



System Configuration

This chapter explains how to configure system configuration settings on the Secure Firewall Management Center.

- [Integrate Management Center with the Cisco Security Cloud, on page 2](#)
- [Requirements and Prerequisites for the System Configuration, on page 8](#)
- [Manage the Secure Firewall Management Center System Configuration, on page 8](#)
- [Access List, on page 8](#)
- [Access Control Preferences, on page 9](#)
- [Audit Log, on page 10](#)
- [Audit Log Certificate, on page 13](#)
- [Change Reconciliation, on page 18](#)
- [DNS Cache, on page 19](#)
- [Dashboard, on page 20](#)
- [Database, on page 20](#)
- [Email Notification, on page 23](#)
- [External Database Access, on page 24](#)
- [HTTPS Certificates, on page 26](#)
- [Information, on page 33](#)
- [Intrusion Policy Preferences, on page 34](#)
- [Language, on page 35](#)
- [Login Banner, on page 36](#)
- [Management Interfaces, on page 36](#)
- [Network Analysis Policy Preferences, on page 50](#)
- [Process, on page 51](#)
- [REST API Preferences, on page 52](#)
- [Remote Console Access Management, on page 52](#)
- [Remote Storage Device, on page 59](#)
- [SNMP, on page 62](#)
- [Session Timeout, on page 63](#)
- [Time, on page 64](#)
- [Time Synchronization, on page 66](#)
- [UCAPL/CC Compliance, on page 69](#)
- [User Configuration, on page 69](#)
- [VMware Tools, on page 73](#)

- [Vulnerability Mapping, on page 73](#)
- [Web Analytics, on page 74](#)
- [History for System Configuration, on page 75](#)

Integrate Management Center with the Cisco Security Cloud

Cisco Security Cloud connects your firewall deployment to the breadth of Cisco's integrated security cloud services for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoints, and applications. Cisco Security Cloud offers a platform approach with simpler, more integrated cloud services that reduce the complexity of managing multiple products.

Use your Cisco Security Cloud Control account to authorize and register the management center with Cisco Security Cloud. This integration brings your firewall deployment onboard to the Cisco cloud tenancy, providing capabilities such as:

- Establish a consistent policy across management centers.
- Implement Zero-Touch Provisioning of the threat defense devices.
- Send events to the cloud and use Cisco Security Cloud services to enrich your threat hunts and investigations.
- Get a centralized view of inventory across management centers.

For more information about onboarding a management center to Security Cloud Control, refer to [Onboard an On-Prem Management Center](#).

To integrate the Secure Firewall Management Center with Cisco XDR, see the [Cisco Secure Firewall Management Center and Cisco XDR Integration Guide](#).

Enable SecureX Integration

Integrate the management center with SecureX to onboard both the management center and its managed devices to a Security Cloud Control tenant. When the management center is onboarded to Security Cloud Control, you can view its managed devices, view managed network objects, and cross-launch to the management center UI to manage associated devices and objects.

Before you begin

- Security Cloud Control uses Cisco Security Cloud Sign On as its identity provider and Duo for multifactor authentication. Ensure that you have your Cisco Security Cloud Sign On credentials and can sign in to the Cisco regional cloud where your account was created.
- You need a Security Cloud Control tenant to integrate the management center with Cisco Security Cloud. If you do not already have a Security Cloud Control tenant, request for a tenant or create one during this workflow. For more information, refer to [Request a Security Cloud Control Tenant](#).
- Link your Security Cloud Control tenant, the one you want to use for onboarding the management center, to your Security Services Exchange (SSE) account. For more information, refer to [Link Your Firewall in Security Cloud Control and Cisco XDR Tenant Accounts](#).
- Your management center must be between version 7.0.2 and 7.0.x, or version 7.2 and later to perform this task.

Procedure

Step 1 In the management center, choose **Integration > SecureX**.

Step 2 Choose a Cisco regional cloud from the **Current Region** drop-down list.

Note

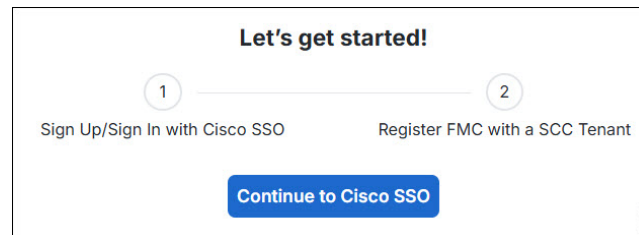
- The regional cloud you choose here is also used for the Cisco Success Network and Cisco Support Diagnostics capabilities. This setting also governs the cloud region for the Secure Network Analytics cloud using Security Analytics and Logging (SaaS).
- If you have already registered the management center with Smart License, the region selected by default will correspond to your Smart Licensing region. In this case, you don't have to change the region.

Step 3 Click **Enable SecureX**.

A separate browser tab opens to log you in to your Security Cloud Control account. Make sure this page is not blocked by a pop-up blocker.

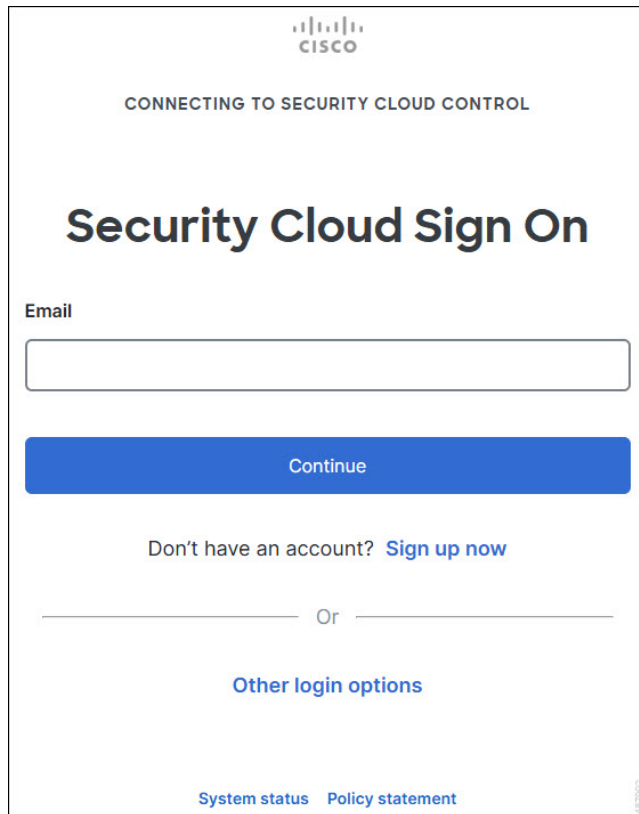
Step 4 Click **Continue to Cisco SSO**.

Figure 1: Welcome Page



Step 5 Log in to your Security Cloud Control account.

Figure 2: Security Cloud Control Sign On

The image shows a web page for "Security Cloud Sign On". At the top, there is a Cisco logo and the text "CONNECTING TO SECURITY CLOUD CONTROL". Below this, the main heading "Security Cloud Sign On" is displayed. Under the heading, there is a label "Email" followed by a text input field. Below the input field is a blue button labeled "Continue". Under the button, there is a link "Don't have an account? Sign up now". Below this link is a horizontal line with the word "Or" in the center. Below the line is a link "Other login options". At the bottom of the page, there are two links: "System status" and "Policy statement".

If you do not have a Security Cloud Sign On account to log in to Security Cloud Control and you want to create one, click **Sign up now** in the **Security Cloud Sign On** page. See [Create a New Cisco Security Cloud Sign On Account](#).

Step 6

Choose a Security Cloud Control tenant that you want to use for this integration. The management center and the managed devices get onboarded to the Security Cloud Control tenant that you choose here.

Figure 3: Choose the Security Cloud Control Tenant

Welcome to Security Cloud Control

To proceed with the registration of your FMC, please select a SCC tenant to register with the FMC and verify the code displayed below matches the user code from your FMC.

☒ Select Tenant ☐ Create Tenant

Search Tenants

- ace2-test
- CDO_cisco-eventing
- cisco-amallio
- Hoysala_CJ
- TechPubs-Cloud
- TechPubs-OnPrem

Grant Application Access

Compare the code below to the authorization code shown in the FMC tab. If the codes match, authorize the FMC to complete the registration. If the codes do not match, [cancel registration](#).

2106C2B8

FMC would like access to your SCC tenant.

- Users:** All internal users in FMC will have read-only access to this SCC tenant.
- Data:** FMC will be able to collect data using SCC APIs.

Authorize FMC

If you do not already have a Security Cloud Control tenant or if you want to use a new tenant for this integration, create a new tenant. See [Request a Security Cloud Control Tenant](#) for more information.

Step 7

Verify that the code displayed in the Security Cloud Control login page matches the code provided by the management center.

Figure 4: Verification Code in Management Center

Grant Application Access

Verify this code in the new window when prompted.

2106C2B8

If the new window doesn't open automatically, [click here to continue](#)

Close

Step 8

Click **Authorize FMC**.

Step 9

In the management center, configure the following:

- **Event Configuration** : Enable this setting to allow threat defense devices to send events directly to the cloud. The event types configured on this page can be used for multiple integrations, where applicable, and enabled. For more information, see [Enable Sending Events to the Cisco Security Cloud](#).
- **Cisco Security Cloud Support**: Enable the Cisco Success Network and Cisco Support Diagnostics capabilities to participate in the customer success initiatives and for an enhanced support experience. For more information, refer to [Configure Management Center to Share Usage Metrics and Statistics with Cisco](#) , on page 6 and [Configure Management Center to Share Device Health Data with Cisco](#), on page 7.

Step 10 Click **Save**.

Configure Management Center to Share Usage Metrics and Statistics with Cisco

Cisco Success Network is a cloud service that enables the management center to establish a secure connection to Cisco cloud and stream usage information and statistics. Streaming this telemetry provides a mechanism to select data of interest from the threat defense device and send it in a structured format to remote management stations for the following reasons:

- To inform you of available, but unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that are available for your product.
- To help Cisco improve its products.

To know more about the telemetry data that Cisco collects, see [Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center Devices](#).

The management center establishes and maintains a secure connection with Cisco cloud at all times when either Cisco Support Diagnostics or Cisco Success Network is enabled. However, the management center and the threat defense devices establish and maintain secure connections with the Cisco cloud when Cisco Support Diagnostics is enabled. You can turn off this connection at any time by disabling both Cisco Success Network and Cisco Support Diagnostics, which disconnects the management center from the Cisco cloud.

You can enable Cisco Success Network when you register the management center with the Smart Software Manager.



Note

- Cisco Success Network is not supported in evaluation mode.
-
- Cisco Success Network is disabled if the management center has a valid Smart Software Manager On-Prem (formerly known as Smart Software Satellite Server) configuration or uses the Specific License Reservation.

Before you begin

Enable SecureX integration or register your management center with the Smart License to perform this task.

Procedure

Step 1 Click **Integration > SecureX**.

Step 2 Under **Cisco Cloud Support**, check the **Enable Cisco Success Network** check box to enable this service.

Note

Read the information provided next to the **Enable Cisco Success Network** check box before you proceed.

Step 3 Click **Save**.

Configure Management Center to Share Device Health Data with Cisco

Cisco Support Diagnostics is a user-enabled cloud-based TAC support service. When enabled, the management center and the managed devices establish a secure connection with the Cisco cloud to stream system health-related information.

Cisco Support Diagnostics provides an enhanced user experience during troubleshooting by allowing Cisco TAC to securely collect essential data from your device during the resolution of a TAC case. Moreover, Cisco periodically collects health data, and processes this data using an automated problem-detection system to notify you of issues if any. While data collection service during the resolution of a TAC case is available for all users with support contracts, the notification service is available only to users with specific service contracts.

Cisco Support Diagnostics allows both threat defense devices and the management center to establish and maintain secure connections with the Cisco cloud. The management center sends the collected data to the regional cloud selected on the **SecureX Integration** page.

You can turn off this connection at any time by disabling both Cisco Success Network and Cisco Support Diagnostics, which disconnect these features from the Cisco cloud.

Administrators can view a sample data set collected from the management center by following the steps in [Producing Troubleshooting Files for Specific System Functions](#).

Before you begin

Enable SecureX integration or register your management center with the Smart License to perform this task.

Procedure

Step 1 Choose **Integration > SecureX**.

Step 2 Under **Cisco Cloud Support**, check the **Enable Cisco Support Diagnostics** check box to enable this service.

Note

Read the information provided next to the **Enable Cisco Support Diagnostics** check box before you proceed.

Step 3 Click **Save**.

Requirements and Prerequisites for the System Configuration

Model Support

Management Center

Supported Domains

Global

User Roles

Admin

Manage the Secure Firewall Management Center System Configuration

The system configuration identifies basic settings for the management center.

Procedure

Step 1 Choose **System** (⚙️) > **Configuration**.

Step 2 Use the navigation panel to choose configurations to change.

Access List

You can limit access to the management center 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 62](#).



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 25](#).



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

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 62](#).

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 62](#).
- 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

[IP Address Conventions](#)

Access Control Preferences

Configure access control preferences on **System** (⚙️) > **Configuration** > **Access Control Preferences**.

Requiring Comments on Rule Changes

You can track changes to access control rules by allowing (or requiring) users to comment when they save. This allows you to quickly assess why critical policies in a deployment were modified. By default, this feature is disabled.

Audit Log

The management center records user activity in read-only audit logs. You can review audit log data in several ways:

- Use the web interface: [Audit and Syslog](#).

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 10](#).
- Stream audit log messages to an HTTP server: [Stream Audit Logs to an HTTP Server, on page 12](#).

Streaming audit log data to an external server allows you to conserve space on the management center. 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 13](#).

Streaming to Multiple Syslog Servers

You can stream audit log data to a maximum of five syslog servers. However, if you have enabled TLS for secured audit log streaming, you can stream only to a single syslog server.

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 management center 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.

Before you begin

Make sure the management center 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 by default uses port 514/UDP to stream audit logs. If you secure the channel (optional, see [Audit Log Certificate, on page 13](#)), 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. You can add a maximum of five syslog hosts, separated by commas. Note You can specify multiple syslog hosts, only when TLS is disabled for the Audit Server Certificate.
Facility	The subsystem that creates the message. Choose a facility described in Syslog Alert Facilities . For example, choose AUDIT.
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 servers 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 Management Center and syslog server are in the same subnet, ARP is used instead of ICMP.

The system displays the result for each 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 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
```

Before you begin

Make sure the device can communicate with the HTTP server. Optionally, secure the channel; see [Audit Log Certificate, on page 13](#).

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 the management center and a trusted audit log server.

Client Certificates (Required)

Generate a certificate signing request (CSR), submit it to a Certificate Authority (CA) for signing, then import the signed certificate onto the management center. Use the local system configuration: [Obtain a Signed Audit Log Client Certificate for the Management Center, on page 14](#) and [Import an Audit Log Client Certificate into the Management Center, on page 15](#).

Server Certificates (Optional)

For additional security, we recommend you require mutual authentication between the management center 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.

Secure Firewall 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 management center web interface.

Use the local system configuration: [Require Valid Audit Log Server Certificates, on page 15](#).

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 management center and the server. You must generate a unique client certificate for each appliance you want to audit.

Before you begin

See ramifications of requiring client and server certificates at [Audit Log Certificate, on page 13](#).

Procedure

Step 1

Obtain and install a signed client certificate on the management center:

- a) [Obtain a Signed Audit Log Client Certificate for the Management Center, on page 14](#):

Generate a Certificate Signing Request (CSR) from the management center 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 management center 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 management center. See [Import an Audit Log Client Certificate into the Management Center, on page 15](#).

- 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 15.
- Step 3** Configure audit log streaming if you have not yet done so.
See [Stream Audit Logs to Syslog](#), on page 10 or [Stream Audit Logs to an HTTP Server](#), on page 12.

Obtain a Signed Audit Log Client Certificate for the Management Center



Important The **Audit Log Certificate** page is not available on a standby management center in a high availability setup. You cannot perform this task from a standby management center.

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

Before you begin

Keep the following in mind:

- 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 Management Center, on page 15](#).

Import an Audit Log Client Certificate into the Management Center

In the management center high availability setup, you *must* use the active peer.

Before you begin

- [Obtain a Signed Audit Log Client Certificate for the Management Center, on page 14](#).
- Make sure you are importing the signed certificate for the correct management center.
- 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 management center, 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.



Important You cannot perform this procedure on the standby management center in a high availability pair.

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 13](#).
- Obtain and import the client certificate following the steps in [Securely Stream Audit Logs, on page 13](#) and the topics referenced in that procedure.

Procedure

-
- Step 1** On the management center, 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, select **Enable TLS**.
- When TLS is enabled, the syslog client (management center) verifies the certificate received from the server. The connection between the client and the server succeeds only if server certificate verification is successful. For this verification process, the following conditions must be met:
- Configure the syslog server to send the certificate to the client.
 - Add (import) a CA certificate to the client to verify the server certificate:
 - You must import the CA certificate during the import of the client certificate.
 - If the issuing CA is a subordinate CA, you have to add the issuing CA before adding the signing CA from the subordinate CA (Root CA), and so on.
- Step 4** If you do not want the client to authenticate itself against the server, but accept the server certificate when the certificate is issued by the same CA (not recommended):
- a) Deselect **Enable Mutual Authentication**.

Important
Ensure that the server is configured to trust the client without verifying any client certificates.
 - b) Click **Save** and skip the remainder of this procedure.
- Step 5** (Optional) To enable client certificate verification by the audit log server, select **Enable Mutual Authentication**.
- Important**
The **Enable Mutual Authentication** option is applicable only when TLS is enabled.

When mutual authentication is enabled, the syslog client (management center) sends a client certificate to the syslog server for verification. The client uses the same CA certificate of the CA who signed the server certificate of the syslog server. The connection succeeds only if client certificate verification is successful. For this verification process, the following conditions must be met:

- Configure the syslog server to verify the certificate received from the client.
- Add a client certificate to be sent to the syslog server. This certificate must be signed by the same CA who signed the server certificate of the syslog server.

Note

To use mutual authentication for streaming Audit Log to the Syslog server, use PKCS#8 format for the private key instead of PKCS#1 format. Use the following command line to convert PKCS#1 keys to PKCS#8 format:

```
openssl pkcs8 -topk8 -inform PEM -outform PEM
-nocrypt -in PKCS1 key file name -out PKCS8 key filename
```

Step 6 (Optional) To automatically recognize server certificates that are no longer valid:

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

Important

This option is displayed only when you select the **Enable Mutual Authentication** check box. However, the **Enable Fetching of CRL** option is applicable only when the TLS option is enabled. The use of CRL is for server certification verification, and it is not dependent on the use of Mutual Authentication which is for enabling client certificate verification.

Enabling fetching of the CRL creates a scheduled task for the client to regularly update (download) the CRL or CRLs. The CRL(s) are used for server certificate verification, where, the verification fails if there is a CRL from the CA specifying that the server certificate being verified has been revoked by the CA.

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 Management Center

You can view the audit log client certificate only for the appliance that you are logged in to. In management center high availability pairs, you can view the certificate only on the active peer.

Procedure

-
- Step 1** Choose **System** (⚙️) > **Configuration**.
Step 2 Click **Audit Log Certificate**.
-

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 24](#) 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 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 threat defense interfaces and routing settings.

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](#)

Dashboard

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 system. The system is delivered with several predefined dashboard widgets.

You can configure the 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**.

Related Topics

[About Dashboards](#)

Database

To manage disk space, the management center 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 management center 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. (Note that in Versions 6.6.0+, you cannot manually delete connection or security Intelligence events in this way.) You can also manually purge the database; see [Data Purge and Storage](#).

Configuring Database Event Limits

Before you begin

- If you want to receive email notifications when events are pruned from the management center's database, you must configure an email server; see [Configuring a Mail Relay Host and Notification Address](#), on page 24.

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 21.
- 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 per management center.

Table 1: Database Event Limits

Event Type	Upper Limit	Lower Limit
Intrusion events	10 million (management center Virtual) 30 million (management center 1000, management center 1600,) 60 million (management center 2500, management center 2600, , FMCv 300) 300 million (management center 4500, management center 4600)	10,000
Discovery events	10 million (management center Virtual) 20 million (management center 2500, management center 2600, management center 4500, management center 4600, FMCv 300)	Zero (disables storage)

Event Type	Upper Limit	Lower Limit
Connection events	50 million (management center Virtual)	Zero (disables storage)
Security-related connection events	100 million (management center 1000, management center 1600,) 300 million (management center 2500, management center 2600, , FMCv 300) 1 billion (management center 4500, management center 4600) Limit is shared between connection events and security-related connection events. The sum of the configured maximums cannot exceed this limit.	<p>If you set the Maximum Connection Events value to zero, then connection events that are not associated with security-related connection, intrusion, file, and malware events are not stored on the management center.</p> <p>Caution Setting Maximum Connection Events to zero immediately purges existing connection events other than security-related connection events.</p> <p>See below for the effect of this setting on Maximum Flow Rate.</p> <p>These settings do not affect connection summaries.</p>
Connection summaries (aggregated connection events)	50 million (management center Virtual) 100 million (management center 1000, management center 1600,) 300 million (management center 2500, management center 2600, , FMCv 300) 1 billion (management center 4500, management center 4600)	Zero (disables storage)
Correlation events and compliance allow list events	1 million (management center Virtual) 2 million (management center 2500, management center 2600, management center 4500, management center 4600, FMCv 300)	One
Malware events	10 million (management center Virtual, management center 1600,) 20 million (management center 2500, management center 2600, , management center 4500, management center 4600, FMCv 300)	10,000
File events	10 million (management center Virtual, management center 1600,) 20 million (management center 2500, management center 2600, , management center 4500, management center 4600, FMCv 300)	Zero (disables storage)
Health events	1 million	Zero (disables storage)
Audit records	100,000	One

Event Type	Upper Limit	Lower Limit
Remediation status events	10 million	One
Allow 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
VPN Troubleshooting database	10 million	Zero (disables storage)

Maximum Flow Rate

The **Maximum flow rate** (flows per second) value for your management center hardware model is specified in the **Platform Specifications** section of the management center datasheet at <https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?cachemode=refresh>

If you set the **Maximum Connection Events** value in platform settings to zero, then connection events that are not associated with security-related connection events, intrusion, file, and malware events are not counted toward the maximum flow rate for your management center hardware.

Any non-zero value in this field causes ALL connection events to be counted against the maximum flow rate.

Other event types on this page do not count against the maximum flow rate.

Email Notification

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**.
-

External Database Access

You can configure the 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 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 that you can use to retrieve and accept the SSL certificate from the management center that you want to access
- the JDBC driver you must use to connect to the database

See the *Secure Firewall Management Center 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 management center.
- Note**
In management center high availability setups, 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

[IP Address Conventions](#)

HTTPS Certificates

Secure Sockets Layer (SSL)/TLS certificates enable management centers to establish an encrypted channel between the system and a web browser. A default certificate is included with all firewall 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 management center supports 4096-bit HTTPS certificates. If the certificate used by the management center was generated using a public server key larger than 4096 bits, you will not be able to log in to the management center web interface. If this happens, contact Cisco TAC.



Note

HTTPS certificates are not supported on the management center REST API.

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 lifetime of the default server certificate depends on when the certificate was generated. To view your default server certificate expiration date, choose **System** (⚙) > **Configuration** > **HTTPS Certificate**.

Note that some Secure Firewall software upgrades can automatically renew the certificate. For more information, see the appropriate version of the [Cisco Secure Firewall Release Notes](#).

On the management center, you can renew the default certificate on the **System** (⚙) > **Configuration** > **HTTPS Certificate** page.

Custom HTTPS Server Certificates

You can use the 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 Secure Firewall 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 entity associated with the public key stored in the subject public key field; must be an X.500 distinguished name (DN). See RFC 5280, section 4.1.2.6 .
Subject Alternative Name	Domain names and IP addresses secured by the certificate. Subject Alternative Name is defined in section RFC 5280, section 4.2.1.6 . We recommend you use this field if the certificate is used for multiple domains or IP addresses.
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 .
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 Secure Firewall appliances, use <code>critical CA:FALSE</code> .

Certificate Field	Description
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 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

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, and Subject Alternative Name.

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**.

The following figure shows an example.

Generate Certificate Signing Request

Subject	
Country Name (two-letter code)	US
State or Province	TX
Locality or City	Austin
Organization	Cisco
Organizational Unit (Department)	Engineering
Common Name	www.example.com
Subject Alternative Name	
Domain Names	www.example.com,www.exchange.e
IP Addresses	192.0.2.1,192.0.2.5,192.0.2.10

[Close](#) [Generate](#)

- 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** To request a certificate that secures multiple domain names or IP addresses, enter the following information in the Subject Alternative Name section:
- a) **Domain Names:** Enter the fully qualified domains and subdomains (if any) secured by the Subject Alternative Name.
 - b) **IP Addresses:** Enter the IP addresses secured by the Subject Alternative Name.
- Step 11** Click **Generate**.
- Step 12** Open a text editor.
- Step 13** 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 14** Save the file as `servername.csr`, where `servername` is the name of the server where you plan to use the certificate.
- Step 15** Click **Close**.

What to do next

- Submit the certificate request to the certificate authority.
- When you receive the signed certificate, import it to the management center; see [Importing HTTPS Server Certificates, on page 30](#).

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 management center supports 4096-bit HTTPS certificates. If the certificate used by the management center was generated using a public server key larger than 4096 bits, you will not be able to log in to the Secure Firewall Management Center 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 management center web interface, contact Support.

Before you begin

- Generate a certificate signing request; see [Generating an HTTPS Server Certificate Signing Request, on page 29](#).
- 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 26](#).

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 Secure Firewall Management Center web interface (as described in [Generating an HTTPS Server Certificate Signing Request, on page 29](#)), 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 management center 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 30](#).
- Import the server certificate chain if needed; see [Importing HTTPS Server Certificates, on page 30](#).

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](#)

Renewing the Default 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**.

The button appears only if your system is configured to use the default HTTPS server certificate.

Step 3 Click **Renew HTTPS Certificate**. (This option appears on the display below the certificate information only if your system is configured to use the default HTTPS server certificate.)

Step 4 (Optional) In the **Renew HTTPS Certificate** dialog box, select **Generate New Key** to generate a new key for the certificate.

Step 5 In the **Renew HTTPS Certificate** dialog box, click **Save**.

What to do next

You can confirm that the certificate has been renewed by checking that that certificate validity dates displayed on the **HTTPS Certificate** page have updated.

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	<p>A descriptive name you assign to the management center appliance. 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.</p> <p>This name is used in certain integrations. For example, it appears in the Devices list in Security Services Exchange when you integrate management center with Cisco XDR.</p> <p>If you change the name, all registered devices are marked out of date and deployment is required to push the new name to the devices.</p>
Product Model	The model name of the appliance.
Serial Number	The serial number of the appliance.
Software Version	The version of the software currently installed on the appliance.
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 (<code>eth0</code>) management interface. If IPv4 management is disabled, this field indicates that.
IPv6 Address	The IPv6 address of the default (<code>eth0</code>) 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.

Intrusion Policy Preferences

Configure various intrusion policy preferences to monitor and track changes to the critical policies in your deployment.

Set Intrusion Policy Preferences

Configure the intrusion policy preferences.

Procedure

-
- Step 1** Choose **System** (⚙️) > **Configuration**.
 - Step 2** Click **Intrusion Policy Preferences**.
 - Step 3** You have the following options:

- **Comments on policy change:** Check this check box to track policy-related changes using the comment functionality when users modify intrusion policies. With policy change comments enabled, administrators can quickly assess why critical policies in a deployment were modified.

If you enable comments on policy changes, you can make the comment optional or mandatory. The management center prompts the user for a comment when each new change to a policy is saved.

- **Write changes in Intrusion Policy to audit log:** Check this check box to record the changes to the intrusion policies to the audit logs. This option is enabled by default.
- **Retain user overrides for deleted Snort 3 rules:** Check this check box to get notifications for changes to any *overridden* system-defined rules during LSP updates. When enabled, the system retains the rule overrides in the new replacement rules that are added as part of the LSP update. On the management center menu bar, click **Notifications** > **Tasks** to view the notifications. This option is enabled by default.

Language

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

Procedure

-
- | | |
|---------------|--|
| Step 1 | Choose System (⚙️) > Configuration . |
| Step 2 | Click Language . |
| Step 3 | Choose the language you want to use. |
| Step 4 | Click Save . |
-

Login Banner

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

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 . |
-

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 management center.

About Management Center Management Interfaces

By default, the management center manages all devices on a single management interface. You can also perform initial setup on the management interface and log into the management center 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* in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

About Device Management

When the management center manages a device, it sets up a two-way, SSL-encrypted communication channel between itself and the device. The management center uses this channel to send information to the device about how you want to analyze and manage your network traffic to the device. As the device evaluates the traffic, it generates events and sends them to the management center using the same channel.

By using the management center to manage devices, you can:

- configure policies for all your devices from a single location, making it easier to change configurations
- install various types of software updates on devices

- push health policies to your managed devices and monitor their health status from the management center



Note If you have a Security Cloud Control-managed device and are using the on-prem management center for analytics only, then the on-prem management center does not support policy configuration or upgrading. Chapters and procedures in this guide related to device configuration and other unsupported features do not apply to devices whose primary manager is Security Cloud Control.

The management center aggregates and correlates intrusion events, network discovery information, and device performance data, allowing you to monitor the information that your devices are reporting in relation to one another, and to assess the overall activity occurring on your network.

You can use the management center to manage nearly every aspect of a device's behavior.



Note Although the management center can manage devices running certain previous releases as specified in the compatibility matrix available at <http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html>, new features that require the latest version of threat defense software are not available to these previous-release devices. Some management center features may be available for earlier versions.

The Management Connection

After you configure the device with the management center information and after you add the device to the management center, either the device or the management center can establish the management connection. Depending on initial setup:

- Either the device or the management center can initiate.
- Only the device can initiate.
- Only the management center can initiate.

Initiation always originates with eth0 on the management center or with the lowest-numbered management interface on the device. Additional management interfaces are tried if the connection is not established. Multiple management interfaces on the management center let you connect to discrete networks or to segregate management and event traffic. However, the initiator does not choose the best interface based on the routing table.

Make sure the management connection is stable, without excessive packet loss, with at least 5 Mbps throughput. By default, the management connection uses TCP port 8305 (this port is configurable). If you place another threat defense between devices and the management center, to prevent potential management disruption, be sure to exempt management traffic from deep inspection by applying a prefilter policy for it.



Note The management connection is a secure, TLS-1.3-encrypted communication channel between itself and the device. You do not need to run this traffic over an additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

Management Interfaces on the Management Center

The management center 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. When the management center manages large numbers of devices on different networks, 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 management center to handle event traffic; you can configure only one event interface. You must also always have a management interface for the management traffic channel. Event traffic can use a large amount of bandwidth, so separating event traffic from management traffic can improve the performance of the management center. 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. Though you may use both management and event interfaces on the same network, we recommend that placing each interface on a separate network to avoid potential routing problems, including routing problems from other devices to the management center. Managed devices will send management traffic to the management center's management interface and event traffic to the management center's 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. However, the management connections cannot be made through the event-only interface.

Management connection initiation from the management center is always attempted first from eth0 and then other interfaces are tried in order; the routing table is not used to determine the best interface.



Note All management interfaces support HTTP administrator access as controlled by your Access List configuration ([Configure an Access List, on page 9](#)). 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 Management Center Model

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

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

Table 2: Management Interface Support on the Management Center

Model	Management Interfaces
MC1000	eth0 (Default) eth1
MC2500, MC4500	eth0 (Default) eth1 eth2 eth3
MC1600, MC2600, MC4600	eth0 (Default) eth1 eth2 eth3 CIMC (Supported for Lights-Out Management only.)
Management Center Virtual	eth0 (Default)

Network Routes on Management Center Management Interfaces

Management interfaces (including event-only interfaces) support only static routes to reach remote networks. When you set up your management center, 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.

You can configure multiple management interfaces on some platforms. The default route does not include an egress interface, so the interface chosen depends on the gateway address you specify, and which interface's network the gateway belongs to. In the case of multiple interfaces on the default network, the device uses the lower-numbered interface as the egress interface.

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 management center.



Note The interface used for management connections is not determined by the routing table. Connections are always tried using eth0 first, and then subsequent interfaces are tried in order until the managed device is reached.

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 management center 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.

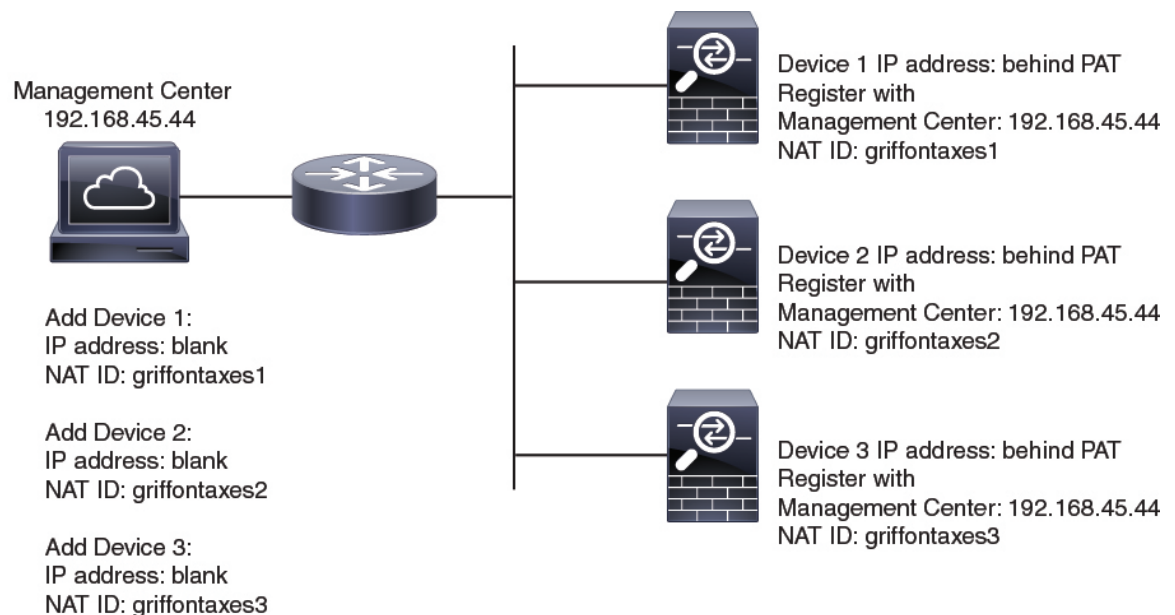
Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the management center specifies the device IP address when you add a device, and the device specifies the management center IP address. However, if you only know one of the IP addresses, 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 management center 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 management center, 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 management center; leave the IP address blank. On the device, you specify the management center IP address, the same NAT ID, and the same registration key. The device registers to the management center's IP address. At this point, the management center uses the NAT ID instead of IP address to authenticate the device.

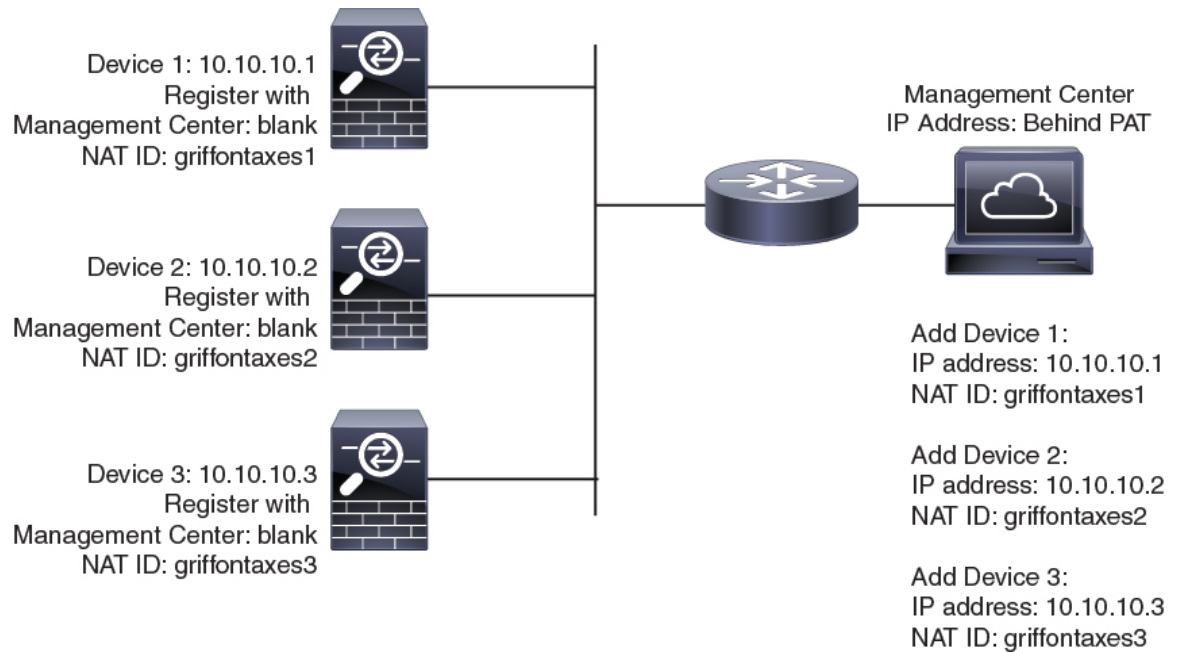
Although the use of a NAT ID is most common for NAT environments, you might choose to use the NAT ID to simplify adding many devices to the management center. On the management center, specify a unique NAT ID for each device you want to add while leaving the IP address blank, and then on each device,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

Figure 5: NAT ID for Managed Devices Behind PAT



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

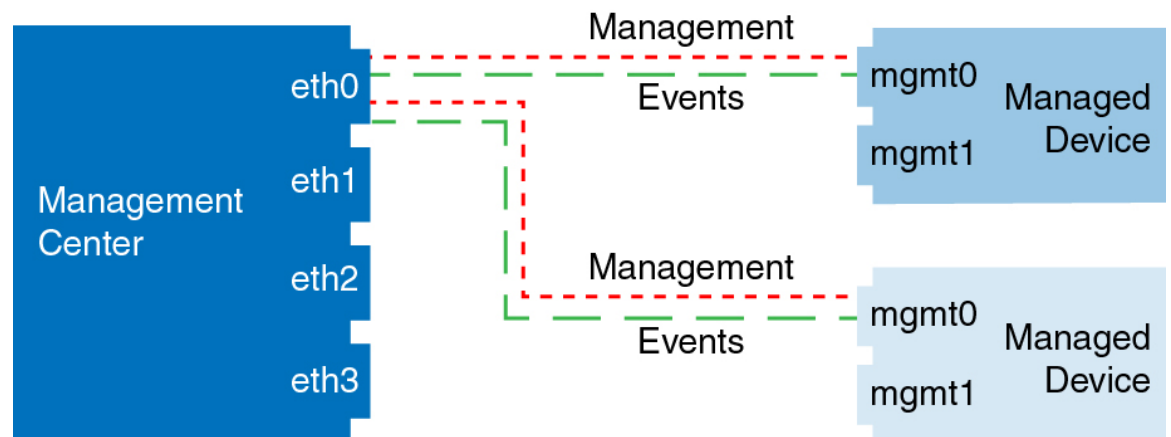
Figure 6: NAT ID for Management Center Behind PAT

Management and Event Traffic Channel Examples



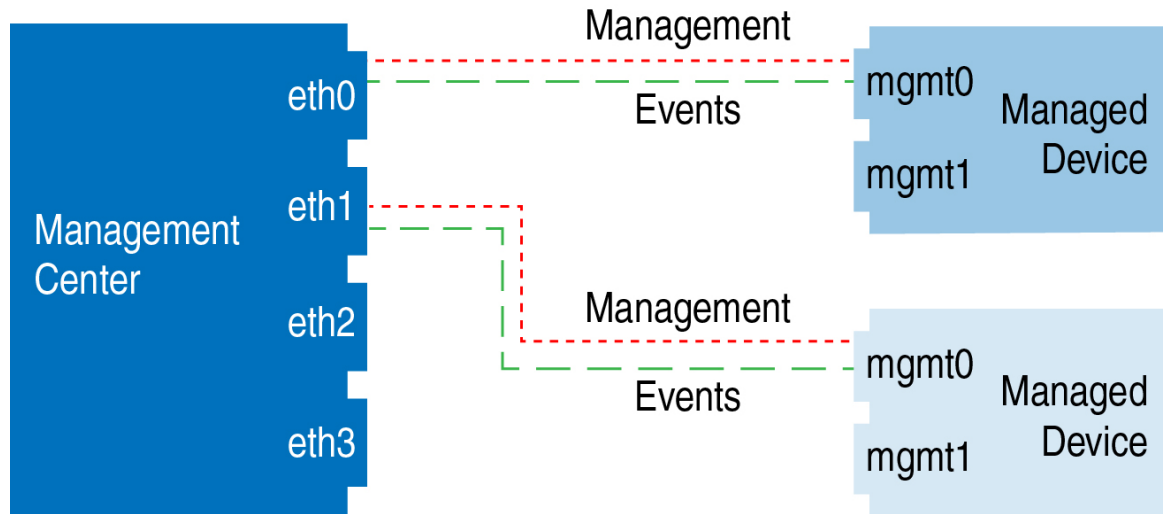
Note If you use a data interface for management on a threat defense, you cannot use separate management and event interfaces for that device.

The following example shows the management center and managed devices using only the default management interfaces.

Figure 7: Single Management Interface on the Secure Firewall Management Center

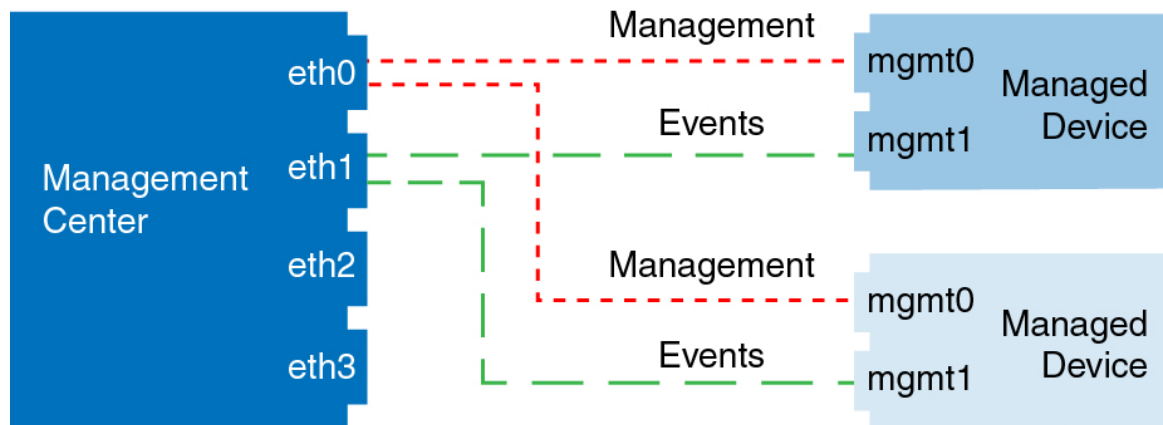
The following example shows the management center using separate management interfaces for devices; and each managed device using 1 management interface.

Figure 8: Multiple Management Interfaces on the Secure Firewall Management Center



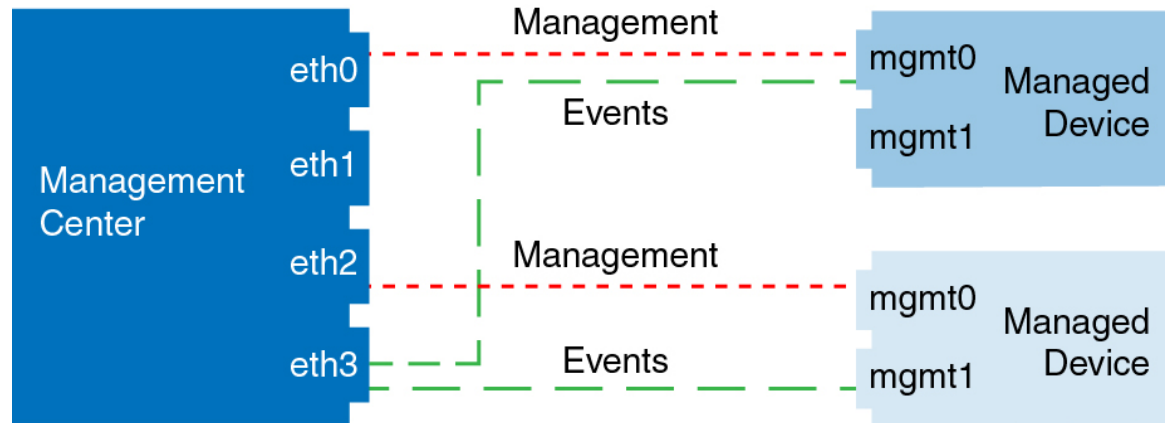
The following example shows the management center and managed devices using a separate event interface.

Figure 9: Separate Event Interface on the Secure Firewall Management Center and Managed Devices



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

Figure 10: Mixed Management and Event Interface Usage



Modify Management Center Management Interfaces

Modify the management interface settings on the 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 reconnect because of a configuration error, you must access the management center console port to reconfigure the network settings in the Linux shell. You must contact Cisco TAC to guide you in this operation.

If you change the management center IP address, then see *Edit the management center IP Address or Hostname on the Device* in the [Cisco Secure Firewall Management Center Device Configuration Guide](#). If you change the management center IP address or hostname, you should also change the value at the device CLI so the configurations match. Although in most cases, the management connection will be reestablished without changing the management center IP address or hostname on the device, in at least one case, you must perform this task for the connection to be reestablished: when you added the device to the management center and you specified the NAT ID only. Even in other cases, we recommend keeping the management center IP address or hostname up to date for extra network resiliency.

In a high availability configuration, when you modify the management IP address of a registered device from the device CLI or from the management center, the secondary management center does not reflect the changes even after an high availability synchronization. To ensure that the secondary management center is also updated, switch roles between the two management centers, making the secondary management center as the active unit. Modify the management IP address of the registered device on the Device Management page of the now active management center.

If you modify the management IP address of one peer management center in a high availability configuration, the remote peer does not reflect the changes even after an high availability synchronization. To ensure that the remote peer management center is also updated, you must log in to the remote peer management center, navigate to **Integration > Other Integrations > High Availability > Peer Manager**, and then manually update the IP address of its peer manager. For more detailed instructions, see [Change the IP Address of the Management Center in a High Availability Pair](#).

Before you begin

- For information about how device management works, see *About Device Management Interfaces* in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).
- 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** > **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**—You must always have at least one interface with **Management Traffic** enabled. You can optionally configure an event-only interface. You can configure only one event interface on the management center. 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 remaining management interfaces. In either case, the device tries to send events to the event-only interface, and if that interface is down, it sends 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 Gigabit Ethernet interfaces.
- **MDI/MDIX**—Set the **Auto-MDIX** setting.
- **MTU**—Set the maximum transmission unit (MTU) between 1280 and 1500. The default is 1500.
- **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).

If you use DHCP, you must use DHCP reservation, so the assigned address does not change. If the DHCP address changes, device registration will fail because the management center network configuration gets out of sync. To recover from a DHCP address change, connect to the management center (using the hostname or the new IP address) and navigate to **System** (⚙️) > **Configuration** > **Management Interfaces** to reset the network.
 - **Disabled**—Disable IPv4. Do **not** disable both IPv4 and IPv6.
- **IPv6 Configuration**—Set the IPv6 IP address. Choose:
 - **Static**—Manually enter the **IPv6 Management IP** address and **IPv6 Prefix Length**.

- **DHCP**—Set the interface to use DHCPv6 (eth0 only).
- **Router Assigned**—Enable stateless autoconfiguration.
- **Disabled**—Disable IPv6. Do **not** disable both IPv4 and IPv6.
- **IPv6 DAD**—When you enable IPv6, enable or disable duplicate address detection (DAD). You might want to disable DAD because the use of DAD opens up the possibility of denial-of-service attacks. If you disable this setting, you need check manually that this interface is not using an already-assigned address.

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

Click the **View** () icon to view the route table.

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 Management Center Management Interfaces, on page 39](#).

Note

For the default route, you can change only the gateway IP address. The egress interface is chosen automatically by matching the specified gateway to the interface's network.

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 management center hostname. The hostname can have a maximum of 64 characters, must start and end with a letter or digit, and have only letters, digits, or a hyphen. If you change the hostname, reboot the management center if you want the new hostname reflected in syslog messages. Syslog messages do not reflect a new hostname until after a reboot.
- **Domains**—Set one or more search domains for the management center, 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 management center and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.

Note

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

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

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

Step 6 In the **Proxy** area, configure HTTP proxy settings.

The management center 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.

- Check the **Enabled** check box.
- 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.
- In the **Port** field, enter a port number.
- Supply authentication credentials by choosing **Use Proxy Authentication**, and then provide a **User Name** and **Password**.

Step 7 Click **Save**.

Step 8 If you change the management center IP address, then see *Edit the management center IP Address or Hostname on the Device* in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

If you change the management center IP address or hostname, you should also change the value at the device CLI so the configurations match. Although in most cases, the management connection will be reestablished without changing the management center IP address or hostname on the device, in at least one case, you must perform this task for the connection to be reestablished: when you added the device to the management center and you specified the NAT ID only. Even in other cases, we recommend keeping the management center IP address or hostname up to date for extra network resiliency.

Change Both Management Center and Threat Defense IP Addresses

You might want to change both management center and threat defense IP addresses if you need to move them to a new network.

Procedure

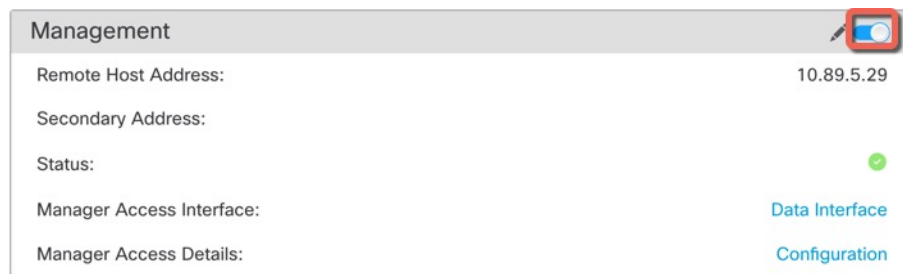
Step 1

Disable the management connection.

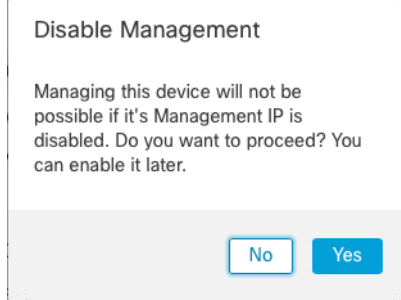
For a high-availability pair or cluster, perform these steps on all units.

- Choose **Devices > Device Management**.
- Next to the device, click **Edit** (✎).
- Click **Device**, and view the **Management** area.
- Disable management temporarily by clicking the slider so it is disabled (☐).

Figure 11: Disable Management



You are prompted to proceed with disabling management; click **Yes**.



Step 2

Change the device IP address in the management center to the new device IP address.

You will change the IP address on the device later.

For a high-availability pair or cluster, perform these steps on all units.

- Edit the **Remote Host Address** IP address and optional **Secondary Address** (when using a redundant data interface) or hostname by clicking **Edit** (✎).

Figure 12: Edit Management Address

- b) In the **Management** dialog box, modify the name or IP address in the **Remote Host Address** field and the optional **Secondary Address** field, and click **Save**.

Figure 13: Management IP Address

Step 3 Change the management center IP address.

Caution

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

- Choose **System** (⚙) > **Configuration** > **Management Interfaces**.
- In the **Interfaces** area, click **Edit** next to the interface that you want to configure.
- Change the IP address, and click **Save**.

Step 4 Change the manager IP address on the device.

For a high-availability pair or cluster, perform these steps on all units.

- At the threat defense CLI, view the management center identifier.

show managers

Example:

```
> show managers
Type           : Manager
Host           : 10.10.1.4
Display name   : 10.10.1.4
Identifier     : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration   : Completed
```


Management type : Configuration

- b) Edit the management center IP address or hostname.

configure manager edit identifier {hostname {ip_address | hostname} | displayname display_name}

If the management center was originally identified by **DONTRESOLVE** and a NAT ID, you can change the value to a hostname or IP address using this command. You cannot change an IP address or hostname to **DONTRESOLVE**.

Example:

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

- Step 5** Change the IP address of the manager access interface at the console port.

For a high-availability pair or cluster, perform these steps on all units.

If you use the dedicated Management interface:


configure network ipv4

configure network ipv6

If you use the dedicated Management interface:

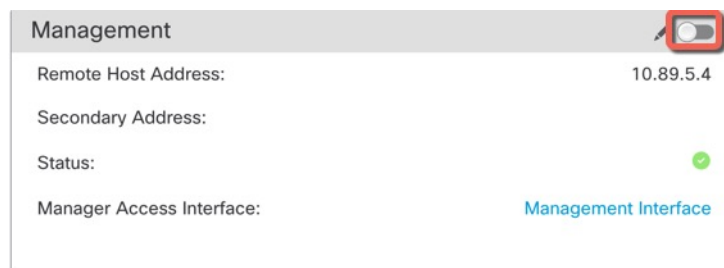
configure network management-data-interface disable

configure network management-data-interface

- Step 6** Reenable management by clicking the slider so it is enabled ().

For a high-availability pair or cluster, perform these steps on all units.

Figure 14: Enable Management Connection



- Step 7** (If using a data interface for manager access) Refresh the data interface settings in the management center.

For a high-availability pair, perform this step on both units.

- Choose **Devices > Device Management > Device > Management > Manager Access - Configuration Details**, and click **Refresh**.
- Choose **Devices > Device Management > Interfaces**, and set the IP address to match the new address.
- Return to the **Manager Access - Configuration Details** dialog box, and click **Acknowledge** to remove the deployment block.

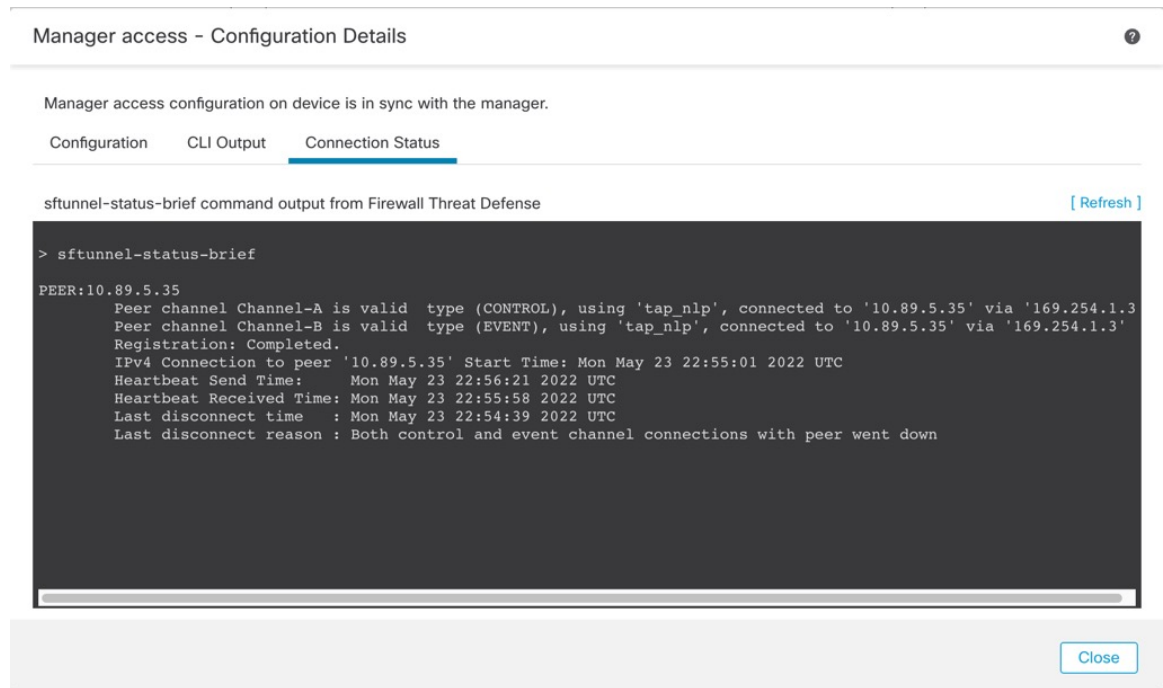
- Step 8** Ensure the management connection is reestablished.

In the management center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

The following status shows a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 15: Connection Status



- Step 9** (For a high-availability management center pair) Repeat configuration changes on the secondary management center.
- Change the secondary management center IP address.
 - Specify the new peer addresses on both units.
 - Make the secondary unit the active unit.
 - Disable the device management connection.
 - Change the device IP address in the management center.
 - Reenable the management connection.

Network Analysis Policy Preferences

You can configure the system to track policy-related changes using the comment functionality when users modify network analysis policies. With policy change comments enabled, administrators can quickly assess why critical policies in a deployment were modified.

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.

Optionally, you can have changes to network analysis policies written to the audit log.

Process

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

- Shut down: Initiate a graceful shutdown of the appliance.



Caution

Do **not** shut off Secure Firewall 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 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 Management Center

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.

REST API Preferences

The management center REST API provides a lightweight interface for third-party applications to view and manage device configuration using a REST client and standard HTTP methods. For more information on the management center REST API, see the [Secure Firewall Management Center REST API Quick Start Guide](#).



Note HTTPS certificates are not supported on the management center REST API.

By default, the management center allows requests from applications using the REST API. You can configure the management center to block this access.

Enabling REST API Access



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

Procedure

-
- Step 1** Choose **System** (⚙) > **Configuration**
 - Step 2** Click **REST API Preferences**.
 - Step 3** To enable or disable REST API access to the management center, 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`
-

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 Secure Firewall deployment.

On supported physical-hardware-based systems, you can use Lights-Out Management (LOM) on a Serial Over LAN (SOL) connection 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. The cable connection to support LOM varies by management center model:

- For management center models MC1600, MC2600, and MC4600, use a connection with the CIMC port to support LOM. See the [Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide](#) for more information.
- For all other management center hardware models, use a connection with the default (eth0) management port to support LOM. See the [Navigating the Cisco Secure Firewall Threat Defense Documentation 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 | Choose a remote console access option: <ul style="list-style-type: none">• Choose VGA to use the appliance's VGA port.• Choose Physical Serial Port to use the appliance's serial port.• Choose Lights-Out Management to use an SOL connection on the management center. (This may use the default management port or the CIMC port depending on your management center model. See the Getting Started Guide for your model for more information.) |
| Step 4 | To configure LOM via SOL: <ul style="list-style-type: none">• Choose the address Configuration for the system (DHCP or Manual).• If you chose manual configuration, enter the necessary IPv4 settings:<ul style="list-style-type: none">• Enter the IP Address to be used for LOM. <p>Note
The LOM IP address must be different from and in the same subnet as the management center management interface IP address.</p> <ul style="list-style-type: none">• Enter the Netmask for the system. |

- Enter the **Default Gateway** for the system.

Step 5 Click **Save**.

Step 6 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 management center model.
- If you configured Lights-Out Management, enable a Lights-Out Management user; see [Lights-Out Management User Access Configuration](#), on page 54.

Lights-Out Management User Access Configuration

You must explicitly grant Lights-Out Management permissions to users who 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 usernames are not supported for LOM users.
- A user's LOM password is the same as that user's system password. The password must comply with the requirements described in [User Passwords](#). 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.
- Physical management centers can have up to 13 LOM users.

Note that if you deactivate and then reactivate a user with LOM while that user is logged in, that user may need to log back into the web interface to regain access to `ipmitool` commands.



Note High Availability synchronization is not applicable for LOM users and hence they are not replicated on high availability management centers. You must create different admin users with LOM enabled on the active management center.

In a high-availability configuration, when you create a local user or reset the password for a local user with LOM privilege enabled, from the UCS-based active management center, the changes get synced to both the active and standby management centers and the active management center CIMC. The new password is not synced with the standby management center for CIMC login. To ensure that the standby management center is also updated, reset the CIMC login password for the local user on the standby management center.

Enabling Lights-Out Management User Access

You must be an Admin user to perform this procedure.

Use this task to grant LOM access to an existing user. To grant LOM access to a new user, see [Add or Edit an Internal User](#).

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 IPMIutil on Windows looks like this:

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

This command connects you to the command line on the appliance where you can log in as if you are physically present near 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.



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 a 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 3: Lights-Out Management Commands

IPMItool	IPMIutil	Description
(not applicable)	<code>-V 4</code>	Enables admin privileges for the IPMI session
<code>-I lanplus</code>	<code>-J 3</code>	Enables encryption for the IPMI session
<code>-H hostname/IP address</code>	<code>-N nodename/IP address</code>	Indicates the LOM IP address or hostname for the management center
<code>-U</code>	<code>-U</code>	Indicates the username of an authorized LOM account
<code>sol activate</code>	<code>sol -a</code>	Starts the SOL session
<code>sol deactivate</code>	<code>sol -d</code>	Ends the SOL session
<code>chassis power cycle</code>	<code>power -c</code>	Restarts the appliance

IPMItool	IPMIutil	Description
chassis power on	power -u	Powers up the appliance
chassis power off	power -d	Powers down the appliance
sdr	sensor	Displays appliance information, such as fan speeds and 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
```

Remote Storage Device

You can store management center backups and reports locally, or mount one of the following systems:

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

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 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. See [Database, on page 20](#).

Configure 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 . |
-

Configure NFS for Remote Storage

The management center can store backups and reports on an NFS mount.

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: <ul style="list-style-type: none">• 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 mount options in **Command Line Options**.

You can specify the version number of the NFS storage using the following format:

vers=version

For example, to select NFSv4, enter:

vers=4.0

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 Click **Test** to test the connection.

Step 8 Click **Save**.

Troubleshooting

When there is a random latency in the NFS connection with the firewall device, perform the following activities, and then contact Cisco TAC for troubleshooting:

- Collect troubleshooting file before or after the issue from the device. You can generate the troubleshoot file from the web interface or using CLI commands. For information on how to generate the troubleshoot file, see [Troubleshoot Firepower File Generation Procedures](#).
- Collect the incoming and exiting traffic PCAP records. For information on the procedure, see [Packet Capture Overview](#).
- Collect system-support trace data while NFS application fails using the following command in the device (CLISH mode):

```
> system support trace
```
- Collect snort counters twice during the failure using the **show snort counters** command to view the statistics for the Snort preprocessor connections. For information on this command, see [show snort counters](#).

Configure SMB for Remote Storage

The management center can store backups and reports on an SMB mount.

Before you begin

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

- 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 management center 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 mount options in **Command Line Options**.
- You can specify the version number of the SMB storage using the following format:
- vers=version**
- If SMB encryption is enabled for a file server, only SMB version 3.0 clients are allowed to access the file server. In this case, enter:
- vers=3.0**
- 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**.
-

Configure SSH for Remote Storage

The management center can store backups and reports on an SSHFS mount.

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 mount options in **Command Line Options**.
- 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** Click **Test** to test the connection.
- Step 8** Click **Save**.
-

SNMP

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

Before you begin

Add SNMP access for each computer you plan to use to poll the system. See [Configure an Access List, on page 9](#).



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**.
-

Session Timeout

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

Procedure

Step 1 Choose **System** (⚙️) > **Configuration**.

Step 2 Click **CLI Timeout**.

Step 3 Configure session timeouts:

- Web interface (management center 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 [Add or Edit an Internal User](#).
- CLI: Configure the **CLI Timeout (Minutes)** field. The default value is 0; the maximum value is 1440 (24 hours).

Step 4 Click **Save**.

Time

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.

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 65](#).

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	<p>The status of the NTP server time synchronization:</p> <ul style="list-style-type: none">• 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.
Authentication	<p>The authentication status for communication between the management center and the NTP server:</p> <ul style="list-style-type: none">• none indicates no authentication is configured.• bad indicates authentication is configured but has failed.• ok indicates authentication is successful. <p>If authentication has been configured, the system displays the key number and key type (SHA-1, MD5, or AES-128 CMAC) following the status value. For example: bad, key 2, MD5.</p>
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.

Time Synchronization

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

Use a Network Time Protocol (NTP) server to synchronize system time on the management center and all devices. The management center supports secure communications with NTP servers using MD5, SHA-1, or AES-128 CMAC symmetric key authentication; for system security, we recommend using this feature.

The management center can also be configured to connect solely with authenticated NTP servers; using this option improves security in a mixed-authentication environment, or when you migrate your system to different NTP servers. It is redundant to use this setting in an environment where all reachable NTP servers are authenticated.



Note If you specified an NTP server for the management center during initial configuration, the connection with that NTP server is not secured. You must edit the configuration for that connection to specify MD5, SHA-1, or AES-128 CMAC keys.



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

To synchronize time on management center and managed devices, see:

- Recommended: [Synchronize Time on the Management Center with an NTP Server, on page 66](#)

This topic provides instructions for configuring your management center 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 68](#)

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

Synchronize Time on the Management Center 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 management center and all managed devices is to use an NTP server on your network.

The management center supports NTPv4.

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

Before you begin

Note the following:

- If your management center 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 68](#).
- Do not specify an untrusted NTP server.
- If you plan to establish a secure connection with an NTP server (recommended for system security), obtain an SHA-1, MD5, or AES-128 CMAC key number and value configured on that 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 management center 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 management center as an NTP server.
- Step 4** For the **Set My Clock** option, choose **Via NTP**.
- Step 5** Click **Add**.
- Step 6** In the **Add NTP Server** dialog box, enter the host name or IPv4 or IPv6 address of an NTP server.
- Step 7** (Optional) To secure communication between your management center and the NTP server:
 - a) Select **MD5**, **SHA-1** or **AES-128 CMAC** from the **Key Type** drop-down list.
 - b) Enter an the corresponding MD5, SHA-1, or AES-128 CMAC **Key Number** and **Key Value** from the specified NTP server.
- Step 8** Click **Add**.
- Step 9** When only two NTP servers are configured, the offset difference between them becomes high. This results in the management center using the Local Time. Hence, we recommend that you configure atleast three NTP servers.

To add more NTP servers, repeat Steps 5 through 8.
- Step 10** (Optional) To force the management center to use only an NTP server that successfully authenticates, check the **Use the authenticated NTP server only** check box.
- Step 11** 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* in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

Note that even if you force the management center to make a secure connection with an NTP server (**Use the authenticated NTP server only**), device connections to that server do not use authentication.

- Deploy configuration changes; see the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

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 management center 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 Management Center with an NTP Server, on page 66](#).
- Do not use a virtual management center as an NTP server.

To change the time manually **after** configuring the management center 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 management center:

- Choose **System** (⚙️) > **Configuration**.
- Click **Time Synchronization**.
- If **Serve Time via NTP** is **Enabled**, choose **Disabled**.
- Click **Save**.
- For **Set My Clock**, choose **Manually in Local Configuration**.
- Click **Save**.
- In the navigation panel at the left side of the screen, click **Time**.
- Use the **Set Time** drop-down lists to set the time.

Note

When you change the time on the management center by more than two hours, you must reboot the device as soon as possible, for example in a maintenance window, to avoid any malfunction.

- If the time zone displayed is not UTC, click it and set the time zone to **UTC**.
- Click **Save**.
- Click **Done**.
- Click **Apply**.

Step 2

Set the management center 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 management center 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 threat defense devices, see *Configure NTP Time Synchronization for Threat Defense* in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

About Changing Time Synchronization Settings

- Your 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 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 management center to serve time using NTP, and then later disable it, the NTP service on managed devices still attempts to synchronize time with the management center. You must update and redeploy any applicable platform settings policies to establish a new time source.
- To change the time manually **after** configuring the management center as an NTP server, you must disable the NTP option, change the time manually, and then re-enable the NTP option.

UCAPL/CC 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. For more information about this setting, see [Security Certifications Compliance Modes](#).

User Configuration

Global User Configuration settings affect all users on the management center. Configure these settings on the User Configuration page (**System** (⚙️) > **Configuration** > **User Configuration**):

- **Password Reuse Limit:** The number of passwords in a user's most recent history that cannot be reused. This limit applies to web interface access for all users. For the `admin` user, this applies to CLI access as well; the system maintains separate password lists for each form of access. Setting the limit to zero (the default) places no restrictions on password reuse. See [Set Password Reuse Limit, on page 70](#).

- **Track Successful Logins:** The number of days that the system tracks successful logins to the management center, per user, per access method (web interface or CLI). When users log in, the system displays their successful login count for the interface being used. When **Track Successful Logins** is set to zero (the default), the system does not track or report successful login activity. See [Track Successful Logins, on page 71](#).
- **Max Number of Login Failures:** The number of times in a row that users can enter incorrect web interface login credentials before the system temporarily blocks the account from access for a configurable time period. If a user continues login attempts while the temporary lockout is in force:
 - The system refuses access for that account (even with a valid password) without informing the user that a temporary lockout is in force.
 - The system continues to increment the failed login count for that account with each login attempt.
 - If the user exceeds the **Maximum Number of Failed Logins** configured for that account on the individual User Configuration page, the account is locked out until an admin user reactivates it.
- **Set Time in Minutes to Temporarily Lockout Users:** The duration in minutes for a temporary web interface user lockout if **Max Number of Failed Logins** is non-zero.
- **Max Concurrent Sessions Allowed:** Maximum sessions for users: The number of sessions of a particular type (read-only or read/write) that can be open at the same time. The type of session is determined by the roles assigned to a user. If a user is assigned only read-only roles, that user's session is counted toward the **(Read Only)** session limit. If a user has any roles with write privileges, the session is counted toward the **Read/Write** session limit. For example, if a user is assigned the Admin role and the **Maximum sessions for users with Read/Write privileges/CLI users** is set to 5, the user will not be allowed to log in if there are already five other users logged in that have read/write privileges.

**Note**

Predefined user roles and custom user roles that the system considers read-only for the purposes of concurrent session limits, are labeled with **(Read Only)** in the role name on the **System (⚙️) > Users > Users** and the **System (⚙️) > Users > User Roles**. If a user role does not contain **(Read Only)** in the role name, the system considers the role to be read/write. The system automatically applies **(Read Only)** to roles that meet the required criteria. You cannot make a role read-only by adding that text string manually to the role name.

For each type of session, you can set a maximum limit ranging from 1 to 1024. When **Max Concurrent Sessions Allowed** is set to zero (the default), the number of concurrent sessions is unlimited.

If you change the concurrent session limit to a value more restrictive, the system will not close any currently open sessions; it will, however, prevent new sessions beyond the number specified from being opened.

Set Password Reuse Limit

If you enable the **Password Reuse Limit**, the system keeps encrypted *password histories* for management center users. Users cannot reuse passwords in their histories. You can specify the number of stored passwords for each user, per access method (web interface or CLI). A user's current password counts towards this number.

If you lower the limit, the system deletes older passwords from the history. Increasing the limit does not restore deleted passwords.

Procedure

-
- Step 1** Choose **System** (⚙️) > **Configuration**.
 - Step 2** Click **User Configuration**.
 - Step 3** Set the **Password Reuse Limit** to the number of passwords you want to maintain in the history (maximum 256).
To disable password reuse checking, enter 0.
 - Step 4** Click **Save**.
-

Track Successful Logins

Use this procedure to enable tracking successful logins for each user for a specified number of days. When this tracking is enabled, the system displays the successful login count when users log into the web interface or the CLI.



Note If you lower the number of days, the system deletes records of older logins. If you then increase the limit, the system does not restore the count from those days. In that case, the reported number of successful logins may be temporarily lower than the actual number.

Procedure

-
- Step 1** Choose **System** (⚙️) > **Configuration**.
 - Step 2** Click **User Configuration**.
 - Step 3** Set **Track Successful Login Days** to the number of days to track successful logins (maximum 365).
To disable login tracking, enter 0.
 - Step 4** Click **Save**.
-

Enabling Temporary Lockouts

Enable the temporary timed lockout feature by specifying the number of failed login attempts in a row that the system allows before the lockout goes into effect.

Procedure

-
- Step 1** Choose **System** (⚙️) > **Configuration**.
- Step 2** Click **User Configuration**.
- Step 3** Set the **Max Number of Login Failures** to the maximum number of consecutive failed login attempts before the user is temporarily locked out.
- To disable the temporary lockout, enter zero.
- Step 4** Set the **Time in Minutes to Temporarily Lockout Users** to the number of minutes to lock out users who have triggered a temporary lockout.
- When this value is zero, users do not have to wait to retry to log in, even if the **Max Number of Login Failures** is non-zero.
- Step 5** Click **Save**.
-

Set Maximum Number of Concurrent Sessions

You can specify the maximum number of sessions of a particular type (read-only or read/write) that can be open at the same time. The type of session is determined by the roles assigned to a user. If a user is assigned only read-only roles, that user's session is counted toward the **Read Only** session limit. If a user has any roles with write privileges, the session is counted toward the **Read/Write** session limit.

Procedure

-
- Step 1** Choose **System** (⚙️) > **Configuration**.
- Step 2** Click **User Configuration**.
- Step 3** For each type of session, set the **Max Concurrent Sessions Allowed** to the maximum number of sessions that can be open at the same time.
- To apply no limits on concurrent sessions per users, enter zero.
- Note**
If you change the concurrent session limit to a value more restrictive, the system will not close any currently open sessions; it will, however, prevent new sessions beyond the number specified from being opened.
- Step 4** Click **Save**.
-

VMware Tools

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. Secure Firewall 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 information on the full functionality of VMware Tools, see the VMware website (<http://www.vmware.com/>).

Enabling VMware Tools on the Secure Firewall Management Center for VMware

Procedure

-
- | | |
|---------------|--|
| Step 1 | Choose System (⚙️) > Configuration . |
| Step 2 | Click VMware Tools . |
| Step 3 | Click Enable VMware Tools . |
| Step 4 | Click Save . |
-

Vulnerability Mapping

The 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 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**.

Web Analytics

By default, in order to improve firewall products, Cisco collects non-personally-identifiable usage data, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your management center appliances.

Data collection begins after you accept the End User License Agreement. If you do not want Cisco to continue to collect this data, you can opt out using the following procedure.

Procedure

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

Step 2 Click **Web Analytics**.

Step 3 Make your choice and click **Save**.

What to do next

(Optional) Determine whether to share data via the [Configure Cisco Success Network Enrollment](#).

History for System Configuration

Feature	Minimum Management Center	Minimum Threat Defense	Details
Access control performance improvements (object optimization).	7.2.4 7.4.0	Any	<p>Upgrade impact. First deployment after management center upgrade to 7.2.4–7.2.5 or 7.4.0 can take a long time and increase CPU use on managed devices.</p> <p>Access control object optimization improves performance and consumes fewer device resources when you have access control rules with overlapping networks. The optimizations occur on the <i>managed device</i> on the first deploy after the feature is enabled on the management center (including if it is enabled by an upgrade). If you have a high number of rules, the system can take several minutes to an hour to evaluate your policies and perform object optimization. During this time, you may also see higher CPU use on your devices. A similar thing occurs on the first deploy after the feature is disabled (including if it is disabled by upgrade). After this feature is enabled or disabled, we recommend you deploy when it will have the least impact, such as a maintenance window or a low-traffic time.</p> <p>New/modified screens (requires Version 7.2.6): System ⚙️ > Configuration > Access Control Preferences > Object-group optimization.</p> <p>Version restrictions: Not supported with management center Version 7.3.x.</p>
French language option.	7.2	Any	<p>You can now switch the management center web interface to French.</p> <p>New/modified screens: System ⚙️ > Configuration > Language.</p>
Exempt most connection events from event rate limits.	7.0	Any	<p>Setting the Maximum Connection Events value for the Connection Database to zero now exempts low priority connection events from counting towards the flow rate limit for your FMC hardware. Previously, setting this value to zero applied only to event storage, and did not affect the flow rate limit.</p> <p>New/modified screens: System ⚙️ > Configuration > Database</p> <p>Supported platforms: Hardware FMCs.</p>
Support for AES-128 CMAC authentication for NTP servers.	7.0	Any	<p>Connections between the FMC and NTP servers can be secured with AES-128 CMAC keys as well as previously-supported MD5 and SHA-1 keys.</p> <p>New/modified screens: System ⚙️ > Configuration > Time Synchronization</p>
Subject Alternative Name (SAN).	6.6	Any	<p>When creating an HTTPS certificate for the FMC, you can specify SAN fields. We recommend you use SAN if the certificate secures multiple domain names or IP addresses. For more information about SAN, see RFC 5280, section 4.2.1.6.</p> <p>New/modified screens: System ⚙️ > Configuration > HTTPS Certificate</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
HTTPS certificates.	6.6	Any	<p>The default HTTPS server certificate provided with the system now expires in 800 days. If your appliance uses a default certificate that was generated before you upgraded to Version 6.6, the certificate lifetime varies depending on the Firepower version being used when the certificate was generated. See Default HTTPS Server Certificates, on page 26 for more information.</p> <p>Supported platforms: Hardware FMCs.</p>
Secure NTP.	6.5	Any	<p>The FMC supports secure communications with NTP servers using SHA1 or MD5 symmetric key authentication.</p> <p>New/modified screens: System(⚙️) > Configuration > Time Synchronization</p>
Web analytics.	6.5	Any	<p>Web analytics data collection begins after you accept the EULA. As before, you can opt not to continue to share data. See Web Analytics, on page 74.</p>
Automatic CLI access for the FMC.	6.5	Any	<p>When you use SSH to log into the FMC, you automatically access the CLI. Although strongly discouraged, you can then use the CLI <code>expert</code> command to access the Linux shell.</p> <p>Note This feature deprecates the Version 6.3 ability to enable and disable CLI access for the FMC. As a consequence of deprecating this option, the virtual FMC no longer displays the System(⚙️) > Configuration > Console Configuration page, which still appears on physical FMCs.</p>
Configurable session limits for read-only and read/write access.	6.5	Any	<p>Added the Max Concurrent Sessions Allowed setting. This setting allows the administrator to specify the maximum number of sessions of a particular type (read-only or read/write) that can be open at the same time.</p> <p>Note Predefined user roles and custom user roles that the system considers read-only for the purposes of concurrent session limits, are labeled with (Read Only) in the role name on System(⚙️) > Users > Users and System(⚙️) > Users > User Roles. If a user role does not contain (Read Only) in the role name, the system considers the role to be read/write.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System(⚙️) > Configuration > User Configuration • System(⚙️) > Users > User Roles

Feature	Minimum Management Center	Minimum Threat Defense	Details
Ability to disable Duplicate Address Detection (DAD) on management interfaces.	6.4	Any	<p>When you enable IPv6, you can disable DAD. You might want to disable DAD because the use of DAD opens up the possibility of denial of service attacks. If you disable this setting, you need check manually that this interface is not using an already-assigned address.</p> <p>New/modified screens: System ⚙️ > Configuration > Management Interfaces > Interfaces > Edit Interface > IPv6 DAD</p> <p>Supported platforms: FMC</p>
Ability to disable ICMPv6 Echo Reply and Destination Unreachable messages on management interfaces.	6.4	Any	<p>When you enable IPv6, you can now disable ICMPv6 Echo Reply and Destination Unreachable messages. You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes.</p> <p>New/modified screens: System ⚙️ > Management Interfaces > ICMPv6</p> <p>New/modified commands: configure network ipv6 destination-unreachable, configure network ipv6 echo-reply</p> <p>Supported platforms: FMC (web interface only), FTD (CLI only)</p>
Global User Configuration Settings.	6.3	Any	<p>Added the Track Successful Logins setting. The system can track the number of successful logins each FMC account has performed within a selected number of days. When this feature is enabled, on log in users see a message reporting how many times they have successfully logged in to the system in the past configured number of days. (Applies to web interface as well as shell/CLI access.)</p> <p>Added the Password Reuse Limit setting. The system can track the password history for each account for a configurable number of previous passwords. The system prevents all users from re-using passwords that appear in that history. (Applies to web interface as well as shell/CLI access.)</p> <p>Added the Max Number of Login Failures and Set Time in Minutes to Temporarily Lockout Users settings. These allow the administrator to limit the number of times in a row a user can enter incorrect web interface login credentials before the system temporarily blocks the account for a configurable period of time.</p> <p>New/modified screens: System ⚙️ > Configuration > User Configuration</p> <p>Supported platforms: FMC</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
HTTPS Certificates.	6.3	Any	<p>The default HTTPS server certificate provided with the system now expires in three years. If your appliance uses a default server certificate that was generated before you upgraded to Version 6.3, the server certificate will expire 20 years from when it was first generated. If you are using the default HTTPS server certificate the system now provides the ability to renew it.</p> <p>New/modified screens: System(⚙️) > Configuration > HTTPS Certificate > Renew HTTPS Certificate</p> <p>Supported platforms: FMC</p>
Ability to enable and disable CLI access for the FMC.	6.3	Any	<p>There is a new check box available to administrators in FMC web interface: Enable CLI Access on the System(⚙️) > Configuration > Console Configuration.</p> <ul style="list-style-type: none"> • Checked: Logging into the FMC using SSH accesses the CLI. • Unchecked: Logging into FMC using SSH accesses the Linux shell. This is the default state for fresh Version 6.3 installations as well as upgrades to Version 6.3 from a previous release. <p>Previous to Version 6.3, there was only one setting on the Console Configuration page, and it applied to physical devices only. So the Console Configuration page was not available on virtual FMCs. With the addition of this new option, the Console Configuration page now appears on virtual FMCs as well as physical. However, for virtual FMCs, this check box is the only thing that appears on the page.</p> <p>Supported platforms: FMC</p>