cannot access any functionality. After a user attempts to log in, their account is listed on the user management page (**System** > **Users**), where you can edit the account settings to grant additional permissions.

Tip If you configure the system to use one user role and apply the policy, then later modify the configuration to use different default user roles, any user accounts created before the modification retain the first user role until you modify the accounts, or delete and recreate them.

If you want to specify the set of users who can authenticate against the LDAP server for CLI/shell access or for CAC authentication and authorization, you must create separate authentication objects for each and enable the objects separately.

If a user with internal authentication attempts to log in, the system first checks if that user is in the local user database. If the user exists, the system then checks the username and password against the local database. If a match is found, the user logs in successfully. If the login fails, however, and external authentication is enabled, the system checks the user against each external authentication server in the authentication order shown in the configuration. If the username and password match results from an external server, the system changes the user to an external user with the default privileges for that authentication object.

If an external user attempts to log in, the system checks the username and password against the external authentication server. If a match is found, the user logs in successfully. If the login fails, the user login attempt is rejected. External users cannot authenticate against the user list in the local database. If the user is a new external user, an external user account is created in the local database with the default privileges from the external authentication object.

Set the Language for the 7000/8000 Series Web Interface

The language you specify here is used for the web interface for every user who logs in. You can choose from:

- English
- Chinese (simplified)
- Chinese (traditional)
- Japanese
- Korean

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **Language**.

Step 3 Choose the language you want to use.

Step 4 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Customize the Login Banner for Classic Devices

You can customize the CLI login banner for Classic devices. For 7000/8000 series devices, the login banner also appears in the web interface. Note that if the banner is too large or causes errors, CLI sessions can fail when the system attempts to display the banner.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Choose **Login Banner**.

Step 3 In the **Custom Login Banner** field, enter the login banner text you want to use.

The system will not preserve tab spacing.

Step 4 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Synchronize Time on Classic Devices with an NTP Server

Synchronizing the system time on your FMC and all its managed devices is essential to successful operations. If your deployment includes the Firepower Threat Defense devices, see Configure NTP Time Synchronization for Threat Defense.

The device supports NTPv4.

⚠ **Caution** Unintended consequences can occur when time is not synchronized between the FMC and managed devices.

After you deploy, it may take a few minutes for managed devices to synchronize with the configured NTP servers.

Before you begin

Make sure the device can communicate with the NTP server or servers you plan to use. You can either:

- (Recommended.) Use the same NTP servers as the FMC: Synchronize Time on the FMC with an NTP Server.

  If you choose this option, the device gets its time directly from the configured NTP server. If the device's configured NTP servers are not reachable for any reason, it synchronizes its time with the FMC.

- If your device cannot reach an NTP server or your organization does not have one, you must use the **Via NTP from Management Center** option discussed in the following proecedure.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **Time Synchronization**.

Step 3 Specify how time is synchronized:

- **Via NTP from**: If your Firepower Management Center is using NTP servers on the network, select this option and enter the fully-qualified DNS name (such as ntp.example.com), or IPv4 or IPv6 address, of the same NTP servers you specified in **System > Configuration > Time Synchronization**. If the NTP servers are not reachable, the Firepower Management Center acts as an NTP server.
- **Via NTP from Management Center**: (Default). The managed device gets time from the NTP servers you configured for the Firepower Management Center (except for authenticated NTP servers) and synchronizes time with those servers directly. However, if any of the following are true, the managed device synchronizes time from the Firepower Management Center:
  - The Firepower Management Center's NTP servers are not reachable by the device.
  - The Firepower Management Center has no unauthenticated servers.

Step 4 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Configure Session Timeouts for Classic Devices

Unattended login sessions may be security risks. You can configure the amount of idle time before a user's login session times out due to inactivity. The maximum value is 24 hours, or 1440 minutes.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **Shell Timeout**.

Step 3 Configure session timeouts:

- Web interface (7000/8000 series only): Enter a **Browser Session Timeout (Minutes)**.

  You can exempt specific web interface users from timeout, for scenarios where you plan to passively, securely monitor the system for long periods of time. For more information, see Add an Internal User at the Web Interface.
- CLI: Enter a **Shell Timeout (Minutes)**.

Step 4 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Configure SNMP Polling on Classic Devices

Simple Network Management Protocol (SNMP) polling allows access to the standard management information base (MIB) on Firepower devices, which includes system details such as contact, administrative, location, service information, IP addressing and routing information, and transmission protocol usage statistics. Additional MIBs for 7000/8000 series devices include statistics on traffic passing through physical interfaces, logical interfaces, virtual interfaces, ARP, NDP, virtual bridges, and virtual routers. Note that enabling SNMP polling does not cause the system to send SNMP traps; it only makes the information in the MIBs available for polling by your network management system.

The system supports SNMPv1, v2, and v3. SNMPv2 only supports read-only communities and SNMPv3 only supports read-only users. SNMPv3 also supports encryption with AES128.

Before you begin

Add SNMP access for each computer you plan to use to poll the system. See Configure Access Lists for Classic Devices, on page 3.

Note The SNMP MIB contains information that could be used to attack your deployment. We recommend that you restrict your access list for SNMP access to the specific hosts that will be used to poll for the MIB. We also recommend you use SNMPv3 and use strong passwords for network management access.

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **SNMP**.

Step 3 From the **SNMP Version** drop-down list, choose the SNMP version you want to use:

- **Version 1** or **Version 2**: Enter a read-only SNMP community name in the **Community String** field, then skip to the end of the procedure.

  Note Do not include special characters (< > / % # & ? ', etc.) in the SNMP community string name.

- **Version 3**: Click **Add User** to display the user definition page. SNMPv3 only supports read-only users and encryption with AES128.

Step 4 Enter a **Username**.

Step 5 Choose the protocol you want to use for authentication from the **Authentication Protocol** drop-down list.

Step 6 Enter the password required for authentication with the SNMP server in the **Authentication Password** field.

Step 7 Re-enter the authentication password in the **Verify Password** field.

Step 8 Choose the privacy protocol you want to use from the **Privacy Protocol** list, or choose **None** to not use a privacy protocol.

Step 9 Enter the SNMP privacy key required by the SNMP server in the **Privacy Password** field.

Step 10 Re-enter the privacy password in the **Verify Password** field.

Step 11 Click **Add**.

Step 12 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Local System Configuration for 7000/8000 Series Devices

You can log into the local web interface on 7000/8000 series devices for non-policy based system configurations. Many of these configurations parallel FMC system configurations, and are documented in the FMC system configuration chapter: System Configuration.

Table 2: Local System Configurations for 7000/8000 Series Devices

System Configuration	Description	See
Audit Log Certificate	As part of audit log secure streaming, obtain and import a signed client certificate for 7000/8000 series devices.	Obtain a Signed Client Certificate for Secure Audit Log Streaming on a 7000/8000 Series Device, on page 13
Change Reconciliation	Send a detailed report of changes to the system over the last 24 hours.	Change Reconciliation
Console Configuration	Configure console access via VGA or serial port, or via Lights-Out Management (LOM).	Remote Console Access Management
HTTPS Certificate	Request an HTTPS server certificate, if needed, from a trusted authority and upload certificates to the system.	HTTPS Certificates
Information	View current information about the appliance and edit the display name.	Appliance Information
Management Interfaces	Change options such as the IP address, hostname, and proxy settings of the appliance.	Configure Management Interfaces on a 7000/8000 Series Device, on page 14
Process	Shut down, reboot, or restart Firepower processes.	Shut Down or Restart a 7000/8000 Series Device, on page 17
Prohibit Packet Transfer	Disable sending packet data from 7000/8000 series devices to the FMC in a low-bandwidth deployment.	Prohibit Packet Transfer to FMC, on page 14
Time	View the current time settings.	View System Time for 7000/8000 Series Devices, on page 17

Obtain a Signed Client Certificate for Secure Audit Log Streaming on a 7000/8000 Series Device

Optionally, you can use Transport Layer Security (TLS) certificates to secure communications between Firepower devices and a trusted audit log server. For *each device* (client certificates are unique), you must generate a certificate signing request (CSR), submit it to a Certificate Authority (CA) for signing, then import the signed certificate onto the device. You cannot use the FMC to import audit log certificates onto its managed devices. These certificates are unique to each device, and you must log into *each device* to import them.

To ensure security, use a globally recognized and trusted CA. The same CA must sign:

- Both the client certificate and the server certificate, if you plan to require mutual authentication between the device and the audit log server.
- Any intermediate certificates in the certificate chain. If the signing CA requires you to trust an intermediate CA, you must provide the necessary certificate chain (or certificate path).

The system generates certificate request keys in Base-64 encoded PEM format.

Step 1 Log into the device's web interface and choose **System** > **Configuration**.

Step 2 Click **Audit Log Certificate**.

Step 3 Generate a CSR.

a) Click **Generate New CSR**.
b) Fill out the required location and organizational information.
c) Enter the fully qualified domain name of the server for which you want to request a certificate in the **Common Name** field. If the common name and the DNS hostname do not match, audit log streaming will fail.
d) Click **Generate**.

Step 4 Create a text file for the CSR.

a) Copy and paste the entire block of text in the certificate request, including the `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST` lines.
b) Save the file as *`clientname`*`.csr`, where *`clientname`* is the name of the device where you plan to use the certificate.

Step 5 Submit the CSR to the CA and wait to receive the signed certificate.

Step 6 Import the signed certificate onto the device.

If you left the page, browse back to **System** > **Configuration > Audit Log Certificate**, then click **Import Audit Client Certificate**. Copy and paste the following:

- **Client Certificate**: All of the text in the signed certificate, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines.
- **Private Key**: All of the text in the private key file, including the `BEGIN RSA PRIVATE KEY` and `END RSA PRIVATE KEY` lines.
- **Certificate Chain**: All of the text in each required intermediate certificate.

Make sure you import the correct certificate. Client certificates are unique.

Step 7 Click **Save**.

What to do next

If you have not already, use the device platform settings on the FMC to configure audit log streaming: Stream Audit Logs from Classic Devices, on page 3.

Prohibit Packet Transfer to FMC

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Any	7000 & 8000 Series	N/A	Admin

You may want to disable sending packet data from 7000 or 8000 Series devices to the Firepower Management Center in a low-bandwidth deployment if you are not concerned about the specific content of the packet that triggered an intrusion policy violation.

Step 1 In the local web interface of your 7000 or 8000 Series device, choose **System** > **Configuration**.

Step 2 Click **Information**.

Step 3 Select **Prohibit Packet Transfer to the Management Center**.

Step 4 Click **Save**.

Configure Management Interfaces on a 7000/8000 Series Device

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Any	7000 & 8000 Series	Global only	Admin

Modify the management interface settings on the managed device using the web interface. You can optionally enable an event interface if your model supports it. For more information on management interfaces, see About Device Management Interfaces.

⚠

Caution Be careful when making changes to the management interface; if you cannot re-connect because of a configuration error, you will need to access the device console port and reconfigure the settings at the CLI.

Step 1 Choose **System** > **Configuration**, and then choose **Management Interfaces**.

Step 2 In the **Interfaces** area, click **Edit** next to the interface that you want to configure.

All available interfaces are listed in this section. You cannot add more interfaces.

You can configure the following options on each management interface:

- **Enabled**—Enable the management interface. Do **not** disable the default eth0 management interface. Some processes require the eth0 interface.

- **Channels**—(8000 series only) Configure an event-only interface. You can enable the eth1 management interface on your 8000 series device to act as an event interface. To do so, uncheck the **Management Traffic** check box, and leave the **Event Traffic** check box checked. For the eth0 management interface, leave both check boxes checked.

The Firepower Management Center event-only interface cannot accept management channel traffic, so you should simply disable the management channel on the device event interface.

You can optionally disable **Event Traffic** for the management interface. In either case, the device will try to send events on the event-only interface, and if that interface is down, it will send events on the management interface even if you disable the event channel.

You cannot disable both event and management channels on an interface.

- **Mode**—Specify a link mode. Note that any changes you make to auto-negotiation are ignored for GigabitEthernet interfaces.
- **MTU**—Set the maximum transmission unit (MTU). The default is 1500. The range within which you can set the MTU can vary depending on the model and interface type.

  Because the system automatically trims 18 bytes from the configured MTU value, any value below 1298 does not comply with the minimum IPv6 MTU setting of 1280, and any value below 594 does not comply with the minimum IPv4 MTU setting of 576. For example, the system automatically trims a configured value of 576 to 558.
- **MDI/MDIX**—Set the **Auto-MDIX** setting.
- **IPv4 Configuration**—Set the IPv4 IP address. Choose:
  - **Static**—Manually enter the **IPv4 Management IP** address and **IPv4 Netmask**.
  - **DHCP**—Set the interface to use DHCP (eth0 only).
  - **Disabled**—Disable IPv4. Do **not** disable both IPv4 and IPv6.
- **IPv6 Configuration**—Set the IPv6 IP address. Choose:
  - **Static**—Manually enter the **IPv6 Management IP** address and **IPv6 Prefix Length**.
  - **DHCP**—Set the interface to use DHCPv6 (eth0 only).
  - **Router Assigned**—Enable stateless autoconfiguration.
  - **Disabled**—Disable IPv6. Do **not** disable both IPv4 and IPv6.
  - **IPv6 DAD**—When you enable IPv6, enable or disable duplicate address detection (DAD). You might want to disable DAD because the use of DAD opens up the possibility of denial of service attacks. If you disable this setting, you need check manually that this interface is not using an already-assigned address.

Step 3 In the **Routes** area, edit a static route by clicking **Edit** (✎), or add a route by clicking **Add** (⊕). View the route statistics by clicking **View** (🔍).

Note You need to add a static route for the event-only interface if the Firepower Management Center is on a remote network; otherwise, all traffic will match the default route through the management interface. For the default route, you can change only the gateway IP address.The egress interface is chosen automatically by matching the specified gateway to the interface's network. For information about routing, see Network Routes on Device Management Interfaces.

You can configure the following settings for a static route:

- **Destination**—Set the destination address of the network to which you want to create a route.
- **Netmask** or **Prefix Length**—Set the netmask (IPv4) or prefix length (IPv6) for the network.

- **Interface**—Set the egress management interface.
- **Gateway**—Set the gateway IP address.

Step 4 In the **Shared Settings** area, set network parameters shared by all interfaces.

Note If you selected **DHCP** for the eth0 interface, you cannot manually specify some shared settings derived from the DHCP server.

You can configure the following shared settings:

- **Hostname**—Set the device hostname. If you change the hostname, reboot the device if you want the new hostname reflected in syslog messages. Syslog messages do not reflect a new hostname until after a reboot.
- **Domains**—Set the search domain(s) for the device, separated by commas. These domains are added to hostnames when you do not specify a fully-qualified domain name in a command, for example, **ping system**. The domains are used only on the management interface, or for commands that go through the management interface.
- **Primary DNS Server**, **Secondary DNS Server**, **Tertiary DNS Server**—Set the DNS servers to be used in order of preference.
- **Remote Management Port**—Set the remote management port for communication with the FMC. The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.

  Note Cisco **strongly** recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for **all** devices in your deployment that need to communicate with each other.

Step 5 In the **ICMPv6** area, configure ICMPv6 settings.

- **Allow Sending Echo Reply Packets**—Enable or disable Echo Reply packets. You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes.
- **Allow Sending Destination Unreachable Packets**—Enable or disable Destination Unreachable packets. You might want to disable these packets to guard against potential denial of service attacks.

Step 6 In the **LCD Panel** area, check the **Allow reconfiguration of network settings** check box to enable changing network settings using the device’s LCD panel.

You can use the LCD panel to edit the IP address for the device. Confirm that any changes you make are reflected on the managing Firepower Management Center. In some cases, you may need to update the data manually on the Firepower Management Center as well.

Caution Allowing reconfiguration using the LCD panel can present a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. The web interface warns you that enabling this option is a potential security issue.

Step 7 In the **Proxy** area, configure HTTP proxy settings.

The device is configured to directly-connect to the internet on ports TCP/443 (HTTPS) and TCP/80 (HTTP). You can use a proxy server, to which you can authenticate via HTTP Digest.

Note Proxies that use NT LAN Manager (NTLM) authentication are not supported.

a) Check the **Enabled** check box.
b) In the **HTTP Proxy** field, enter the IP address or fully-qualified domain name of your proxy server.
c) In the **Port** field, enter a port number.
d) Supply authentication credentials by choosing **Use Proxy Authentication**, and then provide a **User Name** and **Password**.

Step 8 Click **Save**.

Step 9 If you changed the management IP address, it might affect communication between the FMC and the managed device.

Changing the IP address will not affect the current connection. However, if the device or FMC reloads, then the connection needs to be reestablished. You need at least one of the devices (FMC or managed device) to have the correct IP address of the peer. For example, if you specified a NAT ID (instead of an IP address) for the FMC during device setup, then the device IP address that you defined on the FMC when you added the device will be wrong, and the FMC will not be able to reestablish communications. In this case, you must change the management IP address of the device in the FMC; see Update the Hostname or IP Address in FMC.

Shut Down or Restart a 7000/8000 Series Device

Step 1 On the device's web interface, choose **System** > **Configuration**.

Step 2 Choose **Process**.

Step 3 Do one of the following:

Shut down	Click **Run Command** next to **Shutdown Appliance**. **Caution** Do **not** shut off Firepower appliances using the power button; it may cause a loss of data. Using the web interface (or CLI) prepares the system to be safely powered off and restarted without losing configuration data.
Reboot	Click **Run Command** next to **Reboot Appliance**. **Note** Rebooting logs you out, and the system runs a database check that can take up to an hour to complete.
Restart the console	Click **Run Command** next to **Restart Appliance Console**.
Restart the Snort process	Click **Run Command** next to **Restart Snort**. **Caution** Restarting the Snort process temporarily interrupts traffic inspection. Whether traffic drops during this interruption or passes without inspection depends on how the device is configured. See Snort® Restart Traffic Behavior for more information.

View System Time for 7000/8000 Series Devices

Time settings are displayed on most pages in local time using the time zone you set on the Time Zone page in User Preferences, but are stored on the appliance using UTC time. In addition, the current time appears in

UTC at the top of the Time Synchronization page (local time is displayed in the Manual clock setting option, if enabled).

Restriction The Time Zone function (in User Preferences) assumes that the default system clock is set to UTC time. ***Do not change this.*** Changing the system time from UTC is ***not*** supported, and you will have to reimage the device.

Use this procedure to verify system time information on 7000 and 8000 Series devices.

Step 1 Log into the device's web interface and choose **System** > **Configuration**.

Step 2 Click **Time**.

If you are using NTP, see NTP Server Status.