



System Configuration

This chapter explains how to configure system configuration settings on the Cloud-Delivered Firewall Management Center.

- [Requirements and Prerequisites for the System Configuration, on page 1](#)
- [Manage the Cloud-Delivered Firewall Management Center System Configuration, on page 1](#)
- [Access Control Preferences, on page 2](#)
- [Audit Log, on page 3](#)
- [Audit Log Certificate, on page 6](#)
- [Change Reconciliation, on page 11](#)
- [Email Notification, on page 13](#)
- [Intrusion Policy Preferences, on page 13](#)
- [Network Analysis Policy Preferences, on page 14](#)

Requirements and Prerequisites for the System Configuration

Model support

Supported domains

Global

User roles

Admin

Manage the Cloud-Delivered Firewall Management Center System Configuration

The system configuration identifies basic settings for the Cloud-Delivered Firewall Management Center.

Procedure

-
- Step 1** Choose **System** (⚙️) > **Configuration**.
- Step 2** Use the navigation panel to choose configurations to change.
-

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.

Object Optimization

When you deploy rule policies to a firewall device, you can configure the Cloud-Delivered Firewall Management Center to evaluate and optimize the network/host policy objects that you use in the rules when it creates the associated network object groups on the device. Optimization merges adjacent networks and removes redundant network entries. This reduces the runtime access list data structures and the size of the configuration, which can be beneficial to some firewall devices that are memory-constrained.



Note Object optimization applies to objects created by the Cloud-Delivered Firewall Management Center only. These are objects created if you directly add IP addresses to an access control rule, rather than using your own network objects. User-defined network objects are not changed.

For example, consider a network/host object that contains the following entries and that is used in an access rule:

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

When optimization is enabled, when you deploy the policy, the resulting object group configuration is generated:

```
object-group network test
description (Optimized by management center)
network-object 10.1.1.0 255.255.255.252
network-object 192.168.1.0 255.255.255.0
```

When optimization is disabled, the group configuration would be as follows:

```
object-group network test
```

```
network-object 192.168.1.0 255.255.255.0
network-object 192.168.1.23 255.255.255.255
network-object 10.1.1.0 255.255.255.255
network-object 10.1.1.1 255.255.255.255
network-object 10.1.1.2 255.255.255.254
```

This optimization does not change the definition of the network/host object, nor does it create a new network/host policy object. If a network object-group contains another network, host object, or object-groups, the objects are not combined. Instead, each network object-group is optimized separately. Also, only inline values of network object-groups are being modified as part of the optimization process during a deployment.



Important The optimizations occur on the *managed device* on the *first deploy* after the feature is enabled on the Cloud-Delivered Firewall Management Center. 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. 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.

This feature is enabled by default. To disable it, contact Cisco TAC.

Audit Log

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

- Use the web interface: .
 - 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 4](#).
- Stream audit log messages to an HTTP server: [Stream Audit Logs to an HTTP Server, on page 5](#).

Streaming audit log data to an external server allows you to conserve space on the Cloud-Delivered Firewall 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 6](#).

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.

Streaming Configuration Changes to Syslog

You can stream configuration changes as part of audit log data to syslog by specifying the configuration data format and the hosts. The Cloud-Delivered Firewall Management Center supports backup and restore of the audit configuration log.

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 Cloud-Delivered Firewall 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 Cloud-Delivered Firewall 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, 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
Send Configuration Changes	To include configuration changes syslog in the audit log streaming, from the drop-down, select the relevant options: <ul style="list-style-type: none"> • JSON—the syslog includes detailed differences in the configuration changes. • API—the syslog includes API to retrieve the detailed differences in the configuration changes. • None—to have all other audit logs except details of the configuration changes.
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. <p>Note You can specify multiple syslog hosts, only when TLS is disabled for the Audit Server Certificate.</p>

Option	Description
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 Cloud-Delivered Firewall 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.

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 Cloud-Delivered Firewall 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 Cloud-Delivered Firewall Management Center. Use the local system configuration: [Obtain a Signed Audit Log Client Certificate for the Cloud-Delivered Firewall Management Center, on page 7](#) and [Import an Audit Log Client Certificate into the Cloud-Delivered Firewall Management Center, on page 9](#).

Server Certificates (Optional)

For additional security, we recommend you require mutual authentication between the Cloud-Delivered Firewall 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 Cloud-Delivered Firewall Management Center web interface.

Use the local system configuration: [Require Valid Audit Log Server Certificates, on page 9](#).

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 Cloud-Delivered Firewall Management Center and the server. You must generate a unique client certificate for each appliance you want to audit.

Procedure

- Step 1** Obtain and install a signed client certificate on the Cloud-Delivered Firewall Management Center:
- a) [Obtain a Signed Audit Log Client Certificate for the Cloud-Delivered Firewall Management Center, on page 7](#):
Generate a Certificate Signing Request (CSR) from the Cloud-Delivered Firewall 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 Cloud-Delivered Firewall 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 Cloud-Delivered Firewall Management Center. See [Import an Audit Log Client Certificate into the Cloud-Delivered Firewall Management Center, on page 9](#).
- Step 2** Configure the communication channel with the server to use Transport Layer Security (TLS) and enable mutual authentication.
- Step 3** Configure audit log streaming if you have not yet done so.
See [Stream Audit Logs to Syslog, on page 4](#) or [Stream Audit Logs to an HTTP Server, on page 5](#).
-

Obtain a Signed Audit Log Client Certificate for the Cloud-Delivered Firewall 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 Cloud-Delivered Firewall Management Center, on page 9](#).

Import an Audit Log Client Certificate into the Cloud-Delivered Firewall Management Center

Before you begin

- [Obtain a Signed Audit Log Client Certificate for the Cloud-Delivered Firewall Management Center, on page 7.](#)
- Make sure you are importing the signed certificate for the correct Cloud-Delivered Firewall 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 Cloud-Delivered Firewall 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.

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 6.](#)

- Obtain and import the client certificate following the steps in [Securely Stream Audit Logs, on page 7](#) and the topics referenced in that procedure.

Procedure

Step 1 On the Cloud-Delivered Firewall 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 (Cloud-Delivered Firewall 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 (Cloud-Delivered Firewall 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. .

View the Audit Log Client Certificate on the Cloud-Delivered Firewall Management Center

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

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

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**.

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 Cloud-Delivered Firewall 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 Firewall Threat Defense interfaces and routing settings.

Email Notification

You cannot configure a mail host. The mail relay host is hardcoded to be used from a static host. It is set to email-smtp.us-west-2.amazonaws.com with authorization. For notifications, the email sender is set to cdo-alert@cisco.com

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 Cloud-Delivered Firewall 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 Cloud-Delivered Firewall Management Center menu bar, click **Notifications** (message center), and then click **Tasks** to view the notifications. This option is enabled by default.
- **Talos Threat Hunting Telemetry:** Check this check box to allow Cisco Talos to conduct threat hunting and to gather critical security intelligence. When enabled, a special set of threat-hunting rules is added to the global intrusion policy. Although the threat-hunting rules are processed like regular IPS rules, the events that the Talos threat hunting rules generate do not appear in the Cloud-Delivered Firewall Management Center's event tables. Instead, the events are sent to Talos as telemetry for analysis. This option is enabled by default.

Note

- If you send firewall events to the Cisco Security Cloud via a direct connection by registering your Cloud-Delivered Firewall Management Center to the cloud tenancy using your Security Cloud

Control account, your Security Cloud Control account must have a Security Analytics and Logging license in order to forward threat-hunting rule events to Talos.

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.