

System Configuration

The following topics explain how to configure system configuration settings on Firepower Management Centers and managed devices:

- Requirements and Prerequisites for the System Configuration, on page 2
- About System Configuration, on page 2
- Appliance Information, on page 4
- HTTPS Certificates, on page 5
- External Database Access Settings, on page 11
- Database Event Limits, on page 12
- Management Interfaces, on page 15
- Shut Down or Restart, on page 23
- Remote Storage Management, on page 24
- Change Reconciliation, on page 27
- Policy Change Comments, on page 28
- Access List, on page 29
- Audit Logs, on page 30
- Audit Log Certificate, on page 33
- Dashboard Settings, on page 38
- DNS Cache, on page 38
- Email Notifications, on page 39
- Language Selection, on page 40
- Login Banners, on page 41
- SNMP Polling, on page 41
- Security Certifications Compliance, on page 43
- Time and Time Synchronization, on page 46
- Session Timeouts, on page 50
- Vulnerability Mapping, on page 51
- Remote Console Access Management, on page 52
- REST API Preferences, on page 57
- VMware Tools and Virtual Systems, on page 58

Requirements and Prerequisites for the System Configuration

Model Support

FMC

Some settings also apply to 7000 & 8000 Series devices.

Supported Domains

Global

User Roles

Admin

About System Configuration

System configuration settings apply to either a Firepower Management Center or a Classic managed device (7000 and 8000 Series, ASA FirePOWER, NGIPSv):

- For the Firepower Management Center these configuration settings are part of a "local" system configuration. Note that system configuration on the Firepower Management Center is specific to a single system, and changes to a FMC's system configuration affect only that system.
- For a Classic managed device, you apply a configuration from the Firepower Management Center as part of a platform settings policy. You create a shared policy to configure a subset of the system configuration settings, appropriate for managed devices, that are likely to be similar across a deployment.

Tip For 7000 and 8000 Series devices, you can perform limited system configuration tasks from the local web interface, such as console configuration and remote management. These are not the same configurations that you apply to a 7000 or 8000 Series device using a platform settings policy.

Navigating the Firepower Management Center System Configuration

The system configuration identifies basic settings for a Firepower Management Center.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Use the navigation panel to choose configurations to change; see Table 1: System Configuration Settings , on page 3 for more information.

System Configuration Settings

Note that for managed devices, many of these configurations are handled by a *platform settings* policy applied from the FMC; see Platform Settings Policies. For 7000/8000 series devices, you can also log into the local web interface for non-policy based system configurations; see Local System Configuration for 7000/8000 Series Devices.

Table 1: System Configuration Settings

Setting	Description
Access Control Preferences	Configure the system to prompt users for a comment when they add or modify an access control policy; see Policy Change Comments, on page 28.
Access List	Control which computers can access the system on specific ports; see Access List, on page 29.
Audit Log	Configure the system to send an audit log to an external host; see Audit Logs, on page 30.
Audit Log Certificate	Configure the system to secure the channel when streaming the audit log to an external host; see Audit Log Certificate, on page 33 .
Change Reconciliation	Configure the system to send a detailed report of changes to the system over the last 24 hours; see Change Reconciliation, on page 27.
Console Configuration	Configure console access via VGA or serial port, or via Lights-Out Management (LOM); see Remote Console Access Management, on page 52.
Dashboard	Enable Custom Analysis widgets on the dashboard; see Dashboard Settings, on page 38.
Database	Specify the maximum number of each type of event that the Firepower Management Center can store; see Database Event Limits, on page 12.
DNS Cache	Configure the system to resolve IP addresses automatically on event view pages; see DNS Cache, on page 38.
Email Notification	Configure a mail host, select an encryption method, and supply authentication credentials for email-based notifications and reporting; see Email Notifications, on page 39.
External Database Access	Enable external read-only access to the database, and provide a client driver to download; see External Database Access Settings, on page 11.
HTTPS Certificate	Request an HTTPS server certificate, if needed, from a trusted authority and upload certificates to the system; see HTTPS Certificates, on page 5.
Information	View current information about the appliance and edit the display name; see Appliance Information, on page 4.
Intrusion Policy Preferences	Configure the system to prompt users for a comment when they modify an intrusion policy; see Policy Change Comments, on page 28.
Language	Specify a different language for the web interface; see Language Selection, on page 40.
Login Banner	Create a custom login banner that appears when users log in; see Login Banners, on page 41.

Setting	Description
Management Interfaces	Change options such as the IP address, hostname, and proxy settings of the appliance; see Management Interfaces, on page 15.
Network Analysis Policy Preferences	Configure the system to prompt users for a comment when they modify a network analysis policy; see Policy Change Comments, on page 28.
Process	Shut down, reboot, or restart Firepower processes; see Shut Down or Restart, on page 23.
Remote Storage Device	Configure remote storage for backups and reports; see Remote Storage Management, on page 24.
REST API Preferences	Enable or disable access to the Firepower Management Center via the Firepower REST API; see REST API Preferences, on page 57.
Shell Timeout	Configure the amount of idle time, in minutes, before a user's login session times out due to inactivity; see Session Timeouts, on page 50.
SNMP	Enable Simple Network Management Protocol (SNMP) polling; see SNMP Polling, on page 41.
Time	View and change the current time setting; see Time and Time Synchronization, on page 46.
Time Synchronization	Manage time synchronization on the system; see Time and Time Synchronization, on page 46.
UCAPL/CC Compliance	Enable compliance with specific requirements set out by the United States Department of Defense; see Enable Security Certifications Compliance, on page 45.
VMware Tools	Enable and use VMware Tools on a Firepower Management Center Virtual; see VMware Tools and Virtual Systems, on page 58.
Vulnerability Mapping	Map vulnerabilities to a host IP address for any application protocol traffic received or sent from that address; see Vulnerability Mapping, on page 51.

Related Topics

About Platform Settings for Classic Devices

Appliance Information

The **System > Configuration** page of the web interface includes the information listed in the table below. Unless otherwise noted, all fields are read-only.



Note See also the **Help > About** page, which includes similar but slightly different information.

Field	Description
Name	A descriptive name you assign to the FMCappliance. Although you can use the host name as the name of the appliance, entering a different name in this field does not change the host name.
Product Model	The model name of the appliance.

Field	Description
Serial Number	The serial number of the appliance.
Software Version	The version of the software currently installed on the appliance.
Prohibit Packet Transfer to the Firepower Management Center	Specifies whether the managed device sends packet data with events, allowing the data to be stored on the Firepower Management Center. This setting is available on the local web interface on 7000 and 8000 Series devices.
Operating System	The operating system currently running on the appliance.
Operating System Version	The version of the operating system currently running on the appliance.
IPv4 Address	The IPv4 address of the default (`eth0`) management interface. If IPv4 management is disabled, this field indicates that.
IPv6 Address	The IPv6 address of the default (`eth0`) management interface. If IPv6 management is disabled, this field indicates that.
Current Policies	The system-level policies currently deployed. If a policy has been updated since it was last deployed, the name of the policy appears in italics.
Model Number	The appliance-specific model number stored on the internal flash drive. This number may be important for troubleshooting.

HTTPS Certificates

Secure Sockets Layer (SSL)/TLS certificates enable Firepower Management Centers and 7000 and 8000 Series devices to establish an encrypted channel between the system and a web browser. A default certificate is included with all Firepower devices, but it is not generated by a certificate authority (CA) trusted by any globally known CA. For this reason, consider replacing it with a custom certificate signed by a globally known or internally trusted CA.



Caution The FMC supports 2048-bit HTTPS certificates. If the certificate used by the FMC was generated using a public server key larger than 2048 bits, you will not be able to log in to the FMC web interface. If this happens, contact Cisco TAC.

Default HTTPS Server Certificates

If you use the default server certificate provided with an appliance, do not configure the system to require a valid HTTPS client certificate for web interface access because the default server certificate is not signed by the CA that signs your client certificate.

The default server certificate provided with an appliance expires 20 years from when it was first generated.

Custom HTTPS Server Certificates

You can use the Firepower Management Center web interface to generate a server certificate request based on your system information and the identification information you supply. You can use that request to sign a certificate if you have an internal certificate authority (CA) installed that is trusted by your browser. You can also send the resulting request to a certificate authority to request a server certificate. After you have a signed certificate from a certificate authority (CA), you can import it.

HTTPS Server Certificate Requirements

When you use HTTPS certificates to secure the connection between your web browser and the Firepower appliance web interface, you must use certificates that comply with the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280). When you import a server certificate to the appliance, the system rejects the certificate if it does not comply with version 3 (X.509 v3) of that standard.

Before importing an HTTPS server certificate, be certain it includes the following fields:

Certificate Field	Description
Version	Version of the encoded certificate. Use version 3. See RFC 5280, section 4.1.2.1.
Serial number	A positive integer assigned to the certificate by the issuing CA. Issuer and serial number together uniquely identify the certificate. See RFC 5280, section 4.1.2.2.
Signature	Identifier for the algorithm used by the CA to sign the certificate. Must match the signatureAlgorithm field. See RFC 5280, section 4.1.2.3.
Issuer	Identifies the entity that signed and issued the certificate. See RFC 5280, section 4.1.2.4.
Validity	Interval during which the CA warrants that it will maintain information about the status of the certificate. See RFC 5280, section 4.1.2.5.
Subject	Identifies the entitity associated with the public key stored in the subject public key field; must be an X.500 disinguished name (DN). See RFC 5280, section 4.1.2.6.
Subject Public Key Info	Public key and an identifier for its algorithm. See RFC 5280, section 4.1.2.7.
Authority Key Identifier	Provides a means of identifying the public key corresponding to the private key used to sign a certificate. See RFC 5280, section 4.2.1.1.
Subject Key Identifier	Provides a means of identifying certificates that contain a particular public key. See RFC 5280, section 4.2.1.2.

Certificate Field	Description
Key Usage	Defines the purpose of the key contained in the certificates. See RFC 5280, section 4.2.1.3.
Basic Constraints	Identifies whether the certificate Subject is a CA, and the maximum depth of validation certification paths that include this certificate. See RFC 5280, section 4.2.1.9. For server certificates used in Firepower appliances, use `critical CA:FALSE`.
Extended Key Usage extension	Indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the Key Usage extension. See RFC 5280, section 4.2.1.12. Be certain you import certificates that can be used as server certificates.
signatureAlgorithm	Identifier for the algorithm the CA used to sign the certificate. Must match the Signature field. See RFC 5280, section 4.1.1.2.
signatureValue	Digital signature. See RFC 5280, section 4.1.1.3.

HTTPS Client Certificates

You can restrict access to the Firepower System web server using client browser certificate checking. When you enable user certificates, the web server checks that a user's browser client has a valid user certificate selected. That user certificate must be generated by the same trusted certificate authority that is used for the server certificate. The browser cannot load the web interface under any of the following circumstances:

- The user selects a certificate in the browser that is not valid.
- The user selects a certificate in the browser that is not generated by the certificate authority that signed the server certificate.
- The user selects a certificate in the browser that is not generated by a certificate authority in the certificate chain on the device.

To verify client browser certificates, configure the system to use the online certificate status protocol (OCSP) or load one or more certificate revocation lists (CRLs). Using the OCSP, when the web server receives a connection request it communicates with the certificate authority to confirm the client certificate's validity before establishing the connection. If you configure the server to load one or more CRLs, the web server compares the client certificate against those listed in the CRLs. If a user selects a certificate that is listed in a CRL as a revoked certificate, the browser cannot load the web interface.



Note If you choose to verify certificates using CRLs, the system uses the same CRLs to validate both client browser certificates and audit log server certificates.

Viewing the Current HTTPS Server Certificate

You can only view server certificates for the appliance you are logged in to.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **HTTPS Certificate**.

Generating an HTTPS Server Certificate Signing Request

If you install a certificate that is not signed by a globally known or internally trusted CA, the user's browser displays a security warning when they try to connect to the web interface.

A certificate signing request (CSR) is unique to the appliance or device from which you generated it. You cannot generate a CSR for multiple devices from a single appliance. Although all fields are optional, we recommend entering values for the following: CN, Organization, Organization Unit, City/Locality, State/Province, Country/Region.

The key generated for the certificate request is in Base-64 encoded PEM format.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **HTTPS Certificate**.

Step 3 Click **Generate New CSR**.

Step 4 Enter a country code in the **Country Name (two-letter code)** field.

Step 5 Enter a state or province postal abbreviation in the **State or Province** field.

Step 6 Enter a **Locality or City**.

Step 7 Enter an **Organization** name.

Step 8 Enter an **Organizational Unit (Department)** name.

Step 9 Enter the fully qualified domain name of the server for which you want to request a certificate in the **Common Name** field.

Note Enter the fully qualified domain name of the server exactly as it should appear in the certificate in the **Common Name** field. If the common name and the DNS hostname do not match, you receive a warning when connecting to the appliance.

Step 10 Click **Generate**.

Step 11 Open a text editor.

Step 12 Copy the entire block of text in the certificate request, including the `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST` lines, and paste it into a blank text file.

Step 13 Save the file as *`servername`*`.csr`, where *servername* is the name of the server where you plan to use the certificate.

Step 14 Click **Close**.

What to do next

- Submit the certificate request to the certificate authority.
- When you receive the signed certificate, import it to the Firepower Management Center; see Importing HTTPS Server Certificates, on page 9.

Importing HTTPS Server Certificates

If the signing authority that generated the certificate requires you to trust an intermediate CA, you must also supply a certificate chain (or certificate path).

If you require client certificates, accessing an appliance via the web interface will fail when the server certificate does not meet either of the following criteria:

- The certificate is signed by the same CA that signed the client certificate.
- The certificate is signed by a CA that has signed an intermediate certificate in the certificate chain.

Caution The Firepower Management Center supports 2048-bit HTTPS certificates. If the certificate used by the Firepower Management Center was generated using a public server key larger than 2048 bits, you will not be able to log in to the FMC web interface. For more information about updating HTTPS Certificates to Version 6.0.0, see "Update Management Center HTTPS Certificates to Version 6.0" in *Firepower System Release Notes, Version 6.0*. If you generate or import an HTTPS Certificate and cannot log in to the FMC web interface, contact Support.

Before you begin

- Generate a certificate signing request; see Generating an HTTPS Server Certificate Signing Request, on page 8.
- Upload the CSR file to the certificate authority where you want to request a certificate, or use the CSR to create a self-signed certificate.
- Confirm that the certificate meets the requirements described in HTTPS Server Certificate Requirements, on page 6.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **HTTPS Certificate**.

Step 3 Click **Import HTTPS Server Certificate**.

Note You cannot import an encrypted HTTPS certificate.

Step 4 Open the server certificate in a text editor, copy the entire block of text, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. Paste this text into the **Server Certificate** field.

Step 5 Whether you must supply a **Private Key** depends on how you generated the Certificate Signing Request:

- If you generated the Certificate Signing Request using the Firepower Management Center web interface (as described in Generating an HTTPS Server Certificate Signing Request, on page 8), the system already has the private key and you need not enter one here.
- If you generated the Certificate Signing Request using some other means, you must supply the private key here. Open the private key file and copy the entire block of text, include the `BEGIN RSA PRIVATE KEY` and `END RSA PRIVATE KEY` lines. Paste this text into the **Private Key** field.

Step 6 Open any required intermediate certificates, copy the entire block of text for each, and paste it into the **Certificate Chain** field. If you received a root certificate, paste it here. If you received an intermediate certificate, paste it below the root certificate. In both cases, copy the entire block of text, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines.

Step 7 Click **Save**.

Requiring Valid HTTPS Client Certificates

Use this procedure to require users connecting to the FMC web interface to supply a user certificate. The system supports validating HTTPS client certificates using either OCSP or imported CRLs in Privacy-enhanced Electronic Mail (PEM) format.

If you choose to use CRLs, to ensure that the list of revoked certificates stays current, you can create a scheduled task to update the CRLs. The system displays the most recent refresh of the CRLs.

Note To access the web interface after enabling client certificates, you **must** have a valid client certificate present in your browser (or a CAC inserted in your reader).

Before you begin

- Import a server certificate signed by the same certificate authority that signed the client certificate to be used for the connection; see Importing HTTPS Server Certificates, on page 9.
- Import the server certificate chain if needed; see Importing HTTPS Server Certificates, on page 9.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **HTTPS Certificate**.

Step 3 Choose **Enable Client Certificates**. If prompted, select the appropriate certificate from the drop-down list.

Step 4 You have three options:

- To verify client certificates using one or more CRLS, select **Enable Fetching of CRL** and continue with Step 5.
- To verify client certificates using OCSP, select **Enable OCSP** and skip to Step 7.

- To accept client certificates without checking for revocation, skip to Step 8.

Step 5 Enter a valid URL to an existing CRL file and click **Add CRL**. Repeat to add up to 25 CRLs.

Step 6 Click **Refresh CRL** to load the current CRL or CRLs from the specified URL or URLs.

Note Enabling fetching of the CRL creates a scheduled task to regularly update the CRL or CRLs. Edit the task to set the frequency of the update.

Step 7 Verify that the client certificate is signed by the certificate authority loaded onto the appliance and the server certificate is signed by a certificate authority loaded in the browser certificate store. (These should be the same certificate authority.)

Caution Saving a configuration with enabled client certificates, with no valid client certificate in your browser certificate store, disables all web server access to the appliance. Make sure that you have a valid client certificate installed before saving settings.

Step 8 Click **Save**.

Related Topics

Configuring Certificate Revocation List Downloads

External Database Access Settings

You can configure the Firepower Management Center to allow read-only access to its database by a third-party client. This allows you to query the database using SQL using any of the following:

- industry-standard reporting tools such as Actuate BIRT, JasperSoft iReport, or Crystal Reports
- any other reporting application (including a custom application) that supports JDBC SSL connections
- the Cisco-provided command-line Java application called RunQuery, which you can either run interactively or use to obtain comma-separated results for a single query

Use the Firepower Management Center's system configuration to enable database access and create an access list that allows selected hosts to query the database. Note that this access list does not also control appliance access.

You can also download a package that contains the following:

- RunQuery, the Cisco-provided database query tool
- InstallCert, a tool you can use to retrieve and accept the SSL certificate from the Firepower Management Center you want to access
- the JDBC driver you must use to connect to the database

See the *Firepower System Database Access Guide* for information on using the tools in the package you downloaded to configure database access.

Enabling External Access to the Database

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **External Database Access**.

Step 3 Select the **Allow External Database Access** check box.

Step 4 Enter an appropriate value in the **Server Hostname** field. Depending on your third-party application requirements, this value can be either the fully qualified domain name (FQDN), IPv4 address, or IPv6 address of the Firepower Management Center.

Note In an FMC high availability setup, enter only the active peer details. We do not recommend entering details of the standby peer.

Step 5 Next to **Client JDBC Driver**, click **Download** and follow your browser's prompts to download the `client.zip` package.

Step 6 To add database access for one or more IP addresses, click **Add Hosts**. An **IP Address** field appears in the **Access List** field.

Step 7 In the **IP Address** field, enter an IP address or address range, or `any`.

Step 8 Click **Add**.

Step 9 Click **Save**.

Tip If you want to revert to the last saved database settings, click **Refresh**.

Related Topics

Firepower System IP Address Conventions

Database Event Limits

To manage disk space, the FMC periodically prunes the oldest intrusion events, audit records, Security Intelligence data, and URL filtering data from the event database. For each event type, you can specify how many records the FMC retains after pruning; never rely on the event database containing more records of any type than the retention limit configured for that type. To improve performance, tailor the event limits to the number of events you regularly work with. You can optionally choose to receive email notifications when pruning occurs. For some event types, you can disable storage.

To manually delete individual events, use the event viewer. You can also manually purge the database; see Data Storage.

Configuring Database Event Limits

Before you begin

- If you want to receive email notifications when events are pruned from the Firepower Management Center's database, you must configure an email server; see Configuring a Mail Relay Host and Notification Address, on page 39.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Choose **Database**.

Step 3 For each of the databases, enter the number of records you want to store.

For information on how many records each database can maintain, see Database Event Limits, on page 13.

Step 4 Optionally, in the **Data Pruning Notification Address** field, enter the email address where you want to receive pruning notifications.

Step 5 Click **Save**.

Database Event Limits

The following table lists the minimum and maximum number of records for each event type that you can store on a Firepower Management Center.

Table 2: Database Event Limits

Event Type	Upper Limit	Lower Limit
Intrusion events	10 million (FMC Virtual) 20 million (FMC750) 30 million (FMC1500,) 60 million (FMC2000,) 150 million (FMC3500) 300 million (FMC4000,)	10,000
Discovery events	10 million (FMC Virtual) 20 million (FMC2000, FMC4000,)	Zero (disables storage)

Event Type	Upper Limit	Lower Limit
Connection events Security Intelligence events	50 million (FMC Virtual, FMC750) 100 million (FMC1500,) 300 million (FMC2000,) 500 million (FMC3500) 1 billion (FMC4000,) Limit is shared between connection events and Security Intelligence events. The sum of the configured maximums cannot exceed this limit.	Zero (disables storage) Setting **Maximum Connection Events** to zero immediately purges existing connection events. Note that disabling connection event storage on the Firepower Management Center does not affect connection summaries or correlation. The system still uses connection event information for features like traffic profiles, correlation policies, and dashboard displays.
Connection summaries (aggregated connection events)	50 million (FMC Virtual, FMC750) 100 million (FMC1500,) 300 million (FMC2000,) 500 million (FMC3500) 1 billion (FMC4000,)	Zero (disables storage)
Correlation events and compliance white list events	1 million (FMC Virtual) 2 million (FMC2000, , FMC4000)	One
Malware events	10 million (FMC Virtual) 20 million (FMC2000,, FMC4000)	10,000
File events	10 million (FMC Virtual) 20 million (FMC2000, , FMC4000)	Zero (disables storage)
Health events	1 million	Zero (disables storage)
Audit records	100,000	One
Remediation status events	10 million	One
White list violation history	a 30-day history of violations	One day’s history
User activity (user events)	10 million	One
User logins (user history)	10 million	One
Intrusion rule update import log records	1 million	One

Management Interfaces

After setup, you can change the management network settings, including adding more management interfaces, hostname, search domains, DNS servers, and HTTP proxy on the FMC.

About FMC Management Interfaces

By default, the FMC manages all devices on a single management interface. You can also perform initial setup on the management interface and log into the FMC on this interface as an administrator. The management interface is also used to communicate with the Smart Licensing server, to download updates, and to perform other management functions.

For information about device management interfaces, see About Device Management Interfaces.

Management Interfaces on the FMC

The FMC uses the eth0 interface for initial setup, HTTP access for administrators, management of devices, as well as other management functions such as licensing and updates.

You can also configure additional management interfaces on the same network, or on different networks. When the FMC manages large numbers of devices, adding more management interfaces can improve throughput and performance. You can also use these interfaces for all other management functions. You might want to use each management interface for particular functions; for example, you might want to use one interface for HTTP administrator access and another for device management.

For device management, the management interface carries two separate traffic channels: the *management traffic channel* carries all internal traffic (such as inter-device traffic specific to managing the device), and the *event traffic channel* carries all event traffic (such as web events). You can optionally configure a separate event-only interface on the FMC to handle event traffic; you can configure only one event interface. Event traffic can use a large amount of bandwidth, so separating event traffic from management traffic can improve the performance of the FMC. For example, you can assign a 10 GigabitEthernet interface to be the event interface, if available, while using 1 GigabitEthernet interfaces for management. You might want to configure an event-only interface on a completely secure, private network while using the regular management interface on a network that includes Internet access, for example. You can also use both management and event interfaces on the same network if the goal is only to take advantage of increased throughput. Managed devices will send management traffic to the FMC management interface and event traffic to the FMCs event-only interface. If the managed device cannot reach the event-only interface, then it will fall back to sending events to the management interface.

Note All management interfaces support HTTP administrator access as controlled by your Access List configuration. Conversely, you cannot restrict an interface to *only* HTTP access; management interfaces always support device management (management traffic, event traffic, or both).

Note Only the eth0 interface supports DHCP IP addressing. Other management interfaces only support static IP addresses.

Management Interface Support Per FMC Model

See the hardware installation guide for your model for the management interface locations.

See the following table for supported management interfaces on each FMC model.

Table 3: Management Interface Support on the FMC

Model	Management Interfaces
MC750, MC1500, MC3500	eth0 (Default) eth1
MC2000, MC4000	eth0 (Default) eth1 eth2 eth3
Firepower Management Center Virtual	eth0 (Default)

Network Routes on FMC Management Interfaces

Management interfaces (including event-only interfaces) support only static routes to reach remote networks. When you set up your FMC, the setup process creates a default route to the gateway IP address that you specify. You cannot delete this route; you can only modify the gateway address.

The default route always uses the lowest-numbered management interface (e.g. eth0).

At least one static route is recommended per management interface to access remote networks. We recommend placing each interface on a separate network to avoid potential routing problems, including routing problems from other devices to the FMC. If you do not experience problems with interfaces on the same network, then be sure to configure static routes correctly. For example, on the FMC both eth0 and eth1 are on the same network, but you want to manage a different group of devices on each interface. The default gateway is 192.168.45.1. If you want eth1 to manage devices on the remote 10.6.6.0/24 destination network, you can create a static route for 10.6.6.0/24 through eth1 with the same gateway of 192.168.45.1. Traffic to 10.6.6.0/24 will hit this route before it hits the default route, so eth1 will be used as expected.

If you want to use two FMC interfaces to manage remote devices that are on the same network, then static routing on the FMC may not scale well, because you need separate static routes per device IP address.

Another example includes separate management and event-only interfaces on both the FMC and the managed device. The event-only interfaces are on a separate network from the management interfaces. In this case, add a static route through the event-only interface for traffic destined for the remote event-only network, and vice versa.

NAT Environments

Network address translation (NAT) is a method of transmitting and receiving network traffic through a router that involves reassigning the source or destination IP address. The most common use for NAT is to allow private networks to communicate with the internet. Static NAT performs a 1:1 translation, which does not pose a problem for FMC communication with devices, but port address translation (PAT) is more common. PAT lets you use a single public IP address and unique ports to access the public network; these ports are dynamically assigned as needed, so you cannot initiate a connection to a device behind a PAT router.

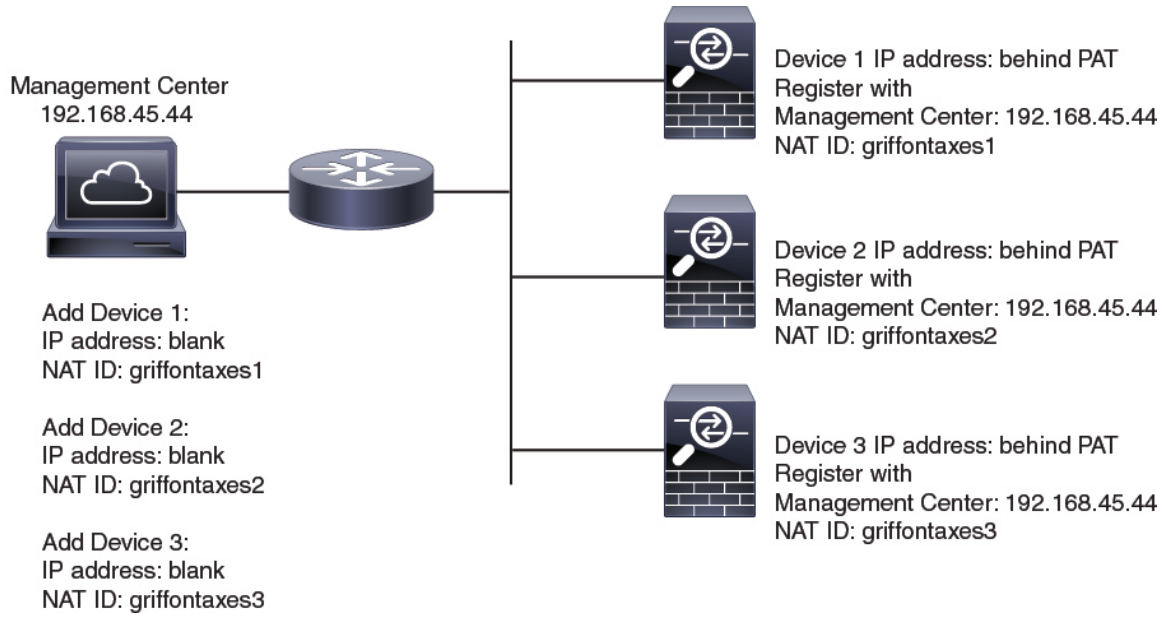
Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address when you add a device, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

For example, you add a device to the FMC, and you do not know the device IP address (for example, the device is behind a PAT router), so you specify only the NAT ID and the registration key on the FMC; leave the IP address blank. On the device, you specify the FMC IP address, the same NAT ID, and the same registration key. The device registers to the FMC's IP address. At this point, the FMC uses the NAT ID instead of IP address to authenticate the device.

Although the use of a NAT ID is most common for NAT environments, you might choose to use the NAT ID to simplify adding many devices to the FMC. On the FMC, specify a unique NAT ID for each device you want to add while leaving the IP address blank, and then on each device, specify both the FMC IP address and the NAT ID. Note: The NAT ID must be unique per device.

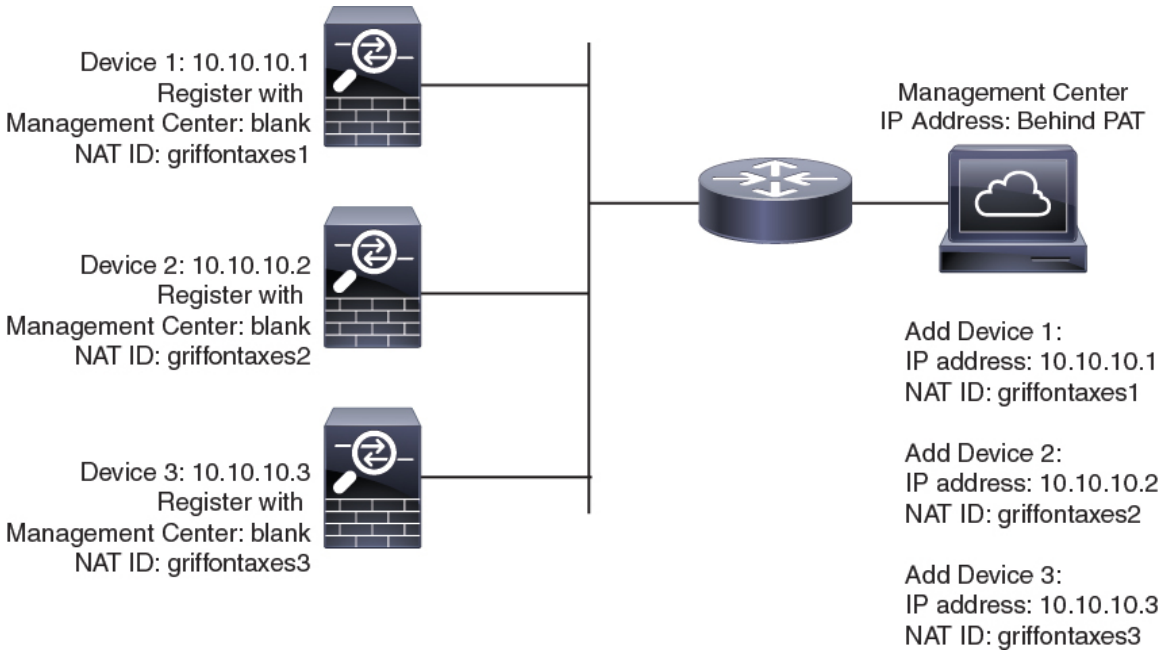
The following example shows three devices behind a PAT IP address. In this case, specify a unique NAT ID per device on both the FMC and the devices, and specify the FMC IP address on the devices.

Figure 1: NAT ID for Managed Devices Behind PAT



The following example shows the FMC behind a PAT IP address. In this case, specify a unique NAT ID per device on both the FMC and the devices, and specify the device IP addresses on the FMC.

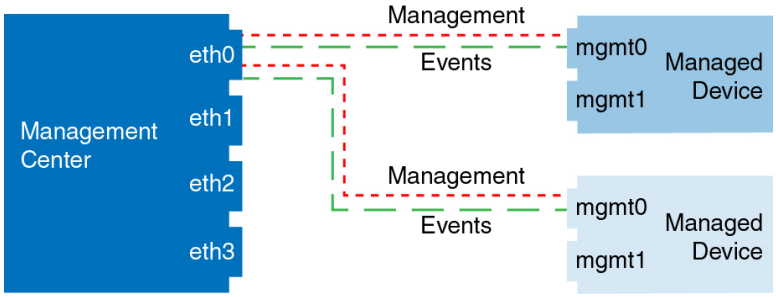
Figure 2: NAT ID for FMC Behind PAT



Management and Event Traffic Channel Examples

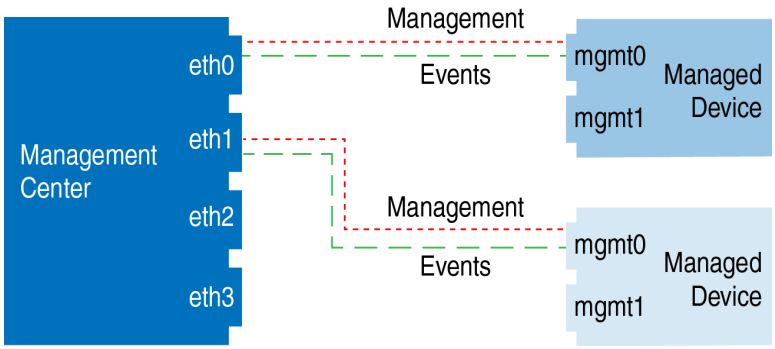
The following example shows the Firepower Management Center and managed devices using only the default management interfaces.

Figure 3: Single Management Interface on the Firepower Management Center



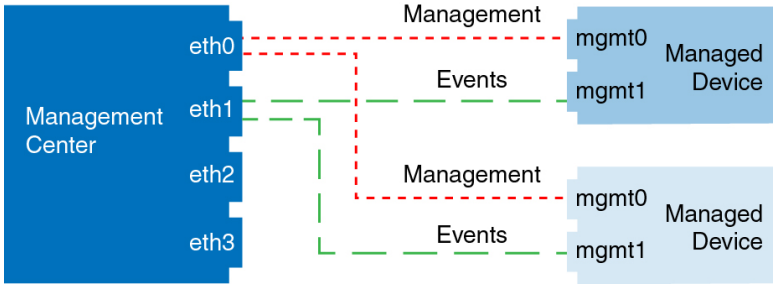
The following example shows the Firepower Management Center using separate management interfaces for devices; and each managed device using 1 management interface.

Figure 4: Mutliple Management Interfaces on the Firepower Management Center



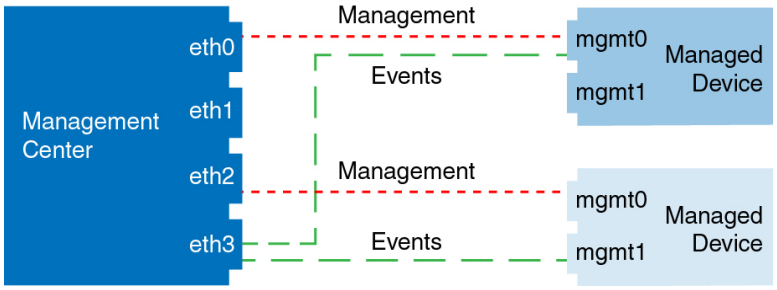
The following example shows the Firepower Management Center and managed devices using a separate event interface.

Figure 5: Separate Event Interface on the Firepower Management Center and Managed Devices



The following example shows a mix of multiple management interfaces and a separate event interface on the Firepower Management Center and a mix of managed devices using a separate event interface, or using a single management interface.

Figure 6: Mixed Management and Event Interface Usage



Modify FMC Management Interfaces

Caution Do NOT push the FMC deployments over a VPN tunnel that is terminating directly on the Firepower Threat Defense. Pushing the FMC deployments can potentially inactivate the tunnel and disconnect the FMC and the Firepower Threat Defense.

Recovering the device from this situation can be very disruptive and require executing the disaster recovery procedure. This procedure resets the Firepower Threat Defense configuration to factory defaults by changing manager from FMC to local and configuring the device from beginning. For more information, see Deploying the FMC Policy Configuration over VPN Tunnel.

Modify the management interface settings on the Firepower Management Center. You can optionally enable additional management interfaces or configure an event-only interface.

Caution Be careful when making changes to the management interface to which you are connected; if you cannot re-connect because of a configuration error, you need to access the FMC console port to re-configure the network settings in the Linux shell. You must contact Cisco TAC to guide you in this operation.

Note If you change the FMC IP address, then see the following tasks to ensure device management connectivity depending on how you added the device to the FMC:

- **IP address—No action.** If you added the device to the FMC using a reachable device IP address, then the management connection will be reestablished automatically after several minutes even though the IP address identified on the FTD is the old IP address. **Note**: If you specified a device IP address that is unreachable, then you must contact Cisco TAC, who can advise you how to restore connectivity for your devices.
- **NAT ID only—Contact Cisco TAC.** If you added the device using only the NAT ID, then the connection cannot be reestablished. In this case, you must contact Cisco TAC, who can advise you how to restore connectivity for your devices.

Before you begin

- For information about how device management works, see About Device Management Interfaces.
- If you use a proxy:
  - Proxies that use NT LAN Manager (NTLM) authentication are not supported.
  - If you use or will use Smart Licensing, the proxy FQDN cannot have more than 64 characters.

Procedure

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**—Configure an event-only interface; you can configure only one event interface on the FMC. To do so, uncheck the **Management Traffic** check box, and leave the **Event Traffic** check box checked. You can optionally disable **Event Traffic** for the management interface(s). In either case, the device will try to send events to 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.
- **MDI/MDIX**—Set the **Auto-MDIX** setting.
- **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.
- **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.

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

View the route table by clicking .

You need a static route for each additional interface to reach remote networks. For more information about when new routes are needed, see Network Routes on FMC Management Interfaces, on page 16.

Note For the default route, you can change only the gateway IP address. The default route always uses the eth0 interface.

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 FMC hostname. The hostname must start and end with a letter or digit, and have only letters, digits, or a hyphen. If you change the hostname, reboot the FMC 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 FMC, 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 managed devices. 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 **Proxy** area, configure HTTP proxy settings.

The FMC 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.

See proxy requirements in the prerequisites to this topic.

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.

   See requirements in the prerequisites to this topic.

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 6 Click **Save**.

Step 7 If you change the FMC IP address, then see If you change the FMC IP address, then see the following tasks to ensure device management connectivity depending on how you added the device to the FMC:

- **IP address—No action.** If you added the device to the FMC using a reachable device IP address, then the management connection will be reestablished automatically after several minutes even though the IP address identified on the FTD is the old IP address. **Note**: If you specified a device IP address that is unreachable, then you must contact Cisco TAC, who can advise you how to restore connectivity for your devices.
- **NAT ID only—Contact Cisco TAC.** If you added the device using only the NAT ID, then the connection cannot be reestablished. In this case, you must contact Cisco TAC, who can advise you how to restore connectivity for your devices.

Shut Down or Restart

Use the web interface to control the shut down and restart of processes on the FMC. You can:

- Shut down: Initiate a graceful shutdown of the 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: Shut down and restart gracefully.
- Restart the console: Restart the communications, database, and HTTP server processes. This is typically used during troubleshooting.

Tip For information on shutting down/restarting a 7000/8000 series device, including restarting the Snort process, see Shut Down or Restart a 7000/8000 Series Device. For virtual devices, refer to the documentation for your virtual platform. For VMware in particular, custom power options are part of VMware Tools.

Shut Down or Restart the FMC

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Choose **Process**.

Step 3 Do one of the following:

Shut down	Click **Run Command** next to **Shutdown Management Center**.

Reboot	Click **Run Command** next to **Reboot Management Center**. **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 Management Center Console**. **Note** Restarting may cause deleted hosts to reappear in the network map.

Related Topics

Snort® Restart Scenarios

Remote Storage Management

On Firepower Management Centers, you can use the following for local or remote storage for backups and reports:

- Network File System (NFS)
- Server Message Block (SMB)/Common Internet File System (CIFS)
- Secure Shell (SSH)

You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center.

Tip After configuring and selecting remote storage, you can switch back to local storage **only** if you **have not** increased the connection database limit.

Configuring Local Storage

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Choose **Remote Storage Device**.

Step 3 Choose **Local (No Remote Storage)** from the **Storage Type** drop-down list.

Step 4 Click **Save**.

Configuring NFS for Remote Storage

Before you begin

- Ensure that your external remote storage system is functional and accessible from your FMC.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Remote Storage Device**.

Step 3 Choose **NFS** from the **Storage Type** drop-down list.

Step 4 Add the connection information:

- Enter the IPv4 address or hostname of the storage system in the **Host** field.
- Enter the path to your storage area in the **Directory** field.

Step 5 Optionally, check the **Use Advanced Options** check box and enter any required command line options; see Remote Storage Management Advanced Options, on page 27.

Step 6 Under **System Usage**:

- Choose **Use for Backups** to store backups on the designated host.
- Choose **Use for Reports** to store reports on the designated host.
- Enter **Disk Space Threshold** for backup to remote storage. Default is 90%.

Step 7 To test the settings, click **Test**.

Step 8 Click **Save**.

Configuring SMB for Remote Storage

Before you begin

Ensure that your external remote storage system is functional and accessible from your FMC:

- The system recognizes top-level SMB shares, not full file paths. You must use Windows to share the exact directory you want to use.
- Make sure the Windows user you will use to access the SMB share from the FMC has ownership of and read/change access to the share location.
- To ensure security, you should install SMB 2.0 or greater.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Remote Storage Device**.

Step 3 Choose **SMB** from the **Storage Type** drop-down list.

Step 4 Add the connection information:

- Enter the IPv4 address or hostname of the storage system in the **Host** field.
- Enter the share of your storage area in the **Share** field.

- Optionally, enter the domain name for the remote storage system in the **Domain** field.
- Enter the user name for the storage system in the **Username** field and the password for that user in the **Password** field.

Step 5 Optionally, check the **Use Advanced Options** check box and enter any required command line options; see Remote Storage Management Advanced Options, on page 27.

Step 6 Under **System Usage**:

- Choose **Use for Backups** to store backups on the designated host.
- Choose **Use for Reports** to store reports on the designated host.

Step 7 To test the settings, click **Test**.

Step 8 Click **Save**.

Configuring SSH for Remote Storage

Before you begin

- Ensure that your external remote storage system is functional and accessible from your Firepower Management Center.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Remote Storage Device**.

Step 3 Choose **SSH** from the **Storage Type** drop-down list.

Step 4 Add the connection information:

- Enter the IP address or host name of the storage system in the **Host** field.
- Enter the path to your storage area in the **Directory** field.
- Enter the storage system's user name in the **Username** field and the password for that user in the **Password** field. To specify a network domain as part of the connection user name, precede the user name with the domain followed by a forward slash (/).
- To use SSH keys, copy the content of the **SSH Public Key** field and place it in your authorized_keys file.

Step 5 Optionally, check the **Use Advanced Options** check box and enter any required command line options; see Remote Storage Management Advanced Options, on page 27.

Step 6 Under System Usage:

- Choose **Use for Backups** to store backups on the designated host.
- Choose **Use for Reports** to store reports on the designated host.

Step 7 If you want to test the settings, you must click **Test**.

Step 8 Click **Save**.

Remote Storage Management Advanced Options

If you select the Network File System (NFS) protocol, Server Message Block (SMB) protocol, or `SSH` to use secure file transfer protocol (SFTP) to store your reports and backups, you can select the **Use Advanced Options** check box to use one of the mount binary options as documented in an NFS, SMB, or SSH mount main page.

If you select SMB or NFS storage type, you can specify the version number of the remote storage in the **Command Line Option** field using the following format:

`vers=`*`version`*

where `version` is the version number of SMB or NFS remote storage you want to use. For example, to select NFSv4, enter `vers=4.0`.

If SMB encryption is enabled for a file server, only SMB version 3.0 clients are allowed to access the file server. To access encrypted SMB file server from the FMC, type the following in the **Command Line Option** field:

`vers=`*`3.0`*

where you select encrypted SMBv3 to copy or save backup files from the FMC to the encrypted SMB file server.

Change Reconciliation

To monitor the changes that users make and ensure that they follow your organization's preferred standard, you can configure the system to send, via email, a detailed report of changes made over the past 24 hours. Whenever a user saves changes to the system configuration, a snapshot is taken of the changes. The change reconciliation report combines information from these snapshots to present a clear summary of recent system changes.

The following sample graphic displays a User section of an example change reconciliation report and lists both the previous value for each configuration and the value after changes. When users make multiple changes to the same configuration, the report lists summaries of each distinct change in chronological order, beginning with the most recent.

You can view changes made during the previous 24 hours.

Configuring Change Reconciliation

Before you begin

- Configure an email server to receive emailed reports of changes made to the system over a 24 hour period; see Configuring a Mail Relay Host and Notification Address, on page 39 for more information.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Change Reconciliation**.

Step 3 Check the **Enable** check box.

Step 4 Choose the time of day you want the system to send out the change reconciliation report from the **Time to Run** drop-down lists.

Step 5 Enter email addresses in the **Email to** field.

Tip Once you have added email addresses, click **Resend Last Report** to send recipients another copy of the most recent change reconciliation report.

Step 6 If you want to include policy changes, check the **Include Policy Configuration** check box.

Step 7 If you want to include all changes over the past 24 hours, check the **Show Full Change History** check box.

Step 8 Click **Save**.

Related Topics

Using the Audit Log to Examine Changes

Change Reconciliation Options

The **Include Policy Configuration** option controls whether the system includes records of policy changes in the change reconciliation report. This includes changes to access control, intrusion, system, health, and network discovery policies. If you do not select this option, the report will not show changes to any policies. This option is available on Firepower Management Centers only.

The **Show Full Change History** option controls whether the system includes records of all changes over the past 24 hours in the change reconciliation report. If you do not select this option, the report includes only a consolidated view of changes for each category.

Note The change reconciliation report does not include changes to Firepower Threat Defense interfaces and routing settings.

Policy Change Comments

You can configure the Firepower System to track several policy-related changes using the comment functionality when users modify access control, intrusion, or network analysis policies.

With policy change comments enabled, administrators can quickly assess why critical policies in a deployment were modified. Optionally, you can have changes to intrusion and network analysis policies written to the audit log.

Configuring Comments to Track Policy Changes

You can configure the Firepower System to prompt users for comments when they modify an access control policy, intrusion policy, or network analysis policy. You can use comments to track users' reasons for policy changes. If you enable comments on policy changes, you can make the comment optional or mandatory. The system prompts the user for a comment when each new change to a policy is saved.

Procedure

Step 1 Choose **System** > **Configuration**.

The system configuration options appear in the left navigation panel.

Step 2 Configure the policy comment preferences for any of the following:

- Click **Access Control Preferences** for comment preferences for access control policies.
- Click **Intrusion Policy Preferences** for comment preferences for intrusion policies.
- Click **Network Analysis Policy Preferences** for comment preferences for network analysis policies.

Step 3 You have the following choices for each policy type:

- **Disabled**—Disables change comments.
- **Optional**—Gives users the option to describe their changes in a comment.
- **Required**—Requires users to describe their changes in a comment before saving.

Step 4 Optionally for intrusion or network analysis policy comments:

- Check **Write changes in Intrusion Policy to audit log** to write all intrusion policy changes to the audit log.
- Check **Write changes in Network Analysis Policy to audit log** to write all network analysis policy changes to the audit log.

Step 5 Click **Save**.

Access List

You can limit access to the FMC by IP address and port. By default, the following ports are enabled for any IP address:

- 443 (HTTPS) for web interface access.
- 22 (SSH) for CLI access.

You can also add access to poll for SNMP information over port 161. Because SNMP is disabled by default, you must first enable SNMP before you can add SNMP access rules. For more information, see Configure SNMP Polling, on page 42.



Caution By default, access is not restricted. To operate in a more secure environment, consider adding access for specific IP addresses and then deleting the default **any** option.

Configure an Access List

This access list does not control external database access. See Enabling External Access to the Database, on page 12.

Caution If you delete access for the IP address that you are currently using to connect to the FMC, and there is no entry for "`IP=any port=443`", you will lose access when you save.

To configure access lists for Classic devices, use device platform settings. See Configure Access Lists for Classic Devices.

Before you begin

By default, the access list includes rules for HTTPS and SSH. To add SNMP rules to the access list, you must first enable SNMP. For more information, see Configure SNMP Polling, on page 42.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 (Optional) Click **SNMP** to configure SNMP if you want to add SNMP rules to the access list. By default, SNMP is disabled; see Configure SNMP Polling, on page 42.

Step 3 Click **Access List**.

Step 4 To add access for one or more IP addresses, click **Add Rules**.

Step 5 In the **IP Address** field, enter an IP address or address range, or `any`.

Step 6 Choose **SSH**, **HTTPS**, **SNMP**, or a combination of these options to specify which ports you want to enable for these IP addresses.

Step 7 Click **Add**.

Step 8 Click **Save**.

Related Topics

Firepower System IP Address Conventions

Audit Logs

The Firepower Management Center records user activity in read-only audit logs. You can review audit log data in several ways:

- Use the web interface: Auditing the System.

  Audit logs are presented in a standard event view where you can view, sort, and filter audit log messages based on any item in the audit view. You can easily delete and report on audit information and you can view detailed reports of the changes that users make.

- Stream audit log messages to the syslog: Stream Audit Logs to Syslog, on page 31..

- Stream audit log messages to an HTTP server: Stream Audit Logs to an HTTP Server, on page 32.

Streaming audit log data to an external server allows you to conserve space on the FMC. Note that sending audit information to an external URL may affect system performance.

Optionally, you can secure the channel for audit log streaming, enable TLS and mutual authentication using TLS certificates; see Audit Log Certificate, on page 33.

Classic devices also maintain audit logs. To stream audit logs from a Classic devices, see Stream Audit Logs from Classic Devices.

Stream Audit Logs to Syslog

When this feature is enabled, audit log records appear in the syslog in the following format :

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

Where the local date, time, and originating hostname precede the bracketed optional tag, and the sending device name precedes the audit log message.

For example, if you specify a tag of `FMC-AUDIT-LOG` for audit log messages from your management center, a sample audit log message from your FMC could appear as follows:

```
Mar 01 14:45:24 localhost [FMC-AUDIT-LOG] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

If you specify a severity and facility, these values do not appear in syslog messages; instead, they tell the system that receives the syslog messages how to categorize them.

To stream audit logs from Classic devices, use device platform settings: Stream Audit Logs from Classic Devices.

Before you begin

Make sure the FMC can communicate with the syslog server. When you save your configuration, the system uses ICMP/ARP and TCP SYN packets to verify that the syslog server is reachable. Then, the system uses port 514/UDP to stream audit logs. If you secure the channel (optional, see Audit Log Certificate, on page 33), you must manually configure port 1470 for TCP.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Audit Log**.

Step 3 Choose **Enabled** from the **Send Audit Log to Syslog** drop-down menu.

Step 4 The following fields are applicable only for audit logs sent to syslog:

Option	Description
Host	The IP address or the fully qualified name of the syslog server to which you will send audit logs.
Facility	The subsystem that creates the message. Choose a facility described in Syslog Alert Facilities. For example, choose AUDIT.

Option	Description
Severity	The severity of the message. Choose a severity described in Syslog Severity Levels.
Tag	An optional tag to include in audit log syslog messages. Best practice: Enter a value in this field to easily differentiate audit log messages from other, similar syslog messages such as health alerts. For example, if you want all audit log records sent to the syslog to be labeled with `FMC-AUDIT-LOG`, enter `FMC-AUDIT-LOG` in the field.

Step 5 (Optional) To test whether the IP address of the syslog server is valid, click **Test Syslog Server**.

The system sends the following packets to verify whether the syslog server is reachable:

a. ICMP echo request

b. TCP SYN on 443 and 80 ports

c. ICMP time stamp query

d. TCP SYN on random ports

Note If the FMC and syslog server are in the same subnet, ARP is used instead of ICMP.

The system displays the result for the server.

Step 6 Click **Save**.

Stream Audit Logs to an HTTP Server

When this feature is enabled, the appliance sends audit log records to an HTTP server in the following format:

```
Date Time Host [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

Where the local date, time, and originating hostname precede the bracketed optional tag, and the sending appliance or device name precedes the audit log message.

For example, if you specify a tag of `FROMMC`, a sample audit log message could appear as follows:

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

To stream audit logs from Classic devices, use device platform settings: Stream Audit Logs from Classic Devices.

Before you begin

Make sure the device can communicate with the HTTP server. Optionally, secure the channel; see Audit Log Certificate, on page 33.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Audit Log**.

Step 3 Optionally, in the **Tag** field, enter the tag name that you want to appear with the message. For example, if you want all audit log records to be preceded with `FROMMC`, enter `FROMMC` in the field.

Step 4 Choose **Enabled** from the **Send Audit Log to HTTP Server** drop-down list.

Step 5 In the **URL to Post Audit** field, designate the URL where you want to send the audit information. Enter a URL that corresponds to a Listener program that expects the HTTP POST variables as listed:

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- `result`
- `time`
- `tag` (if defined; see Step 3)

Caution To allow encrypted posts, use an HTTPS URL. Sending audit information to an external URL may affect system performance.

Step 6 Click **Save**.

Audit Log Certificate

You can use Transport Layer Security (TLS) certificates to secure communications between Firepower appliances and a trusted audit log server.

Client Certificates (Required)

For *each appliance* (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 appliance.

You cannot use the FMC to import audit log certificates onto its managed devices. These certificates are unique to each appliance, and you must log into *each appliance* to import them locally:

- For the FMC, use the local system configuration: Obtain a Signed Audit Log Client Certificate for the FMC, on page 35 and Import an Audit Log Client Certificate into the FMC, on page 36.
- For 7000/8000 series devices, use the local system configuration: Obtain a Signed Client Certificate for Secure Audit Log Streaming on a 7000/8000 Series Device.

- For ASA FirePOWER and NGIPSv, generate a CSR with a tool like OpenSSL, then use the CLI to import the signed certificate: **configure audit_cert import**.

Server Certificates (Optional)

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.

To require valid audit log server certificates, use the FMC web interface:

- For the FMC, use the local system configuration: Require Valid Audit Log Server Certificates, on page 36.
- For Classic devices (including 7000/8000 series), use device platform settings: Require Valid Audit Log Server Certificates for Classic Devices.

Securely Stream Audit Logs

If you stream the audit log to a trusted HTTP server or syslog server, you can use Transport Layer Security (TLS) certificates to secure the channel between the FMC and the server. You must generate a unique client certificate for each appliance you want to audit.

To securely stream audit logs to Classic devices, see Stream Audit Logs from Classic Devices.

Before you begin

See ramifications of requiring client and server certificates at Audit Log Certificate, on page 33.

Procedure

Step 1 Obtain and install a signed client certificate on the FMC:

a) Obtain a Signed Audit Log Client Certificate for the FMC, on page 35:

Generate a Certificate Signing Request (CSR) from the FMC based on your system information and the identification information you supply.

Submit the CSR to a recognized, trusted certificate authority (CA) to request a signed client certificate.

If you will require mutual authentication between the FMC and the audit log server, the client certificate must be signed by the same CA that signed the server certificate to be used for the connection.

b) After you receive the signed certificate from the certificate authority, import it into the FMC. See Import an Audit Log Client Certificate into the FMC, on page 36.

Step 2 Configure the communication channel with the server to use Transport Layer Security (TLS) and enable mutual authentication.

See Require Valid Audit Log Server Certificates, on page 36.

Step 3 Configure audit log streaming if you have not yet done so.

See Stream Audit Logs to Syslog, on page 31 or Stream Audit Logs to an HTTP Server, on page 32.

Obtain a Signed Audit Log Client Certificate for the FMC

To obtain a certificate for a managed Classic device, see Obtain a Signed Client Certificate for Secure Audit Log Streaming on a 7000/8000 Series Device.

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

Before you begin

Keep the following in mind:

- You must generate a certificate signing request (CSR) from the device or appliance on which you will install the certificate. (For example, you cannot generate a certificate signing request for Device B from Appliance A.) You must generate a unique certificate signing request from each device and appliance.
- To ensure security, use a globally recognized and trusted Certificate Authority (CA) to sign your certificate.
- If you will require mutual authentication between the appliance and the audit log server, the same Certificate Authority must sign both the client certificate and the server certificate.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Audit Log Certificate**.

Step 3 Click **Generate New CSR**.

Step 4 Enter a country code in the **Country Name (two-letter code)** field.

Step 5 Enter a state or province postal abbreviation in the **State or Province** field.

Step 6 Enter a **Locality or City**.

Step 7 Enter an **Organization** name.

Step 8 Enter an **Organizational Unit (Department)** name.

Step 9 Enter the fully qualified domain name of the server for which you want to request a certificate in the **Common Name** field.

Note If the common name and the DNS hostname do not match, audit log streaming will fail.

Step 10 Click **Generate**.

Step 11 Open a new blank file with a text editor.

Step 12 Copy the entire block of text in the certificate request, including the `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST` lines, and paste it into a blank text file.

Step 13 Save the file as *`clientname`*`.csr`, where *`clientname`* is the name of the appliance where you plan to use the certificate.

Step 14 Click **Close**.

What to do next

- Submit the certificate signing request to the certificate authority that you selected using the guidelines in the "Before You Begin" section of this procedure.
- When you receive the signed certificate, import it to the appliance; see Import an Audit Log Client Certificate into the FMC, on page 36.

Import an Audit Log Client Certificate into the FMC

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

Before you begin

- Obtain a Signed Audit Log Client Certificate for the FMC, on page 35.
- Make sure you are importing the signed certificate for the correct appliance. Each certificate is unique to a specific appliance or device.
- If the signing authority that generated the certificate requires you to trust an intermediate CA, be prepared to provide the necessary certificate chain (or certificate path). The CA that signed the client certificate must be the same CA that signed any intermediate certificates in the certificate chain.

Procedure

Step 1 On the FMC, choose **System** > **Configuration**.

Step 2 Click **Audit Log Certificate**.

Step 3 Click **Import Audit Client Certificate**.

Step 4 Open the client certificate in a text editor, copy the entire block of text, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. Paste this text into the **Client Certificate** field.

Step 5 To upload a private key, open the private key file and copy the entire block of text, including the `BEGIN RSA PRIVATE KEY` and `END RSA PRIVATE KEY` lines. Paste this text into the **Private Key** field.

Step 6 Open any required intermediate certificates, copy the entire block of text for each, and paste it into the **Certificate Chain** field.

Step 7 Click **Save**.

Require Valid Audit Log Server Certificates

The system supports validating audit log server certificates using imported CRLs in Distinguished Encoding Rules (DER) format.

Note If you choose to verify certificates using CRLs, the system uses the same CRLs to validate both audit log server certificates and certificates used to secure the HTTP connection between an appliance and a web browser.

Before you begin

- Understand the ramifications of requiring mutual authentication and of using certificate revocation lists (CRLs) to ensure that certificates are still valid. See Audit Log Certificate, on page 33.
- Obtain and import the client certificate following the steps in Securely Stream Audit Logs, on page 34 and the topics referenced in that procedure.

Procedure

Step 1 On the FMC, choose **System** > **Configuration**.

Step 2 Click **Audit Log Certificate**.

Step 3 To use Transport Layer Security to securely stream the audit log to an external server, choose **Enable TLS**.

Step 4 If you want to accept server certificates without verification (not recommended):

a) Deselect **Enable Mutual Authentication**.

b) Click **Save** and skip the remainder of this procedure.

Step 5 To verify the certificate of the audit log server, choose **Enable Mutual Authentication**.

Step 6 (If you enabled mutual authentication) To automatically recognize certificates that are no longer valid:

a) Select **Enable Fetching of CRL**.

Note Enabling fetching of the CRL creates a scheduled task to regularly update the CRL or CRLs.

b) Enter a valid URL to an existing CRL file and click **Add CRL**.

Repeat to add up to 25 CRLs.

c) Click **Refresh CRL** to load the current CRL or CRLs from the specified URL or URLs.

Step 7 Verify that you have a valid server certificate generated by the same certificate authority that created the client certificate.

Step 8 Click **Save**.

What to do next

(Optional) Set the frequency of CRL updates. See Configuring Certificate Revocation List Downloads.

View the Audit Log Client Certificate on the FMC

You can view the audit log client certificate only for the appliance that you are logged in to.

To view audit log certificates on Classic devices, use the system configuration on a 7000/8000 series device's web interface, or the CLI: **show audit_cert**.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Audit Log Certificate**.

Dashboard Settings

Dashboards provide you with at-a-glance views of current system status through the use of widgets: small, self-contained components that provide insight into different aspects of the Firepower System. The Firepower System is delivered with several predefined dashboard widgets.

You can configure the Firepower Management Center so that Custom Analysis widgets are enabled on the dashboard.

Related Topics

About Dashboards

Enabling Custom Analysis Widgets for Dashboards

Use Custom Analysis dashboard widgets to create a visual representation of events based on a flexible, user-configurable query.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Dashboard**.

Step 3 Check the **Enable Custom Analysis Widgets** check box to allow users to add Custom Analysis widgets to dashboards.

Step 4 Click **Save**.

DNS Cache

You can configure the system to resolve IP addresses automatically on the event view pages. You can also configure basic properties for DNS caching performed by the appliance. Configuring DNS caching allows you to identify IP addresses you previously resolved without performing additional lookups. This can reduce the amount of traffic on your network and speed the display of event pages when IP address resolution is enabled.

Configuring DNS Cache Properties

DNS resolution caching is a system-wide setting that allows the caching of previously resolved DNS lookups.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Choose **DNS Cache**.

Step 3 From the **DNS Resolution Caching** drop-down list, choose one of the following:

- **Enabled**—Enable caching.
- **Disabled**—Disable caching.

Step 4 In the **DNS Cache Timeout (in minutes)** field, enter the number of minutes a DNS entry remains cached in memory before it is removed for inactivity.

The default setting is 300 minutes (five hours).

Step 5 Click **Save**.

Related Topics

Configuring Event View Settings

Email Notifications

Configure a mail host if you plan to:

- Email event-based reports
- Email status reports for scheduled tasks
- Email change reconciliation reports
- Email data-pruning notifications
- Use email for discovery event, impact flag, correlation event alerting, intrusion event alerting, and health event alerting

When you configure email notification, you can select an encryption method for the communication between the system and mail relay host, and can supply authentication credentials for the mail server if needed. After configuring, you can test the connection.

Configuring a Mail Relay Host and Notification Address

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Email Notification**.

Step 3 In the **Mail Relay Host** field, enter the hostname or IP address of the mail server you want to use. The mail host you enter **must** allow access from the appliance.

Step 4 In the **Port Number** field, enter the port number to use on the email server.

Typical ports include:

- 25, when using no encryption
- 465, when using SSLv3
- 587, when using TLS

Step 5 Choose an **Encryption Method**:

- **TLS**—Encrypt communications using Transport Layer Security.
- **SSLv3**—Encrypt communications using Secure Socket Layers.
- **None**—Allow unencrypted communication.

Note Certificate validation is not required for encrypted communication between the appliance and mail server.

Step 6 In the **From Address** field, enter the valid email address you want to use as the source email address for messages sent by the appliance.

Step 7 Optionally, to supply a user name and password when connecting to the mail server, choose **Use Authentication**. Enter a user name in the **Username** field. Enter a password in the **Password** field.

Step 8 To send a test email using the configured mail server, click **Test Mail Server Settings**.

A message appears next to the button indicating the success or failure of the test.

Step 9 Click **Save**.

Language Selection

You can use the Language page to specify a different language for the web interface.

Set the Language for the Web Interface

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

- English
- Chinese (simplified)
- Japanese
- Korean

To set the language for 7000/8000 series devices, use device platform settings: Set the Language for the 7000/8000 Series Web Interface.

Procedure

Step 1 Choose **System** > **Configuration**.
Step 2 Click **Language**.
Step 3 Choose the language you want to use.
Step 4 Click **Save**.

Login Banners

You can use the Login Banner page to specify session, login, or custom message banners for a security appliance or shared policy.

You can use ASCII characters and carriage returns to create a custom login banner. The system does not preserve tab spacing. If your login banner is too large or causes errors, Telnet or SSH sessions can fail when the system attempts to display the banner.

Customize the Login Banner

To customize login banners for Classic devices, use device platform settings. See Customize the Login Banner for Classic Devices.

Procedure

Step 1 Choose **System** > **Configuration**.
Step 2 Choose **Login Banner**.
Step 3 In the **Custom Login Banner** field, enter the login banner text you want to use.
Step 4 Click **Save**.

SNMP Polling

You can enable Simple Network Management Protocol (SNMP) polling. This feature supports use of versions 1, 2, and 3 of the SNMP protocol. This feature allows access to the standard management information base (MIB), which includes system details such as contact, administrative, location, service information, IP addressing and routing information, and transmission protocol usage statistics.

Note When selecting SNMP versions for the SNMP protocol, note that SNMPv2 only supports read-only communities and SNMPv3 only supports read-only users. SNMPv3 also supports encryption with AES128.

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.

Configure SNMP Polling

To configure SNMP polling on Classic managed devices, use the device platform settings. See Configure SNMP Polling on Classic Devices.

Before you begin

Add SNMP access for each computer you plan to use to poll the system. See Configure an Access List, on page 30.



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 **System** > **Configuration**.

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**.

Security Certifications Compliance

Your organization might be required to use only equipment and software complying with security standards established by the U.S. Department of Defense and global certification organizations. The following security certifications standards are supported:

- Common Criteria (CC): a global standard established by the international Common Criteria Recognition Arrangement, defining properties for security products
- Unified Capabilities Approved Products List (UCAPL): a list of products meeting security requirements established by the U.S. Defense Information Systems Agency (DISA)



Note The U.S. Government has changed the name of the Unified Capabilities Approved Products List (UCAPL) to the Department of Defense Information Network Approved Products List (DODIN APL). References to UCAPL in this documentation and the FMC web interface can be interpreted as references to DODIN APL.

- Federal Information Processing Standards (FIPS) 140: a requirements specification for encryption modules

You can enable security certifications compliance in CC mode or UCAPL mode. Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. For more information on hardening procedures, refer to the guidelines for this product provided by the certifying entity.



Caution After you enable this setting, you cannot disable it. If you need to take an appliance out of CC or UCAPL mode, you must reimage.

Security Certifications Compliance Characteristics

The following table describes behavior changes when you enable CC or UCAPL mode. (Restrictions on login accounts refers to command line or shell access, not web interface access.)

System Change	CC Mode	UCAPL Mode
FIPS compliance is enabled.	Yes	Yes
The system does not allow remote storage for backups or reports.	Yes	Yes
The system starts an additional system audit daemon.	No	Yes
The system boot loader is secured.	No	Yes
The system applies additional security to login accounts.	No	Yes
The system disables the reboot key sequence Ctrl-Alt-Del.	No	Yes
The system enforces a maximum of ten simultaneous login sessions.	No	Yes

System Change	CC Mode	UCAPL Mode
The system automtically rekeys an SSH session with an appliance: • After a key has been in use for one hour of session activity • After a key has been used to transmit 1 GB of data over the connection This applies to Version 6.1.0.4 or a subsequent 6.1.0.x patch.	Yes	Yes
The system supports exporting event data using eStreamer only for Version 6.1.0.6 or subsequent 6.1.0.x patches.	Yes	Yes
The system applies more stringent safeguards for login accounts: • Passwords must be at least fifteen alphanumeric characters of mixed case and must include at least one numeric character. • Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters. • The system locks out a user after three failed login attempts in a row. In this case, the password must be reset by an administrator. • The system stores password history.	No	Yes

Security Certifications Compliance Recommendations

Cisco recommends that you observe the following best practices when using a system with security certifications compliance enabled:

- To enable security certifications compliance in your deployment, enable it first on the Firepower Management Center, then enable it in the same mode on all managed devices.



Caution The Firepower Management Center will not receive event data from a managed device unless both are operating in the same security certifications compliance mode.

- For all users, enable password strength checking and set the minimum password length to the value required by the certifying agency.
- If you are using Firepower Management Centers in a high-availability configuration, configure them both to use the same security certifications compliance mode.
- Do not configure the system to use any of the following features:
  - Email reports, alerts, or data pruning notifications.
  - Nmap Scan, Cisco IOS Null Route, Set Attribute Value, or ISE EPS remediations.
  - Remote storage for backups or reports.
  - Third-party client access to the system database.

- External notifications or alerts transmitted via email, SNMP trap, or syslog.
- Audit log messages transmitted to an HTTP server or to a syslog server without using SSL certificates to secure the channel between the appliance and the server.

- You may configure the system to export event data to an external client using eStreamer only for Version 6.1.0.6 and subsequent 6.1.0.x patches.
- Do not enable external authentication using LDAP or RADIUS in deployments using CC mode.
- Do not enable CACs in deployments using CC mode.
- Disable access to the Firepower Management Center and managed devices via the Firepower REST API in deployments using CC or UCAPL mode.
- Enable CACs in deployments using UCAPL mode.



Note The Firepower System does not support CC or UCAPL mode for classic devices in stacks or high availability pairs.

Enable Security Certifications Compliance

This configuration applies to either a Firepower Management Center or a Classic managed device:

- For the Firepower Management Center, this configuration is part of the system configuration.
- For a managed device, you apply this configuration from the FMC as part of a platform settings policy.

In either case, the configuration does not take effect until you save your system configuration changes or deploy the shared platform settings policy.



Caution After you enable this setting, you cannot disable it. If you need to take the appliance out of CC or UCAPL mode, you must reimage.

Before you begin

- We recommend you register all devices that you plan to be part of your deployment to the FMC before enabling security certifications compliance on any appliances.
- You must be an Admin user to perform this task.

Procedure

Step 1 Depending on whether you are configuring an FMC or a managed device:

- FMC: Choose **System** > **Configuration**.
- Classic device: Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **UCAPL/CC Compliance**.

Note Appliances reboot when you enable UCAPL or CC compliance. The FMC reboots when you save the system configuration; managed devices reboot when you deploy configuration changes.

Step 3 To *permanently* enable security certifications compliance on the appliance, you have two choices:

- To enable security certifications compliance in Common Criteria mode, choose **CC** from the drop-down list.
- To enable security certifications compliance in Unified Capabilities Approved Products List mode, choose **UCAPL** from the drop-down list.

Step 4 Click **Save**.

What to do next

- If you have not already, apply Control and Protection licenses to all Classic devices in your deployment.
- If your appliances were updated from versions earlier than Version 5.2.0, enabling security certifications compliance regenerates appliance certificates. After you enable security certifications compliance in the same mode across your deployment, reregister managed devices to the FMC.
- Deploy configuration changes; see Deploy Configuration Changes.

Time and Time Synchronization

Synchronizing the system time on your Firepower Management Center (FMC) and its managed devices is essential to successful operation of your Firepower System. We recommend that you specify NTP servers during FMC initial configuration, but you can use the information in this section to establish or change time sychronization settings after intial configuration is complete.

Use a Network Time Protocol (NTP) server to synchronize system time on the FMC and all devices.



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

To synchronize time on FMC and managed devices, see:

- Recommended: Synchronize Time on the FMC with an NTP Server, on page 47

  This topic provides instructions for configuring your FMC to synchronize with an NTP server or servers and includes links to instructions on configuring managed devices to synchronize with the same NTP server or servers.

- Otherwise: Synchronize Time Without Access to a Network NTP Server, on page 48

  This topic provides instructions for setting the time on your FMC, configuring your FMC to serve as an NTP server, and links to instructions on configuring managed devices to synchronize with the FMC NTP server.

Synchronize Time on the FMC with an NTP Server

Time synchronization among all of the components of your system is critically important.

The best way to ensure proper time synchronization between FMC and all managed devices is to use an NTP server on your network.

The FMC supports NTPv4.

You must have Admin or Network Admin privileges to do this procedure.

Before you begin

Note the following:

- If your FMC and managed devices cannot access a network NTP server, do not use this procedure. Instead, see Synchronize Time Without Access to a Network NTP Server, on page 48.
- Do not specify an untrusted NTP server.
- Connections to NTP servers do not use configured proxy settings.
- Firepower 4100 Series devices and Firepower 9300 devices cannot use this procedure to set the system time. Instead, configure those devices to use the same NTP server(s) that you configure using this procedure. For instructions, see the documentation for your hardware model.

Caution If the FMC is rebooted and your DHCP server sets an NTP server record different than the one you specify here, the DHCP-provided NTP server will be used instead. To avoid this situation, configure your DHCP server to use the same NTP server.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Time Synchronization**.

Step 3 If **Serve Time via NTP** is **Enabled**, choose **Disabled** to disable the FMC as an NTP server.

Step 4 For the **Set My Clock** option, choose **Via NTP from** and enter the hostname or IP address of an NTP server.

If your organization has corroborative NTP servers, enter multiple NTP servers as a comma-separated list.

Step 5 Click **Save**.

What to do next

Set managed devices to synchronize with the same NTP server or servers:

- Configure device platform settings: Configure NTP Time Synchronization for Threat Defense and Synchronize Time on Classic Devices with an NTP Server.
- Deploy configuration changes; see Deploy Configuration Changes.

Synchronize Time Without Access to a Network NTP Server

If your devices cannot directly reach the network NTP server, or your organization does not have a network NTP server, a physical-hardware FMC can serve as an NTP server.



Important

- Do not use this procedure unless you have no other NTP server. Instead, use the procedure in Synchronize Time on the FMC with an NTP Server, on page 47.
- Do not use a virtual FMC as an NTP server.

To change the time manually **after** configuring the FMC as an NTP server, you must disable the NTP option, change the time manually, and then re-enable the NTP option.

Procedure

Step 1 Manually set the system time on the FMC:

a) Choose **System** > **Configuration**.
b) Click **Time Synchronization**.
c) If **Serve Time via NTP** is **Enabled**, choose **Disabled**.
d) Click **Save**.
e) For **Set My Clock**, choose **Manually in Local Configuration**.
f) Click **Save**.
g) In the navigation panel at the left side of the screen, click **Time**.
h) Use the **Set Time** drop-down lists to set the time.
i) If the time zone displayed is not UTC, click it and set the time zone to **UTC**.
j) Click **Save**.
k) Click **Done**.
l) Click **Apply**.

Step 2 Set the FMC to serve as an NTP server:

a) In the navigation panel at the left side of the screen, click **Time Synchronization**.
b) For **Serve Time via NTP**, choose **Enabled**.
c) Click **Save**.

Step 3 Set managed devices to synchronize with the FMC NTP server:

a) In the Time Synchronization settings for the platform settings policy assigned to your managed devices, set the clock to synchronize **Via NTP from Management Center**.
b) Deploy the change to managed devices.

For instructions:

- For FTD devices, see Configure NTP Time Synchronization for Threat Defense.
- For all other devices, see Synchronize Time on Classic Devices with an NTP Server.

About Changing Time Synchronization Settings

- Your Firepower Management Center and its managed devices are heavily dependent on accurate time. The system clock is a system facility that maintains the time of the Firepower System. The system clock is set to Universal Coordinated Time (UTC), which is the primary time standard by which the world regulates clocks and time.

  DO NOT ATTEMPT TO CHANGE THE SYSTEM TIME. Changing the system time zone from UTC is NOT supported, and doing so will require you to reimage the device to recover from an unsupported state.

- If you configure the FMC to serve time using NTP, and then later disable it, the NTP service on managed devices still attempts to synchronize time with the FMC. You must update and redeploy any applicable platform settings policies to establish a new time source.

- To change the time manually **after** configuring the Firepower Management Center as an NTP server, you must disable the NTP option, change the time manually, and then re-enable the NTP option.

View Current System Time, Source, and NTP Server Connection Status

Time settings are displayed on most pages in local time using the time zone you set on the Time Zone page in User Preferences (the default is America/New York), but are stored on the appliance using UTC time.



Restriction The Time Zone function (in User Preferences) assumes that the default system clock is set to UTC time. DO NOT ATTEMPT TO CHANGE THE SYSTEM TIME. Be advised that changing the system time from UTC is NOT supported, and doing so will require you to reimage the device to recover from an unsupported state.



Note To view time and time source information on your 7000- and 8000-Series hardware device, see View System Time for 7000/8000 Series Devices.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Time**.

The current time is displayed using the time zone specified for your account in User Preferences.

If your appliance uses an NTP server: For information about the table entries, see NTP Server Status, on page 49.

NTP Server Status

If you are synchronizing time from an NTP server, you can view connection status on the **Time** page (choose **System > Configuration**).

Table 4: NTP Status

Column	Description
NTP Server	The IP address or name of the configured NTP server.
Status	The status of the NTP server time synchronization: • **Being Used** indicates that the appliance is synchronized with the NTP server. • **Available** indicates that the NTP server is available for use, but time is not yet synchronized. • **Not Available** indicates that the NTP server is in your configuration, but the NTP daemon is unable to use it. • **Pending** indicates that the NTP server is new or the NTP daemon was recently restarted. Over time, its value should change to **Being Used**, **Available**, or **Not Available**. • **Unknown** indicates that the status of the NTP server is unknown.
Offset	The number of milliseconds of difference between the time on the appliance and the configured NTP server. Negative values indicate that the appliance is behind the NTP server, and positive values indicate that it is ahead.
Last Update	The number of seconds that have elapsed since the time was last synchronized with the NTP server. The NTP daemon automatically adjusts the synchronization times based on a number of conditions. For example, if you see larger update times such as 300 seconds, that indicates that the time is relatively stable and the NTP daemon has determined that it does not need to use a lower update increment.

Session Timeouts

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.

Note that 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. Users with the Administrator role, whose complete access to menu options poses an extra risk if compromised, cannot be made exempt from session timeouts.

Configure Session Timeouts

To configure session timeouts for Classic devices, use device platform settings. See Configure Session Timeouts for Classic Devices.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Shell Timeout**.

Step 3 Configure session timeouts:

- Web interface (FMC only): Configure the **Browser Session Timeout (Minutes)**. The default value is `60`; the maximum value is `1440` (24 hours).

  To exempt users from this session timeout, see User Account Login Options.

- CLI: Configure the **Shell Timeout (Minutes)** field. The default value is `0`; the maximum value is `1440` (24 hours).

Step 4 Click **Save**.

Vulnerability Mapping

The Firepower System automatically maps vulnerabilities to a host IP address for any application protocol traffic received or sent from that address, when the server has an application ID in the discovery event database and the packet header for the traffic includes a vendor and version.

For any servers which do not include vendor or version information in their packets, you can configure whether the system associates vulnerabilities with server traffic for these vendor and versionless servers.

For example, a host serves SMTP traffic that does not have a vendor or version in the header. If you enable the SMTP server on the Vulnerability Mapping page of a system configuration, then save that configuration to the Firepower Management Center managing the device that detects the traffic, all vulnerabilities associated with SMTP servers are added to the host profile for the host.

Although detectors collect server information and add it to host profiles, the application protocol detectors will not be used for vulnerability mapping, because you cannot specify a vendor or version for a custom application protocol detector and cannot select the server for vulnerability mapping.

Mapping Vulnerabilities for Servers

This procedure requires any Smart License or the Protection classic license.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Choose **Vulnerability Mapping**.

Step 3 You have the following choices:

- To prevent vulnerabilities for a server from being mapped to hosts that receive application protocol traffic without vendor or version information, clear the check box for that server.
- To cause vulnerabilities for a server to be mapped to hosts that receive application protocol traffic without vendor or version information, check the check box for that server.

Tip You can check or clear all check boxes at once using the check box next to **Enabled**.

Step 4 Click **Save**.

Remote Console Access Management

You can use a Linux system console for remote access on supported systems via either the VGA port (which is the default) or the serial port on the physical appliance. Use the Console Configuration page to choose the option most suitable to the physical layout of your organization's Firepower deployment.

On supported physical-hardware-based Firepower systems, you can use Lights-Out Management (LOM) on a Serial Over LAN (SOL) connection on the default (`eth0`) management interface to remotely monitor or manage the system without logging into the management interface of the system. You can perform limited tasks, such as viewing the chassis serial number or monitoring such conditions as fan speed and temperature, using a command line interface on an out-of-band management connection. For information about the cable connection to support LOM, see the *Firepower Management Center Getting Started Guide* for your hardware model.

You must enable LOM for both the system and the user you want to manage the system. After you enable the system and the user, you use a third-party Intelligent Platform Management Interface (IPMI) utility to access and manage your system.

Configuring Remote Console Settings on the System

You must be an Admin user to perform this procedure.

Before you begin

- Disable Spanning Tree Protocol (STP) on any third-party switching equipment connected to the device's management interface.
- If you plan to enable Lights-Out Management see the *Getting Started Guide* for your appliance for information about installing and using an Intelligent Platform Management Interface (IPMI) utility.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Console Configuration**.

Step 3 Click **Save**.

Step 4 The system displays the following warning: "You will have to reboot your system for these changes to take effect." Click **OK** to reboot now or **Cancel** to reboot later.

What to do next

- If you configured serial access, be sure the rear-panel serial port is connected to a local computer, terminal server, or other device that can support remote serial access over ethernet as described in the *Getting Started Guide* for your FMC model.
- If you configured Lights-Out Management, enable a Lights-Out Management user; see Lights-Out Management User Access Configuration, on page 53.

Lights-Out Management User Access Configuration

You must explicitly grant Lights-Out Management permissions to users who will use the feature. LOM users also have the following restrictions:

- You must assign the Administrator role to the user.
- The username may have up to 16 alphanumeric characters. Hyphens and longer user names are not supported for LOM users.
- A user's LOM password is the same as that user's system password. Cisco recommends that you use a complex, non-dictionary-based password of the maximum supported length for your appliance and change it every three months.
- If LOM is enabled on a Firepower 7110, 7115, 7120, or 7125 device, the password may have up to 16 alphanumeric characters.
- Physical Firepower Management Centers and 8000 Series devices can have up to 13 LOM users. 7000 Series devices can have up to eight LOM users.

Note that if you deactivate, then reactivate, a user with LOM while a that user is logged in, or restore a user from a backup during that user's login session, that user may need to log back into the web interface to regain access to `impitool` commands.

Enabling Lights-Out Management User Access

You must be an Admin user to perform this procedure.

You configure LOM and LOM users on a per-system basis using each system's local web interface. You cannot use the Firepower Management Center to configure LOM on a managed device. Similarly, because users are managed independently per appliance, enabling or creating a LOM-enabled user on the Firepower Management Center does not transfer that capability to users on managed devices.

Procedure

Step 1 Choose **System** > **Users** > **Users**.

Step 2 To grant LOM user access to an existing user, click **Edit** ( ) next to a user name in the list.

Step 3 Under **User Configuration**, enable the Administrator role.

Step 4 Check the **Allow Lights-Out Management Access** check box.

Step 5 Click **Save**.

Serial Over LAN Connection Configuration

You use a third-party IPMI utility on your computer to create a Serial Over LAN connection to the appliance. If your computer uses a Linux-like or Mac environment, use IPMItool; for Windows environments, you can use IPMIutil or IPMItool, depending on your Windows version.

Note Cisco recommends using IPMItool version 1.8.12 or greater.

Linux

IPMItool is standard with many distributions and is ready to use.

Mac

You must install IPMItool on a Mac. First, confirm that your Mac has Apple's XCode Developer tools installed, making sure that the optional components for command line development are installed (UNIX Development and System Tools in newer versions, or Command Line Support in older versions). Then you can install macports and the IPMItool. Use your favorite search engine for more information or try these sites:

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

Windows

For Windows Versions 10 and greater with Windows Subsystem for Linux (WSL) enabled, as well as some older versions of Windows Server, you can use IPMItool. Otherwise, you must compile IPMIutil on your Windows system; you can use IPMIutil itself to compile. Use your favorite search engine for more information or try this site:

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

Understanding IPMI Utility Commands

Commands used for IPMI utilities are composed of segments as in the following example for IPMItool on Mac:

```
ipmitool -I lanplus -H IP_address -U user_name command
```

where:

- `ipmitool` invokes the utility.
- `-I lanplus` specifies to use an encrypted IPMI v2.0 RMCP+ LAN Interface for the session.
- `-H IP_address` indicates the IP address you have configured for Lights-Out Management on the appliance you want to access.
- `-U user_name` is the name of an authorized remote session user.
- *`command`* is the name of the command you want to use.

Note Cisco recommends using IPMItool version 1.8.12 or greater.

The same command for IMPIutil on Windows looks like this:

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

This command connects you to the command line on the appliance where you can log in as if you were physically present at the appliance. You may be prompted to enter a password.

Configuring Serial Over LAN with IPMItool

You must be an Admin user with LOM access to perform this procedure.

Procedure

Using IPMItool, enter the following command, and a password if prompted:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

Configuring Serial Over LAN with IPMIutil

You must be an Admin user with LOM access to perform this procedure.

Procedure

Using IPMIutil, enter the following command, and a password if prompted:

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

Lights-Out Management Overview

Lights-Out Management (LOM) provides the ability to perform a limited set of actions over an SOL connection on the default (`eth0`) management interface without the need to log into the system. You use the command to create a SOL connection followed by one of the LOM commands. After the command is completed, the connection ends. Note that not all power control commands are valid on 70xx Family devices.

Note The baseboard management controller (BMC) for a Firepower 71xx, Firepower 82xx, or a Firepower 83xx device is only accessible via 1 Gbps link speeds when the host is powered on. When the device is powered down, the BMC can only establish Ethernet link at 10 and 100 Mbps. Therefore if LOM is being used to remotely power the device, connect the device to the network using 10 and 100 Mbps link speeds only.

Caution In rare cases, if your computer is on a different subnet than the system's management interface and the system is configured for DHCP, attempting to access LOM features can fail. If this occurs, you can either disable and then re-enable LOM on the system, or use a computer on the same subnet as the system to ping its management interface. You should then be able to use LOM.

Caution Cisco is aware of a vulnerability inherent in the Intelligent Platform Management Interface (IPMI) standard (CVE-2013-4786). Enabling Lights-Out Management (LOM) on an system exposes this vulnerability. To mitigate this vulnerability, deploy your systems on a secure management network accessible only to trusted users and use a complex, non-dictionary-based password of the maximum supported length for your system and change it every three months. To prevent exposure to this vulnerability, do not enable LOM.

If all attempts to access your system have failed, you can use LOM to restart your system remotely. Note that if a system is restarted while the SOL connection is active, the LOM session may disconnect or time out.

Caution Do **not** restart your system unless it does not respond to any other attempts to restart. Remotely restarting does not gracefully reboot the system and you may lose data.

Table 5: Lights-Out Management Commands

IPMItool	IPMIutil	Description
(not applicable)	`-V 4`	Enables admin privileges for the IPMI session
`-I lanplus`	`-J 3`	Enables encryption for the IPMI session
`-H` *`hostname/IP address`*	`-N` *`nodename/IP address`*	Indicates the LOM IP address or hostname for the FM
`-U`	`-U`	Indicates the username of an authorized LOM account
`sol activate`	`sol -a`	Starts the SOL session
`sol deactivate`	`sol -d`	Ends the SOL session
`chassis power cycle`	`power -c`	Restarts the appliance (not valid on 70xx Family devic
`chassis power on`	`power -u`	Powers up the appliance
`chassis power off`	`power -d`	Powers down the appliance (not valid on 70xx Family
`sdr`	`sensor`	Displays appliance information, such as fan speeds an temperatures

For example, to display a list of appliance information, the IPMItool command is:

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

Note Cisco recommends using IPMItool version 1.8.12 or greater.

The same command with the IPMIutil utility is:

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

Configuring Lights-Out Management with IPMItool

You must be an Admin user with LOM access to perform this procedure.

Procedure

Enter the following command for IPMItool and a password if prompted:

```
ipmitool -I lanplus -H IP_address -U user_name command
```

Configuring Lights-Out Management with IPMIutil

You must be an Admin user with LOM access to perform this procedure.

Procedure

Enter the following command for IPMIutil and a password if prompted:

```
ipmiutil -J 3 -N IP_address -U username command
```

REST API Preferences

The Firepower REST API provides a lightweight interface for third-party applications to view and manage appliance configuration using a REST client and standard HTTP methods. For more information on the Firepower REST API, see the *Firepower REST API Quick Start Guide*.

By default, the Firepower Management Center allows requests from applications using the REST API. You can configure the Firepower Management Center to block this access.

Enabling REST API Access

Note In deployments using the FMC high availability, this feature is available only in the active FMC.

Procedure

Step 1 Choose **System** > **Configuration**

Step 2 Click **REST API Preferences**.

Step 3 To enable or disable REST API access to the FMC, check or uncheck the **Enable REST API** check box.

Step 4 Click **Save**.

Step 5 Access the REST API Explorer at:
`https://<management_center_IP_or_name>:<https_port>/api/api-explorer`

VMware Tools and Virtual Systems

VMware Tools is a suite of performance-enhancing utilities intended for virtual machines. These utilities allow you to make full use of the convenient features of VMware products. Firepower virtual appliances running on VMware support the following plugins:

- guestInfo
- powerOps
- timeSync
- vmbackup

You can also enable VMware Tools on all supported versions of ESXi. For a list of supported versions, see the Cisco Firepower NGIPSv Quick Start Guide for VMware. For information on the full functionality of VMware Tools, see the VMware website (http://www.vmware.com/).

Enabling VMware Tools on the Firepower Management Center for VMware

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Firepower Management Center	Global only	Admin

Because NGIPSv does not have a web interface, you must use the CLI to enable VMware Tools on that platform; see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Procedure

Step 1 Choose **System** > **Configuration**.

Step 2 Click **VMware Tools**.

Step 3 Click **Enable VMware Tools**.

Step 4 Click **Save**.