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:

- 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
Login Banner	Create a custom login banner that appears when users log in.	Customize the Login Banner for Classic Devices , on page 6

Platform Setting	Description	See
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 8
SNMP	Enable Simple Network Management Protocol (SNMP) polling.	Configure SNMP Polling on Classic Devices, on page 8
Time Synchronization	Manage time synchronization on the system.	Synchronize Time on Classic Devices with an NTP Server, on page 7
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.

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.

Procedure

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.

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.

Procedure

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.

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.

Procedure

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**.

To verify that the certificate imported correctly, use **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**.

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.

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**.

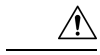
What to do next

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.

Procedure

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
```

Customize the Login Banner for Classic Devices

You can customize the CLI login banner for Classic devices. Note that if the banner is too large or causes errors, CLI sessions can fail when the system attempts to display the banner.

Procedure

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.

  Note that even if you configure secure communications between the FMC and an NTP server (**Use the authenticated NTP server only**), device connections to that server do not use authentication.

  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.

Procedure

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.

Procedure

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

Step 2 Click **CLI Timeout**.

Step 3 Enter a **CLI 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. 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.

Procedure

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.