

System Configuration

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

- Meet requirements and prerequisites for the system configuration, on page 1
- Manage the Cloud-Delivered Firewall Management Center system configuration, on page 2
- Configure access control preferences, on page 2
- Audit logs, on page 4
- Audit log certificates, on page 8
- Change reconciliation, on page 14
- Email notifications, on page 16
- Intrusion policy preferences, on page 16
- Network analysis policy preferences, on page 18

Meet requirements and prerequisites for the system configuration

This reference lists the requirements and prerequisites for the system configuration, including supported models, domains, and user roles.

Model support

Firewall Management Center

Supported domains

Global

User roles

Admin

Manage the Cloud-Delivered Firewall Management Center system configuration

Configure the system to establish and maintain the essential settings for the Cloud-Delivered Firewall Management Center. Ensure that these settings align with organizational requirements.

The system configuration identifies basic settings for the Cloud-Delivered Firewall Management Center. Use this task when you need to review or update the fundamental configuration options for the management center.

Before you begin

Access to the Cloud-Delivered Firewall Management Center interface may be required. Follow these steps to manage the Cloud-Delivered Firewall Management Center system configuration.

Procedure

Step 1 Choose **Administration** > **Configuration**.

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

When you complete the steps, the basic settings for the Cloud-Delivered Firewall Management Center will update to maintain proper system operation.

What to do next

Verify that the configuration changes are applied and the system is functioning as expected.

Configure access control preferences

Configure access control preferences to track access control rule changes, optimize object groups, validate access rule capacity, and define default connection logging for new rules. Access control preferences are configured at the Cloud-Delivered Firewall Management Center level and apply to all access control policies on the Cloud-Delivered Firewall Management Center. Default logging settings apply to new rules. You can override these settings for individual rules.

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

Configure object optimization to evaluate and optimize network or host policy objects that are used in rules. The system then creates associated network object groups on the device. For more information, refer to Object-group optimization.

Procedure

Step 1 Choose **Administration** > **Configuration** > **Access Control Preferences**.

Step 2 From the **Comments on rule change** list, choose an option:

- **Disabled**: Disables comments for access control rule changes.
- **Optional**: Allows users to optionally add a comment when they change an access control rule.
- **Required**: Requires users to add a comment when they change an access control rule.

Step 3 From the **Object-group optimization** list, choose an option:

- **Enabled**: Enables object-group optimization. The setting takes effect after deployment.
- **Disabled**: Disables object-group optimization.



Warning For the first deployment to a threat defense device after you enable object-group optimization, the device can take several minutes to an hour to reevaluate the policy configuration and optimize object groups. CPU utilization on the device can also increase. Schedule the deployment during a low-traffic period or a maintenance window.

Step 4 From the **Access Rule Capacity Validation** list, choose an option:

- **Enabled**: Calculates access rule expansion when you open or edit an access control policy. The Cloud-Delivered Firewall Management Center displays policy-level and rule-level warnings for rules that can expand into a large number of access control entries. For more information, refer to the *Access control rule expansion* in *Cisco Secure Firewall Management Center Device Configuration Guide*.
- **Disabled**: Disables access rule capacity validation when you open or edit an access control policy.

Step 5 From the **Access Rule Deploy Validation** list, choose an option:

- **Enabled**: Validates access rule capacity before deploying a changed access control policy. The Cloud-Delivered Firewall Management Center uses current device data and the enabled access control and prefilter rules to allow the deployment.
- **Disabled**: Disables access rule deploy validation during deployment.

Step 6 Under **Default logging settings**, configure the default logging options for new access control rules:

a) Check the **Enable logging by default for new rules** check box to enable default logging for new rules.
b) Expand **Advanced options**.
c) Specify your logging preferences for the **Block actions** and **Allow, Trust, and Interactive Block actions**.

To optimize performance, log either the beginning or the end of any connection, but not both.



Note New rules use the default logging settings configured here. If you change the rule action from the access control policy rule editor, the logging setting resets to the defaults for that action.

Enabling this feature does not change the logging settings of existing access control rules.

d) (Optional.) To restore the system-provided default logging settings, click the **Reset logging settings** button.

Step 7 Click **Save**.

What to do next

Deploy the access control policies for object-group optimization to take effect.

Audit logs

An audit log is a security record that

- records user activity in read-only logs,
- allows review, sorting, filtering, deletion, and reporting of audit information, and
- supports streaming audit log messages to external servers such as syslog and HTTP servers.

Audit log review and streaming options

You can review audit log data in several ways:

- Use the web interface: .

  Audit logs appear in a standard event view. In this view, you can view, sort, and filter audit log messages based on any item. You can also delete audit information, generate reports, and view detailed reports of user changes.

- 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 6.

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; refer to Audit log certificates, on page 8.

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

Configure audit log streaming to syslog servers to ensure centralized monitoring and compliance tracking for your system. Enable external logging of configuration changes and security events.

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.

This task is relevant when you need to send audit logs from your management center to an external syslog server for compliance or operational monitoring. Use this procedure when integrating with centralized log management solutions.

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 syslog server connectivity. By default, the system uses port 514/UDP to stream audit logs. To secure the channel, manually configure port 1470 for TCP.

Follow these steps to stream audit logs to a syslog server:

Procedure

Step 1 Choose **Administration** > **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: • 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. **Note** You can specify multiple syslog hosts, only when TLS is disabled for the Audit Server Certificate.

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**.

After you complete this task, audit logs are sent from the management center to the specified syslog server, allowing you to monitor and review system activity externally.

What to do next

Verify that the syslog server is receiving audit log messages as expected. Check for log entries corresponding to configuration changes or security events.

Stream audit logs to an HTTP server

Stream audit logs from the device to an HTTP server to centralize log management and support compliance requirements.

Use this task to forward audit logs from your device to an external HTTP server for monitoring, analysis, or compliance.

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.

Follow these steps to stream audit logs to an HTTP server.

Procedure

Step 1 Choose **Administration** > **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**.

When you complete this task, the device sends audit logs to the specified HTTP server. Centralized monitoring and record-keeping become possible.

Audit log certificates

An audit log certificate is a security credential that

- secures communications between the Cloud-Delivered Firewall Management Center and a trusted audit log server,
- enables authentication and encryption using Transport Layer Security (TLS), and
- supports mutual authentication and certificate revocation checks for enhanced security.

Client certificates

Client certificates are required to secure communications between the Cloud-Delivered Firewall Management Center and the audit log server.

- Generate a certificate signing request (CSR). Submit it to a Certificate Authority (CA) for signing. 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 10 and Import an audit log client certificate into the Cloud-Delivered Firewall Management Center, on page 11.

Server certificates

Server certificates are optional and provide additional security through mutual authentication.

- Require mutual authentication between the Cloud-Delivered Firewall Management Center and the audit log server by loading 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. These are the same CRLs used 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 12.

Audit log certificate example

For example, a signed client certificate imported onto the Cloud-Delivered Firewall Management Center enables secure TLS communication with an audit log server, ensuring log integrity and confidentiality.

Non-compliant audit log certificate

A certificate that is not signed by a trusted Certificate Authority or is listed in a certificate revocation list (CRL) cannot be used to stream audit logs securely.

Audit log certificate analogy

An audit log certificate is like a passport for secure communication, verifying identity and granting access between the management center and the audit log server.

Secure audit log streaming

Configure secure audit log streaming to ensure that audit logs are transmitted safely between the Cloud-Delivered Firewall Management Center and a trusted server.

When you stream the audit log to a trusted HTTP server or syslog server, 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. Mutual authentication requires the client certificate to be signed by the same CA as the server certificate. For more considerations on client and server certificate requirements, refer to Audit log certificates, on page 8.

Before you begin

Refer to ramifications of requiring client and server certificates at Audit log certificates, on page 8. Ensure you have access to a recognized certificate authority (CA) for signing client certificates.

Follow these steps to secure audit log streaming.

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 10:

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, ensure the client certificate is signed by the same CA that signed the server certificate.

b) After you receive the signed certificate from the certificate authority, import it into the Cloud-Delivered Firewall Management Center. Refer to Import an audit log client certificate into the Cloud-Delivered Firewall Management Center, on page 11.

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

Step 3 If you have not yet configured audit log streaming, do so now.

Refer to Stream audit logs to syslog, on page 4 or Stream audit logs to an HTTP server, on page 6.

Audit logs are securely streamed to the trusted server using TLS, with mutual authentication enabled. The Cloud-Delivered Firewall Management Center and the server verify each other's certificates, ensuring secure transmission and integrity of audit log data.

What to do next

Monitor the audit log streaming status and verify certificate validity periodically. Renew client and server certificates before expiration to maintain secure log streaming.

Obtain a signed audit log client certificate for the Cloud-Delivered Firewall Management Center

Obtain a signed audit log client certificate for the Cloud-Delivered Firewall Management Center. This certificate enables secure communication between the appliance and the audit log server. It ensures that the server can authenticate audit log data and that the data is transmitted securely.

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

Perform this task on the active appliance to generate a certificate signing request for audit log client authentication. Do not perform this task on a standby appliance in a high availability setup.

Before you begin

Keep this 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.

Follow these steps to obtain a signed audit log client certificate for the Cloud-Delivered Firewall Management Center:

Procedure

Step 1 Choose **Administration** > **Configuration** and click **Audit Log Certificate**.

Step 2 Click **Generate New CSR**.

Step 3 Enter a country code in the **Country Name (two-letter code)** field.

Step 4 Enter a state or province postal abbreviation in the **State or Province** field.

Step 5 Enter a **Locality or City**, an **Organization** name, and an **Organizational Unit (Department)** name.

Step 6 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 7 Click **Generate** and then open a new blank file with a text editor.

Step 8 Copy the block of text from the certificate request, including the `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST` lines. Paste this information into a blank text file.

Step 9 Save the file as *`clientname`*`.CSR`. Replace *`clientname`* with the appliance name where you plan to use the certificate. Click **Close**.

After completing these steps, you will have a certificate signing request (CSR) file that can be submitted to a trusted certificate authority. After it is signed, you can import the certificate to the appliance for secure audit log streaming.

What to do next

- Submit the certificate signing request to the certificate authority you selected, according to the guidelines in the 'Before You Begin' section.
- When you receive the signed certificate, import it to the appliance; refer to Import an audit log client certificate into the Cloud-Delivered Firewall Management Center, on page 11.

Import an audit log client certificate into the Cloud-Delivered Firewall Management Center

Importing an audit log client certificate enables secure communication between the Secure Firewall Management Center and external systems during audit log transmission. This task verifies that you import the correct signed certificate and any necessary intermediate certificates for secure operations.

In a Secure Firewall Management Center high availability setup, you must use the active peer when importing the audit log client certificate. This procedure is relevant when configuring audit log security or after obtaining a new signed client certificate.

Before you begin

- Obtain a signed audit log client certificate for the Cloud-Delivered Firewall Management Center, on page 10.
- Make sure you are importing the signed certificate for the correct Cloud-Delivered Firewall Management Center.
- If the signing authority requires an intermediate CA, ensure you provide the certificate chain. The same CA must sign both the client certificate and the intermediate certificates.

Follow these steps to import an audit log client certificate into the Secure Firewall Management Center.

Procedure

Step 1 On the Cloud-Delivered Firewall Management Center, choose **Administration** > **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**.

The audit log client certificate and any required intermediate certificates are successfully imported into the Secure Firewall Management Center.

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. Refer to Audit log certificates, on page 8.
- Obtain and import the client certificate following the steps in Secure audit log streaming, on page 9 and the topics referenced in that procedure.

Procedure

Step 1 On the Cloud-Delivered Firewall Management Center , choose **Administration** > **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, these 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, add the issuing CA before adding the signing CA from the subordinate CA (Root CA).

Step 4 If you do not want the client to authenticate itself against the server, but wish to accept the server certificate when the certificate is issued by the same CA (not recommended), complete these steps.

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, these 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 this 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.

When you enable fetching of the CRL, the client creates a scheduled task to regularly update (download) the CRL or CRLs. The CRLs are used for server certificate verification. Verification fails if a CRL from the CA specifies that the server certificate has been revoked.

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. Refer to Schedule certificate revocation list (CRL) updates.

View the audit log client certificate on the Cloud-Delivered Firewall Management Center

View the audit log client certificate to confirm its presence and details on the appliance you are logged in to. This helps ensure that audit log operations are secured with the correct certificate.

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

Before you begin

Follow these steps to view the audit log client certificate on the appliance:

Procedure

Step 1 Choose **Administration** > **Configuration**.

Step 2 Click **Audit Log Certificate**.

The appliance you are logged in to displays the audit log client certificate details. For high availability pairs, only the active peer shows the certificate.

Change reconciliation

A change reconciliation report is a configuration monitoring tool that

- captures snapshots whenever a user saves changes to the system configuration,
- combines information from these snapshots to present a clear summary of recent system changes, and
- provides a detailed report of changes made over the past 24 hours through email.

User change summaries

The change reconciliation report displays both the previous value for each configuration and the value after changes.

Users can view summaries of each distinct change in chronological order, beginning with the most recent.

- Lists both previous and updated values for each configuration.
- Summarizes multiple changes to the same configuration.
- Orders changes chronologically, starting with the most recent.

Change reconciliation report example

An example change reconciliation report includes a User section that lists configuration changes, showing both the previous and updated values for each item.

Non-reconciled changes

Changes made without reconciliation are not summarized or tracked in a report, making it difficult to monitor user activity.

Change reconciliation as a transaction log

Change reconciliation is similar to a transaction log, where each modification is recorded and summarized for review.

Configure change reconciliation

Configure change reconciliation to enable the system to generate and send daily reports of configuration changes, supporting audit and compliance requirements. This helps administrators monitor and review all changes made to the system within a 24-hour period.

Use this task when you need to track and review configuration changes made to your system for security, compliance, or operational awareness.

Change reconciliation is especially useful in environments where multiple administrators make changes or where audit trails are required for regulatory purposes. Perform this configuration after setting up your email server to ensure reports are delivered successfully.

Procedure

Step 1 Choose **Administration** > **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**.

After you complete this task, the system will automatically generate and email daily reports of all configuration changes, allowing you to monitor and review system modifications for compliance and troubleshooting.

Change reconciliation options

The change reconciliation options control whether the system includes records of policy changes and the full change history in the change reconciliation report. These options determine the scope and detail of reported changes.

The **Include Policy Configuration** option controls whether the system includes records of policy changes in the change reconciliation report. It 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 only on Cloud-Delivered Firewall Management Centers.

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 notifications

An email notification is a system alert mechanism that enables automated emailing of event-based, status, change reconciliation, and data-pruning reports.

Email notification restrictions for static mail relay hosts

You cannot configure a mail host. TThe mail relay host is hardcoded to 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

An intrusion policy preference is a configuration option that

- enables monitoring of critical policies,
- tracks changes to those policies, and
- supports management of policy settings in a deployment.

Set intrusion policy preferences

Configure intrusion policy preferences to manage how policy changes are tracked, logged, and monitored for security intelligence. You can enable or disable comments on policy changes, audit logging, user overrides for deleted Snort 3 rules, and Talos Threat Hunting Telemetry.

This task is relevant when you need to control how intrusion policy changes are documented, audited, and monitored for advanced threat detection and compliance.

Use this configuration to ensure that policy modifications are properly tracked and that security events are sent to Cisco Talos for analysis when required. Perform this task during initial setup or when updating security and compliance requirements for your deployment.

Before you begin

Follow these steps to set intrusion policy preferences:

Procedure

Step 1 Choose **Administration** > **Configuration**.

Step 2 Click **Intrusion Policy Preferences**.

Step 3 You have these 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 you enable this feature, 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). 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, events generated by these rules do not appear in the Cloud-Delivered Firewall Management Center's event tables. These 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.

After completing this task, your intrusion policy preferences are set according to your selections. Policy changes are tracked, logged, and, if enabled, threat-hunting telemetry is sent to Cisco Talos for analysis.

Network analysis policy preferences

Network analysis policy preferences are configuration settings that enable tracking and documentation of policy modifications within the system.

Policy Change Tracking Options

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.