



Event Analysis Using External Tools

- [Cisco Cloud Event Settings, on page 1](#)
- [Event Investigation Using Web-Based Resources, on page 5](#)
- [Configure Cross-Launch Links for Secure Network Analytics, on page 8](#)
- [About Sending Syslog Messages for Security Events, on page 9](#)
- [eStreamer Server Streaming, on page 23](#)
- [Event Analysis in Splunk, on page 27](#)
- [Splunk Integration: Send Events Directly from Management Center, on page 27](#)
- [Guidelines and Limitations for Splunk Integration, on page 27](#)
- [Configure Splunk in Secure Firewall Management Center, on page 28](#)
- [Configure Secure Firewall App in Splunk, on page 33](#)
- [Event Analysis in IBM QRadar, on page 34](#)
- [History for Analyzing Event Data Using External Tools, on page 34](#)

Cisco Cloud Event Settings

Sending firewall events to the cloud allows you to use external tools to investigate the firewall incidents. The devices send firewall events to the Security Services Exchange (SSE), from where they can be forwarded to various cloud services to unify visibility and enhance your threat investigations.

To allow your devices to send firewall events to Security Cloud Control, you must either register the Firewall Management Center with the smart license (**Administration > Licenses > Smart Licenses**) or enable Security Cloud Control integration. Security Cloud Control integration associates the Firewall Management Center with your Security Cloud Control account and brings your secure firewall deployment onboard to the Cisco cloud tenancy, allowing it to connect to Cisco's integrated security cloud services.

For more information about integrating the Firewall Management Center with Security Cloud Control, see [Enable Security Cloud Control Integration](#).

Security Services Exchange Event Consolidation

The Security Services Exchange does not display the complete list of events from the Firewall Management Center. Instead, it correlates and consolidates events, presenting only unique events. This approach reduces redundancy of events and enhances clarity. The current categorization parameters used for this consolidation are detailed as follows:

- For identifying duplication of intrusion events, the following elements are considered: Initiator IP, Initiator IP, SID, and GID.

- For identifying duplication of connection events and security-related connection events, the following elements are considered: Initiator IP, Initiator IP, and Security Intelligence Category.
- For identifying duplication of file and malware events, all elements except Event Second are considered.

Enable Sending Events to the Security Cloud Control

Configure your Firewall Management Center to enable the managed Firewall Threat Defense devices send events directly to Security Cloud Control. The cloud region and event types that you configure in the **Security Cloud Control Integration** page can be used for multiple integrations when applicable and enabled.

Before you begin

- Determine the Cisco regional cloud that you want to use for sending firewall events. While choosing a regional cloud, keep in mind that:
 - The regional cloud you select is also used for the Cisco Support Diagnostics and Cisco Support Network capabilities. This setting also governs the cloud region for the Secure Network Analytics cloud using Security Analytics and Logging (SaaS).
 - You cannot merge or aggregate data in different regional clouds. To aggregate data from multiple regions, devices in all the regions must send data to the same regional cloud.
- Ensure that you register the management center with Smart License (**Administration** > **Licenses** > **Smart Licenses**) or enable Security Cloud Control integration to allow your devices to send firewall events to Cisco cloud.



Note

If you were already sending events to Security Cloud Control using a SecureX subscription prior to Version 7.6, you can continue to send events to Security Cloud Control services such as Cisco XDR. However, if you now register your 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 to forward events to Security Cloud Control services such as Cisco XDR.

- In the Firewall Management Center:
 - Go to the **Administration** > **Configuration** page and give your Firewall Management Center a unique name to clearly identify it in the **Devices** list in the cloud.
 - Add your Firewall Threat Defense devices to the Firewall Management Center, assign licenses to them, and ensure that the system is working correctly. Ensure that you have created the necessary policies and that the generated events are displayed as expected in the Firewall Management Center UI under the **Analysis** menu.
- Ensure that you have your Security Cloud Sign-On credentials and can sign in to the regional cloud in which your account was created.
For more information on regional cloud URLs and supported device versions, see [Regional Clouds](#).
- Ensure that you link your smart account or the Security Cloud Control tenant to your SSE account.

- If you are currently sending events to the cloud using syslog, disable it to avoid duplication.

Procedure

- Step 1** Determine the regional cloud that you want to use for sending firewall events. For more information about choosing a regional cloud, refer to [Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide](#).

Note

If Security Cloud Control integration is enabled and the Firewall Management Center is registered to the selected regional cloud, changing the regional cloud disables Security Cloud Control integration. You can enable the Security Cloud Control integration again after changing the regional cloud.

- Step 2** In your Firewall Management Center, choose **Integrations > Security Cloud Control**.

- Step 3** Choose a regional cloud from the **Current Region** drop-down list.

- Step 4** Check the **Send events to the cloud** check box to enable the cloud event configuration.

- Step 5** Select the event types that you want to send to the cloud.

Note

Events that you send to the cloud can be used for multiple integrations, as shown in the this table.

Integration	Supported Event Options	Notes
Cisco Security Analytics and Logging (SaaS)	All	High-priority connection events include: <ul style="list-style-type: none"> • Security-related connection events • Connection events related to file and malware events • Connection events related to intrusion events
Cisco Extended Detection and Response (Cisco XDR)	Depending on your version: <ul style="list-style-type: none"> • Security-related connection events • Intrusion events • File and malware events 	Even if you send all the connection events, Cisco XDR supports only security-related connection events. Note Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses required for Cisco Secure Firewall products. For more information, see Cisco XDR Licenses .

Note

- When you enable **Intrusion Events**, the Firewall Threat Defense device sends events along with the impact flag.
- When you enable **Intrusion Events**, the Firewall Threat Defense device sends the captured packet data to Security Cloud Control along with the intrusion events. Talos uses this packet data to analyze and eliminate false threats. This ensures focus on actual threats, enhancing the accuracy and efficiency of Talos' threat recommendations.
- If you enable **File and Malware Events**, in addition to the events sent from the Firewall Threat Defense devices, the Firewall Management Center sends retrospective events.

Step 6 Click **Save**.

Analyze Events Using Cisco XDR

Cisco Extended Detection and Response (Cisco XDR) is a cloud-based solution that unifies visibility by correlating detections across multiple telemetry sources, and enables security teams to detect, prioritize, and respond to the most sophisticated threats. Integrate Firewall Threat Defense with Cisco XDR to connect Cisco's integrated security portfolio and your firewall deployment for a consistent experience that unifies visibility, enables automation, and strengthens your security across network.

For more information about Cisco XDR, see [Cisco XDR Help Center](#).

**Important**

- Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses required for Cisco Secure Firewall products. For more information, see [Cisco XDR Licenses](#).
- If you were already sending events to the Security Cloud Control using a SecureX subscription before Version 7.6, you can continue to send events to Cisco XDR. However, if you now register your Firewall Management Center to the cloud tenancy using your Security Cloud Control account to send firewall events to Cisco XDR, your Security Cloud Control account must have a Security Analytics and Logging license to forward events to Cisco XDR.

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

**Note**

As of July 31, 2024, Cisco SecureX is phased out and no longer available. Cisco SecureX cannot be provisioned for users, and access to Cisco SecureX is not provided alongside Cisco Secure Firewall product purchases. Additionally, all existing Cisco SecureX environments are disabled, and all capabilities are made unavailable. If you are using Firefox, you should remove Cisco SecureX Ribbon browser extension. For more information, see the [Frequently Asked Questions](#).

Analyze and Respond to Threats Using Cisco XDR Automation

Enable this setting to allow the automated workflows created by Cisco Extended Detection and Response (Cisco XDR) users to interact with your Firewall Management Center resources.

Cisco XDR automation provides a no-to-low code approach for building automated workflows. You can design your own workflows with the drag-and-drop interface, and they can be set to run in response to different schedules and events. Cisco XDR automation helps you to rectify threats using automation and guided response recommendations across all relevant control points.

**Note**

Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses for Cisco Secure Firewall products. For more information, see [Cisco XDR Licenses](#).

For more information about the Cisco XDR automation capabilities, see the [Cisco XDR documentation](#).

Before you begin

Enable Cisco Security Cloud and register your management center to the cloud. See [Enable Security Cloud Control Integration](#).

Procedure

-
- | | |
|---------------|--|
| Step 1 | Click Integrations > Security Cloud Control . |
| Step 2 | Check the Enable Cisco XDR Automation check box. |
| Step 3 | Choose the Firewall Management Center user role that you want to assign to the Cisco XDR automation workflows.

The Access Admin role is set as the default, allowing access to access control policy and associated functionality in the Policies menu. |
| Step 4 | Click Save . |
-

Event Investigation Using Web-Based Resources

Use the contextual cross-launch feature to quickly find more information about potential threats in web-based resources outside of the Secure Firewall Management Center. For example, you might:

- Look up a suspicious source IP address in a Cisco or third-party cloud-hosted service that publishes information about known and suspected threats, or
- Look for past instances of a particular threat in your organization's historical logs, if your organization stores that data in a Security Information and Event Management (SIEM) application.
- Look for information about a particular file, including file trajectory information, if your organization has deployed Cisco Secure Endpoint.

When investigating an event, you can click directly from an event in the event viewer or dashboard in the Secure Firewall Management Center to the relevant information in the external resource. This lets you quickly gather context around a specific event based on its IP addresses, ports, protocol, domain, and/or SHA 256 hash.

For example, suppose you are looking at the Top Attackers dashboard widget and you want to find out more information about one of the source IP addresses listed. You want to see what information Talos publishes about this IP address, so you choose the "Talos IP" resource. The Talos web site opens to a page with information about this specific IP address.

You can choose from a set of pre-defined links to commonly used Cisco and third-party threat intelligence services, and add custom links to other web-based services, and to SIEMs or other products that have a web interface. Note that some resources may require an account or a product purchase.

About Managing Contextual Cross-Launch Resources

Manage external web-based resources using the **Events & Logs > + Show more > Advanced > Contextual Cross-Launch** page.

Exception: Manage cross-launch links to a Secure Network Analytics appliance following the procedure in [Configure Cross-Launch Links for Secure Network Analytics, on page 8](#).

Pre-defined resources offered by Cisco are marked with the Cisco logo. The remaining links are third-party resources.

You can disable or delete any resources that you do not need, or you can rename them, for example by prefixing a name with a lower-case "z" so the resource sorts to the bottom of the list. Disabling a cross-launch resource disables it for all users. You cannot reinstate deleted resources, but you can re-create them.

To add a resource, see [Add Contextual Cross-Launch Resources, on page 6](#).

Requirements for Custom Contextual Cross-Launch Resources

When adding custom contextual cross-launch resources:

- Resources must be accessible via web browser.
- Only http and https protocols are supported.
- Only GET requests are supported; POST requests are not.
- Encoding of variables in URLs is not supported. While IPv6 addresses may require colon separators to be encoded, most services do not require this encoding.
- Up to 100 resources can be configured, including pre-defined resources.
- You must be an Admin or Security Analyst user to create a cross launch, but you can also be a read-only Security Analyst to use them.

Add Contextual Cross-Launch Resources

You can add contextual cross-launch resources such as threat intelligence services and Security Information and Event Management (SIEM) tools.

In multidomain deployments, you can see and use resources in parent domains, but you can only create and edit resources in the current domain. The total number of resources across all domains is limited to 100.

Before you begin

- If you are adding links to a Secure Network Analytics appliance, check to see if the links you want already exist; most links are automatically created for you when you configure Security Analytics and Logging (On Premises).
- See [Requirements for Custom Contextual Cross-Launch Resources, on page 6](#).
- If needed for the resource you will link to, create or obtain an account and the credentials needed for access. Optionally, assign and distribute credentials for each user who needs access.
- Determine the syntax of the query link for the resource that you will link to:


Access the resource via browser and, using the documentation for that resource as needed, formulate the query link needed to search for a specific sample of the type of information you want your query link to find, such as an IP address.

Run the query, then copy the resulting URL from the browser's location bar.

For example, you might have the query URL

`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10.`

Procedure

-
- Step 1** Choose **Events & Logs** > **+ Show more** > **Advanced** > **Contextual Cross-Launch**.
- Step 2** Click **New Cross-launch**.
- In the form that appears, all fields marked with an asterisk require a value.
- Step 3** Enter a unique resource name.
- Step 4** Paste the working URL string from your resource into the **URL Template** field.
- Step 5** Replace the specific data (such as an IP address) in the query string with an appropriate variable: Position your cursor, then click a variable (for example, **ip**) once to insert the variable.
- In the example from the "Before You Begin" section above, the resulting URL might be `https://www.talosintelligence.com/reputation_center/lookup?search={ip}`. When the contextual cross-launch link is used, the `{ip}` variable in the URL will be replaced by the IP address that the user right-clicks on in the event viewer or dashboard.
- For a description of each variable, hover over the variable.
- You can create multiple contextual cross-launch links for a single tool or service, using different variables for each.
- Step 6** Click **Test with example data** () to test your link with example data.
- Step 7** Fix any problems.
- Step 8** Click **Save**.
-

Investigate Events Using Contextual Cross-Launch

Before you begin

If the resource you will access requires credentials, make sure you have those credentials.

Procedure

-
- Step 1** Navigate to one of the following pages in the Secure Firewall Management Center that shows events:
- A dashboard (**Insights & Reports** > **Dashboard**), or
 - An event viewer page (any menu option under the **Analysis** menu that includes a table of events.)
- Step 2** Right-click the event of interest and choose the contextual cross-launch resource to use.
- If necessary, scroll down in the context menu to see all available options.

The data type you right-click on determines the options you see; for example, if you right-click an IP address, you will only see contextual cross-launch options that are relevant to IP addresses.

For example, to get threat intelligence from Cisco Talos about a source IP address in the intrusion event, choose **Talos SrcIP** or **Talos IP**.

If a resource includes multiple variables, the option to choose that resource is available only for events that have a single possible value for each included variable.

The contextual cross-launch resource opens in a separate browser window.

It may take some time for the query to be processed, depending on the amount of data to be queried, speed of and demand on the resource, and so on.

Step 3 Sign in to the resource if necessary.

Configure Cross-Launch Links for Secure Network Analytics

You can cross-launch from event data in Firewall Threat Defense to related data in your Secure Network Analytics appliance. For more information about the Secure Network Analytics product, visit the [Cisco Security Analytics and Logging](#) product page.

For general information about contextual cross-launching, see [Investigate Events Using Contextual Cross-Launch, on page 7](#).

Use this procedure to configure a set of cross-launch links to your Secure Network Analytics appliance.



Note

- If you want to change these links later, return to this procedure; you cannot make changes directly on the contextual cross-launch listing page.
- You can manually create additional links to cross-launch into your Secure Network Analytics appliance using the procedure in [Add Contextual Cross-Launch Resources, on page 6](#), but those links remain independent of the auto-created resources and you must manage them manually.

Before you begin

- Ensure that a Secure Network Analytics appliance is available for use
- If your device sends events directly to Secure Network Analytics, disable syslog for those devices or assign them an access control policy without syslog configurations. This avoids duplicate events on the remote volume.
- Ensure you have these items:
 - Hostname or IP address of your manager.
 - Credentials for an account on your Secure Network Analytics appliance that has administrator privileges.

If you want to send Firewall Threat Defense data to your Secure Network Analytics appliance using Security Analytics and Logging (On Premises), see [Remote Data Storage on a Secure Network Analytics Appliance](#).

Procedure

-
- Step 1** Choose **Integrations** > + **Show more** > **Security Analytics & Logging**.
- Step 2** Click **Start** to begin configuring the Secure Network Analytics data store.
- To receive and store events, you need to deploy a Secure Network Analytics Flow Collector, a Secure Network Analytics data store, and a manager for reviewing and querying events.
- Step 3** Complete the wizard. For more information, see the Firewall Management Center Configuration section of [Cisco Security Analytics and Logging Firewall Event Integration Guide](#).
- Step 4** Choose **Events & Logs** > + **Show more** > **Advanced** > **Contextual Cross-Launch** to verify your new cross-launch links.
- If you want to make changes, return to this procedure; you cannot make changes directly on the contextual cross-launch listing page.
-

What to do next

Use your Secure Network Analytics credentials to cross-launch from an event into the Secure Network Analytics event viewer.

To cross launch from an event in the Firewall Management Center event viewer or dashboard, right-click a relevant event's table cell and choose the appropriate option.

Processing queries may take some time, depending on the amount of data, data transfer speed on the Secure Network Analytics Manager, and other factors.

About Sending Syslog Messages for Security Events

You can send data related to connection, security intelligence, intrusion, and file and malware events via syslog to a Security Information and Event Management (SIEM) tool or another external event storage and management solution.

These events are also sometimes referred to as Snort® events.



-
- Note** In version 7.2.1, syslog traffic was allowed to be forwarded using route lookup. This enabled the traffic to be forwarded regardless of the interface specified in the logging host configuration. However, in versions 7.2.5.1 and higher, the changes introduced in 7.2.1 were removed.
- Thus, from 7.2.5.1 and higher versions, the configuration specified in logging host configuration precedes over the route lookup and the syslog traffic is forwarded from the specified interface.
-

About Configuring the System to Send Security Event Data to Syslog

To find more about the platform settings that apply to syslog messages for security events, refer to *Threat Defense Platform Settings that Apply to Security Event Syslog Messages* in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

Note that if you make changes to syslog settings in any policy, you must redeploy for the changes to take effect.

Best Practices for Configuring Security Event Syslog Messaging

Device and Version	Configuration Location
All	If you will use syslog or store events externally, avoid special characters in object names such as policy and rule names. Object names should not contain special characters, such as commas, that the receiving application may use as separators.
Secure Firewall Threat Defense	<ol style="list-style-type: none"> Do the following to configure syslog in Firewall Threat Defense platform settings: <ol style="list-style-type: none"> Click Devices > Platform Settings. Edit the threat defense settings policy. In the left navigation pane, click Syslog. <p>See also <i>Threat Defense Platform Settings That Apply to Security Event Syslog Messages</i> in the Cisco Secure Firewall Management Center Device Configuration Guide.</p> In your access control policy Logging tab, opt to use the Firewall Threat Defense platform settings. (For intrusion events) Configure intrusion policies to use the settings in your access control policy Logging tab. (This is the default.) <p>Overriding any of these settings is not recommended.</p> <p>For essential details, see Send Security Event Syslog Messages from Firewall Threat Defense Devices, on page 10.</p>
All other devices	<ol style="list-style-type: none"> Create an alert response. Configure access control policy Logging to use the alert response. (For intrusion events) Configure syslog settings in intrusion policies. <p>For complete details, see Send Security Event Syslog Messages from Classic Devices, on page 13.</p>

Send Security Event Syslog Messages from Firewall Threat Defense Devices

This procedure documents the best practice configuration for sending syslog messages for security events (connection, Security Intelligence, intrusion, file, and malware events) from Firewall Threat Defense devices.



Note Many Firewall Threat Defense syslog settings are not applicable to security events. Configure only the options described in this procedure.

Before you begin

- In Secure Firewall Management Center, configure policies to generate security events and verify that the events you expect to see appear in the applicable tables under the Analysis menu.
- Gather the syslog server IP address, port, and protocol (UDP or TCP):
- Ensure that your devices can reach the syslog server(s).
- Confirm that the syslog server(s) can accept remote messages.
- For important information about connection logging, see the chapter on [Connection Logging](#).

Procedure

Step 1

Configure syslog settings for your Firewall Threat Defense device:

- Click **Devices > Platform Settings**.
- Edit** the platform settings policy associated with your Firewall Threat Defense device.
- In the left navigation pane, click **Syslog**.
- Click **Syslog Servers** and click **Add (+)** to enter server, protocol, interface, and related information.
If you have questions about options on this page, see [Cisco Secure Firewall Management Center Device Configuration Guide](#).
- Click **Syslog Settings** and configure the following settings:
 - **Enable timestamp on syslog messages**
 - **Timestamp Format**
 - **Enable syslog device ID**
- Click **Logging Setup**.
- On the **Basic Logging Settings**, select whether or not to **Send syslogs in EMBLEM format**.
- Click **Save**, to save your settings.

Step 2

Configure general logging settings for the access control policy (including file and malware logging):

- Click **Policies > Security policies > Access Control**.
- Edit the applicable access control policy.
- From the **More** drop-down, click **Logging**.
- Firewall Threat Defense 6.3 and later: Select **Use the syslog settings configured in the Threat Defense Platform Settings policy deployed on the device**.
- (Optional) Select a **Syslog Severity**.
- If you want to send file and malware events, select **Send Syslog messages for File and Malware events**.
- Click **Save**.

- Step 3** Enable logging for Security Intelligence events for the access control policy:
- In the same access control policy, click the **Security Intelligence** tab.
 - In each of the following locations, click **Logging** (📄) and enable beginning and end of connections and **Syslog Server**:
 - Beside **DNS Policy**.
 - In the **Block List** box, for **Networks** and for **URLs**.
 - Click **Save**.

- Step 4** Enable syslog logging for each rule in the access control policy:
- In the same access control policy, click **Access Control**, and then choose **Add Rule**.
 - Select a rule to edit.
 - Click the **Logging** tab in the rule.
 - Choose whether to log the beginning or end of connections, or both.
(Connection logging generates a lot of data; logging both beginning and end generates roughly double that much data. Not every connection can be logged both at beginning and end.)
 - If you want to log file events, select **Log Files**.
 - Enable **Syslog Server**.
 - Verify that the rule is "Using default syslog configuration in Access Control Logging."
 - Click **Confirm**.
 - Repeat for each rule in the policy.

- Step 5** If you send intrusion events:
- Navigate to the intrusion policy associated with your access control policy.
 - In your intrusion policy, from **Advanced Settings** drop-down menu, click **Syslog Alerting**, and then click **Enabled**.
 - If necessary, click **Edit**.
 - Enter options:

Option	Value
Logging Host	Unless you will send intrusion event syslog messages to a different syslog server than you will send other syslog messages, leave this blank to use the settings you have configured above.
Facility	This setting is applicable only if you specify a Logging Host on this page. For descriptions, see Syslog Alert Facilities .
Severity	This setting is applicable only if you specify a Logging Host on this page. For descriptions, see Syslog Severity Levels .

- Click **Back**.
- Click **Policy Information** in the left navigation pane.
- Click **Commit Changes**.

What to do next

- (Optional) Configure different logging settings for individual policies and rules.
See the applicable table rows in [Configuration Locations for Syslogs for Connection and Security Intelligence Events \(All Devices\)](#), on page 14.
These settings will require syslog alert responses, which are configured as described in [Creating a Syslog Alert Response](#). They do not use the platform settings you configured in this procedure.
- To configure security event syslog logging for Classic devices, see [Send Security Event Syslog Messages from Classic Devices](#), on page 13.
- If you are done making changes, deploy your changes to managed devices.

Send Security Event Syslog Messages from Classic Devices

Before you begin

- Configure policies to generate security events.
- Ensure that your devices can reach the syslog server(s).
- Confirm that the syslog server(s) can accept remote messages.
- For important information about connection logging, see the chapter on [Connection Logging](#).

Procedure

-
- Step 1** Configure an alert response for your Classic devices:
See [Creating a Syslog Alert Response](#).
- Step 2** Configure syslog settings in the access control policy:
- a) Click **Policies > Security policies > Access Control**.
 - b) Edit the applicable access control policy.
 - c) Click **Logging**.
 - d) Select **Send using specific syslog alert**.
 - e) Select the **Syslog Alert** you created above.
 - f) Click **Save**.
- Step 3** If you will send file and malware events:
- a) Select **Send Syslog messages for File and Malware events**.
 - b) Click **Save**.
- Step 4** If you will send intrusion events:
- a) Navigate to the intrusion policy associated with your access control policy.
 - b) In your intrusion policy, from **Advanced Settings** drop-down menu, click **Syslog Alerting**, and then click **Enabled**.
 - c) If necessary, click **Edit**
 - d) Enter options:

Option	Value
Logging Host	Unless you will send intrusion event syslog messages to a different syslog server than you will send other syslog messages, leave this blank to use the settings you have configured above.
Facility	This setting is applicable only if you specify a Logging Host on this page. See Syslog Alert Facilities .
Severity	This setting is applicable only if you specify a Logging Host on this page. See Syslog Severity Levels .

- e) Click **Back**.
- f) Click **Policy Information** in the left navigation pane.
- g) Click **Commit Changes**.

What to do next

- (Optional) Configure different logging settings for individual access control rules. See the applicable table rows in [Configuration Locations for Syslogs for Connection and Security Intelligence Events \(All Devices\)](#), on page 14. These settings will require syslog alert responses, which are configured as described in [Creating a Syslog Alert Response](#). They do not use the settings you configured above.
- To configure security event syslog logging for Firewall Threat Defense devices, see [Send Security Event Syslog Messages from Firewall Threat Defense Devices](#), on page 10.

Configuration Locations for Security Event Syslogs

These topics describe how to configure location for security event syslogs:

Configuration Locations for Syslogs for Connection and Security Intelligence Events (All Devices)

There are many places to configure logging settings. Use the table below to ensure that you set the options you need.



Important

- Pay careful attention when configuring syslog settings, especially when using inherited defaults from other configurations. Some options may NOT be available to all managed device models and software versions, as noted in the table below.
- For important information when configuring connection logging, see the chapter on [Connection Logging](#).

Configuration Location	Description and More Information
Devices > Platform Settings , Threat Defense Settings policy, Syslog	<p>This option applies only to Firewall Threat Defense devices.</p> <p>Settings you configure here can be specified in the Logging settings for an Access Control policy and then used or overridden in the remaining policies and rules in this table.</p> <p>See Cisco Secure Firewall Management Center Device Configuration Guide.</p>
Policies > Security policies > Access Control , <each policy>, Logging	<p>Settings you configure here are the default settings for syslogs for all connection and security intelligence events, unless you override the defaults in descendant policies and rules at the locations specified in the remaining rows of this table.</p> <p>Recommended setting for Firewall Threat Defense devices: Use Threat Defense Platform Settings. For information, see Cisco Secure Firewall Management Center Device Configuration Guide.</p> <p>Required setting for all other devices: Use a syslog alert.</p> <p>If you specify a syslog alert, see Creating a Syslog Alert Response.</p> <p>For more information about the settings on the Logging tab, see Cisco Secure Firewall Management Center Device Configuration Guide.</p>
Policies > Security policies > Access Control , <each policy>, Rules , Default Action row, Logging (📄)	<p>Logging settings for the default action associated with an access control policy.</p> <p>See information about logging in Cisco Secure Firewall Management Center Device Configuration Guide and Logging Connections with a Policy Default Action.</p>
Policies > Security policies > Access Control , <each policy>, Rules , <each rule>, Logging	<p>Logging settings for a particular rule in an access control policy.</p> <p>See information about logging in Cisco Secure Firewall Management Center Device Configuration Guide.</p>
Policies > Security policies > Access Control , <each policy>, Security Intelligence , Logging (📄)	<p>Logging settings for Security Intelligence Block lists.</p> <p>Click these buttons to configure:</p> <ul style="list-style-type: none"> • DNS Block List Logging Options • URL Block List Logging Options • Network Block List Logging Options (for IP addresses on the blocked list) <p>See Cisco Secure Firewall Management Center Device Configuration Guide</p>
Policies > Security policies > Decryption , <each policy>, Default Action row, Logging (📄)	<p>Logging settings for the default action associated with an SSL policy.</p> <p>See Logging Connections with a Policy Default Action.</p>

Configuration Locations for Syslogs for Intrusion Events (Firewall Threat Defense Devices)

Configuration Location	Description and More Information
Policies > Security policies > Decryption , <each policy>, <each rule>, Logging	Logging settings for SSL rules. See Cisco Secure Firewall Management Center Device Configuration Guide .
Policies > Security policies > Prefilter , <each policy>, Default Action row, Logging (📄)	Logging settings for the default action associated with a prefilter policy. See Logging Connections with a Policy Default Action .
Policies > Security policies > Prefilter , <each policy>, <each prefilter rule>, Logging	Logging settings for each prefilter rule in a prefilter policy. See Cisco Secure Firewall Management Center Device Configuration Guide
Policies > Security policies > Prefilter , <each policy>, <each tunnel rule>, Logging	Logging settings for each tunnel rule in a prefilter policy. See Cisco Secure Firewall Management Center Device Configuration Guide
Additional syslog settings for Firewall Threat Defense cluster configurations:	The Cisco Secure Firewall Management Center Device Configuration Guide has multiple references to syslog; search the chapter for "syslog."

Configuration Locations for Syslogs for Intrusion Events (Firewall Threat Defense Devices)

You can specify syslog settings for intrusion policies in various places and, optionally, inherit settings from the access control policy or the Threat Defense Platform Settings or both.

Configuration Location	Description and More Information
Devices > Platform Settings , Threat Defense Settings policy, Syslog	Syslog destinations that you configure here can be specified in the Logging tab of an access control policy which can be the default for an intrusion policy. See Cisco Secure Firewall Management Center Device Configuration Guide .
Policies > Security policies > Access Control , <each policy>, Logging	Default setting for syslog destination for intrusion events, if the intrusion policy does not specify other logging hosts. See Cisco Secure Firewall Management Center Device Configuration Guide .

Configuration Location	Description and More Information
Policies > Security policies > Intrusion , <each policy>, Advanced Settings , enable Syslog Alerting , click Edit	To specify syslog collectors other than the destinations specified in the access control policy Logging tab, and to specify facility and severity, see Configuring Syslog Alerting for Intrusion Events . If you want to use the Severity or Facility or both as configured in the intrusion policy, you must also configure the logging hosts in the policy. If you use the logging hosts specified in the access control policy, the severity and facility specified in the intrusion policy will not be used.
Policies > Security policies > Intrusion > Logging > IPS settings	If you want to send Syslog messages for IPS events. Default syslog settings configured are used for syslog destinations for IPS events.

Configuration Locations for Syslogs for Intrusion Events (Devices Other than Firewall Threat Defense)

- (Default) Access control policy [Cisco Secure Firewall Management Center Device Configuration Guide](#), IF you specify a syslog alert (See [Creating a Syslog Alert Response](#).)
- Or see [Configuring Syslog Alerting for Intrusion Events](#).

By default, the intrusion policy uses the settings in the Logging tab of the access control policy. If settings applicable to devices other than Firewall Threat Defense are not configured there, syslogs will not be sent for devices other than Firewall Threat Defense and no warning appears.

Configuration Locations for Syslogs for File and Malware Events

Configuration Location	Description and More Information
In an access control policy: Policies > Access Control , <each policy>, Logging	This is the main location for configuring the system to send syslogs for file and malware events. If you do not use the syslog settings in Firewall Threat Defense Platform Settings, you must also create an alert response. See Creating a Syslog Alert Response .
In Firewall Threat Defense Platform Settings: Devices > Platform Settings , Threat Defense Settings policy, Syslog	These settings apply only to Firewall Threat Defense devices running supported versions, and only if you configure the Logging tab in the access control policy to use Firewall Threat Defense platform settings. See Cisco Secure Firewall Management Center Device Configuration Guide .
In an access control rule: Policies > Access Control , <each policy>, <each rule>, Logging	If you do not use the syslog settings in Firewall Threat Defense Platform Settings, you must also create an alert response. See Creating a Syslog Alert Response .

Configuration Location for Syslogs for Application Logs (Threat Defense)

Configuration Location	Description and More Information
In an access control policy: Policies > Security policies > Access Control , <each policy>, Advanced Settings > Advanced Logging .	This is the main location for configuring the system to send syslogs for application-aware logs from Snort. If you do not use the default syslog settings in the access control policy, you can send the logs to Splunk, Secure Network Analytics, or to the syslog settings in the Firewall Threat Defense Platform Settings. For more information, see Application-Aware and Protocol-Aware Syslogs .
In an access control rule: Policies > Security policies > Access Control , <each policy>, <each rule>, Advanced Logging .	This is the where you enable logging for the access control rule and choose the applications for which you want to generate the application-aware logs from Snort.

Anatomy of Security Event Syslog Messages

Example security event message from Firewall Threat Defense (Intrusion Event)

```

0          1          2          3          4 5 6
-----
<37>2018-06-27 192.168.0.81 SFIMS : %FTD-5-430001:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Rev
Message: "DCE2_EVENT SMB_INVALID_DSIZE", Classifi
Potentially Bad Traffic, User: No Authentication R
Client: NetBIOS-ssn (SMB) client, ApplicationProto
(SMB), ACPolicy: test, NAPPolicy: Balanced Securit
Connectivity, InlineResult: Blocked

```

Table 1: Components of Security Event Syslog Messages

Item Number in Sample Message	Header Element	Description
0	PRI	The priority value that represents both Facility and Severity of the alert. The value appears in the syslog messages only when you enable logging in EMBLEM format using Firewall Management Center platform settings. If you enable logging of intrusion events through access control policy Logging tab, the PRI value is automatically displayed in the syslog messages. For information on how to enable the EMBLEM format, see Cisco Secure Firewall Management Center Device Configuration Guide . For information on PRI, see RFC5424 .
1	Timestamp	<p>Date and time the syslog message was sent from the device.</p> <ul style="list-style-type: none"> • (Syslogs sent from Firewall Threat Defense devices) For syslogs sent using settings in the access control policy and its descendants, or if specified to use this format in the Threat Defense Platform Settings, the date format is the format defined in the ISO 8601 timestamp format as specified in RFC 5424 (yyyy-MM-ddTHH:mm:ssZ), where the letter Z indicates the UTC time zone. • (Syslogs sent from all other devices) For syslogs sent using settings in the access control policy and its descendants, the date format is the format defined in the ISO 8601 timestamp format as specified in RFC 5424 (yyyy-MM-ddTHH:mm:ssZ), where the letter Z indicates the UTC time zone. • Otherwise, it is the month, day, and time in UTC time zone, though the time zone is not indicated. <p>To configure the timestamp setting in Threat Defense Platform Settings, see Cisco Secure Firewall Management Center Device Configuration Guide.</p>
2	<p>Device or interface from which the message was sent.</p> <p>This can be:</p> <ul style="list-style-type: none"> • IP address of the interface • Device hostname • Custom device identifier 	<p>(For syslogs sent from Firewall Threat Defense devices)</p> <p>If the syslog message was sent using the Threat Defense Platform Settings, this is the value configured in Syslog Settings for the Enable Syslog Device ID option, if specified.</p> <p>Otherwise, this element is not present in the header.</p> <p>To configure this setting in Threat Defense Platform Settings, see Cisco Secure Firewall Management Center Device Configuration Guide.</p>

Item Number in Sample Message	Header Element	Description
3	Custom value	If the message was sent using an alert response, this is the Tag value configured in the alert response that sent the message, if configured. (See Creating a Syslog Alert Response .) Otherwise, this element is not present in the header.
4	%FTD	Type of device that sent the message. %FTD is Secure Firewall Threat Defense
5	Severity	The severity specified in the syslog settings for the policy that triggered the message. For severity descriptions, see <i>Severity Levels</i> in the Cisco Secure Firewall Management Center Device Configuration Guide or Syslog Severity Levels .
6	Event type identifier	<ul style="list-style-type: none"> • 430001: Intrusion event • 430002: Connection event logged at beginning of connection • 430003: Connection event logged at end of connection • 430004: File event • 430005: File malware event <p>Use the following to identify application and protocol-aware logs generated by Snort:</p> <ul style="list-style-type: none"> • 431001: HTTP application log. • 431002: FTP application log. • 431003: CONN application log. • 431004: DNS application log. • 431005: WEIRD application log. • 431006: NOTICE application log.
--	Facility	See Facility in Security Event Syslog Messages , on page 21.

Item Number in Sample Message	Header Element	Description
--	Remainder of message	<p>Fields and values separated by colons.</p> <p>Fields with empty or unknown values are omitted from messages.</p> <p>For field descriptions, see:</p> <ul style="list-style-type: none"> • Connection and Security-Related Connection Event Fields. • Intrusion Event Fields • File and Malware Event Fields <p>Note</p> <p>Field description lists include both syslog fields and fields visible in the event viewer (menu options under the Analysis menu in the Firewall Management Center web interface.) Fields available via syslog are labeled as such.</p> <p>Some fields visible in the event viewer are not available via syslog. Also, some syslog fields are not included in the event viewer (but may be available via search), and some fields are combined or separated.</p>

Facility in Security Event Syslog Messages

Facility values are not generally relevant in syslog messages for security events. However, if you require Facility, use the following table:

Device	To Include Facility in Connection Events	To Include Facility in Intrusion Events	Location in Syslog Message
Firewall Threat Defense	Use the EMBLEM option in Threat Defense Platform Settings. Facility is always ALERT for connection events when sending syslog messages using Threat Defense Platform Settings.	Use the EMBLEM option in Threat Defense Platform Settings or configure logging using the syslog settings in the intrusion policy. If you use the intrusion policy, you must also specify the logging host in the intrusion policy settings. Enable syslog alerting and configure facility and severity on the intrusion policy. See Configuring Syslog Alerting for Intrusion Events .	Facility does not appear in the message header, but the syslog collector can derive the value based on RFC 5424, section 6.2.1.
Devices other than Firewall Threat Defense	Use an alert response.	Use the syslog setting in the intrusion policy advanced settings or an alert response identified in the access control policy Logging tab.	

For more information, see [Facilities and Severities for Intrusion Syslog Alerts](#) and [Creating a Syslog Alert Response](#).

Secure Firewall Syslog Message Types

Secure Firewall can send multiple syslog data types, as described in the following table:

Syslog Data Type	See
Audit logs from Firewall Management Center	Stream Audit Logs to Syslog and the Audit and Syslog chapter
Device health and network-related logs from Firewall Threat Defense devices	Cisco Secure Firewall Management Center Device Configuration Guide
Connection, security intelligence, and intrusion event logs from Firewall Threat Defense devices	About Configuring the System to Send Security Event Data to Syslog, on page 10.
Connection, security intelligence, and intrusion event logs from Classic devices	About Configuring the System to Send Security Event Data to Syslog, on page 10
Logs for file and malware events	About Configuring the System to Send Security Event Data to Syslog, on page 10
IPS Settings	Send Syslog messages for IPS events. Configuration Locations for Syslogs for Intrusion Events (Firewall Threat Defense Devices), on page 16

Syslog Data Type	See
Application and protocol-aware logs from Firewall Threat Defense.	Application-Aware and Protocol-Aware Syslogs.

Limitations of Syslog for Security Events

- If you will use syslog or store events externally, avoid special characters in object names such as policy and rule names. Object names should not contain special characters, such as commas, that the receiving application may use as separators.
- It may take up to 15 minutes for events to appear on your syslog collector.
- Data for the following file and malware events is not available via syslog:
 - Retrospective events
 - Events generated by Secure Endpoint

eStreamer Server Streaming

The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Secure Firewall Management Center to a custom-developed client application. The event data can either be streamed as binary data, or as fully-qualified events in plaintext format. For more information, see *Secure Firewall eStreamer Fully-Qualified Events Guide*, or *Secure Firewall Management Center Event Streamer Integration Guide*.



Note eStreamer Client has been deprioritized, and the eNcoreCLI is End of Life as of 7/1/2024.

Before the appliance you want to use as an eStreamer server can begin streaming eStreamer events to an external client, you must configure the eStreamer server to send events to clients, provide information about the client, and generate a set of authentication credentials to use when establishing communication. You can perform all of these tasks from the appliance's user interface. Once your settings are saved, the events you selected will be forwarded to eStreamer clients when requested.

You can control which types of events the eStreamer server is able to transmit to clients that request them.

Table 2: Event Types Transmittable by the eStreamer Server

Event Type	Description
Intrusion Events	intrusion events generated by managed devices
Intrusion Event Packet Data	packets associated with intrusion events
Intrusion Event Extra Data	additional data associated with an intrusion event such as the originating IP addresses of a client connecting to a web server through an HTTP proxy or load balancer
Discovery Events	Network discovery events

Event Type	Description
Correlation and Allow List Events	correlation and compliance allow list events
Impact Flag Alerts	impact alerts generated by the Firewall Management Center
User Events	user events
Malware Events	malware events
File Events	file events
Connection Events	information about the session traffic between your monitored hosts and all other hosts.

Comparison of Syslog and eStreamer for Security Eventing

Generally, organizations that do not currently have significant existing investment in eStreamer should use syslog rather than eStreamer to manage security event data externally.

Syslog	eStreamer
No customization required	Significant customization and ongoing maintenance required to accommodate changes in each release
Standard	Proprietary
Syslog standard does not protect against data loss, especially when using UDP	Protection against data loss
Sends directly from devices	Sends from Firewall Management Center, adding processing overhead
Support for file and malware events, connection events (including security intelligence events) and intrusion events.	Support for all event types listed in eStreamer Server Streaming, on page 23 .
Some event data can be sent only from Firewall Management Center. See Data Sent Only via eStreamer, Not via Syslog, on page 24 .	Includes data that cannot be sent via syslog directly from devices. See Data Sent Only via eStreamer, Not via Syslog, on page 24 .

Data Sent Only via eStreamer, Not via Syslog

The following data is available only from Secure Firewall Management Center and thus cannot be sent via syslog from devices:

- Packet Logs
- Intrusion Event Extra Data events

For a description, see [eStreamer Server Streaming, on page 23](#).

- Statistics and aggregate events

- Network Discovery events
 - User activity and login events
 - Correlation events
 - For malware events:
 - retrospective verdicts
 - ThreatName and Disposition, unless information about the relevant SHAs has already been synchronized to the device
 - The following fields:
 - Impact and ImpactFlag fields
For a description, see [eStreamer Server Streaming, on page 23](#).
 - the IOC_Count field
 - Most raw IDs and UUIDs.
Exceptions:
 - Syslogs for connection events do include the following: FirewallPolicyUUID, FirewallRuleID, TunnelRuleID, MonitorRuleID, SI_CategoryID, SSL_PolicyUUID, and SSL_RuleID
 - Syslogs for intrusion events do include IntrusionPolicyUUID, GeneratorID, and SignatureID
 - Extended metadata, including but not limited to:
 - User details provided by LDAP, such as full name, department, phone number, etc.
Syslog only provides usernames in the events.
 - Details for state-based information such as SSL Certificate details.
Syslog provides basic information like the certificate fingerprint, but will not provide other certificate details like the cert CN.
 - Detailed application information, such as App Tags and Categories.
Syslog provides only Application names.
- Some metadata messages also include extra information about the objects.
- Geolocation information

Choosing eStreamer Event Types

The **eStreamer Event Configuration** check boxes control which events the eStreamer server can transmit. Your client must still specifically request the types of events you want it to receive in the request message it sends to the eStreamer server. For more information, see the *Secure Firewall Management Center Event Streamer Integration Guide*.

In a multidomain deployment, you can configure eStreamer Event Configuration at any domain level. However, if an ancestor domain has enabled a particular event type, you cannot disable that event type in the descendant domains.

You must be an Admin user to perform this task, for Firewall Management Center.

Procedure

-
- Step 1** Choose **Integrations** > + **Show more** > **eStreamer**
 - Step 2** Under **eStreamer Event Configuration**, check or clear the check boxes next to the types of events you want eStreamer to forward to requesting clients, described in [eStreamer Server Streaming, on page 23](#).
 - Step 3** Click **Save**.
-

Configuring eStreamer Client Communications

Before eStreamer can send eStreamer events to a client, you must add the client to the eStreamer server's peers database from the eStreamer page. You must also copy the authentication certificate generated by the eStreamer server to the client. After completing these steps you do not need to restart the eStreamer service to enable the client to connect to the eStreamer server.

In a multidomain deployment, you can create an eStreamer client in any domain. The authentication certificate allows the client to request events only from the client certificate's domain and any descendant domains. The eStreamer configuration page shows only clients associated with the current domain, so if you want to download or revoke a certificate, switch to the domain where the client was created.

You must be an Admin or Discovery Admin user to perform this task, for Firewall Management Center.

Procedure

-
- Step 1** Choose **Integrations** > + **Show more** > **eStreamer**
 - Step 2** Click **Create Client**.
 - Step 3** In the **Hostname** field, enter the host name or IP address of the host running the eStreamer client.
Note
If you have not configured DNS resolution, use an IP address.
 - Step 4** If you want to encrypt the certificate file, enter a password in the **Password** field.
 - Step 5** Click **Save**.
The eStreamer server now allows the host to access port 8302 on the eStreamer server and creates an authentication certificate to use during client-server authentication.
 - Step 6** Click **Download** (📄) next to the client hostname to download the certificate file.
 - Step 7** Save the certificate file to the appropriate directory used by your client for SSL authentication.
 - Step 8** To revoke access for a client, click **Delete** (🗑️) next to the host you want to remove.

Note that you do not need to restart the eStreamer service; access is revoked immediately.

Event Analysis in Splunk

You can use the Cisco Secure Firewall app for Splunk as an external tool to display and work with Secure Firewall event data, to hunt and investigate threats on your network. To use the Splunk tool, eStreamer is required. This is an advanced functionality. See [eStreamer Server Streaming, on page 23](#). For more information, see [User Guide for Cisco Secure Firewall App for Splunk](#).

Alternatively, you can use the **Integrations > Splunk** to configure Splunk server settings in the Firewall Management Center web interface. For information about configuration steps, see [Splunk Integration: Send Events Directly from Management Center, on page 27](#).

Splunk Integration: Send Events Directly from Management Center

Cisco Splunk is a Security Information and Event Management (SIEM) tool that provides visibility and monitoring of security events across Cisco Secure Firewall devices.

In Firewall Management Center versions earlier to 10.0, security events were sent to Splunk using eStreamer. From Firewall Management Center version 10.0, you can send events directly to the Splunk server using the Firewall Management Center web interface. The wizard-driven interface helps you set up Splunk integration effortlessly.

This integration allows you to perform these actions.

- Customize event flow by specifying event types—such as connection, intrusion, malware, file, user activity, correlation, discovery, intrusion packet—and their sources (Firewall Management Center or Firewall Threat Defense device) according to your monitoring requirements.
- Select the source interface for sending syslog events. You can choose to send events from the Firewall Management Center's management interface or Firewall Threat Defense device's management or data interfaces.
- Create profiles with various configurations to suit different monitoring requirements.



Note

While the integration procedure described in this topic is for Splunk, you can use the Splunk Integration wizard to integrate any SIEM tool with Firewall Management Center to send syslog messages to an external syslog server.

Guidelines and Limitations for Splunk Integration

- When you enable Splunk integration, your existing syslog server configuration is not migrated.

- You cannot configure a Splunk profile to send events from both Firewall Management Center and Firewall Threat Defense device for the same event type.
- If you set up domains in Firewall Management Center, you can configure Splunk only from leaf domains.
- You can create a maximum of 15 Splunk profiles per domain. However, multiple domains can be configured to send syslog messages to the same or different servers.
- Do not create duplicate profiles for the same devices because it results in devices sending duplicated events to the Splunk server.
- Only basic TLS encryption is supported over data interfaces from devices; client and server authentication are not supported.
- The syslog payload is sent to the Splunk server in JSON format.
- In a high availability set up, Splunk configuration is synchronized between the Firewall Management Center HA pair. Only active unit sends the events. In the case of a failover, the new active unit will start sending the events.
- The message header of syslog events sent through data interfaces contains only the syslog tag and not the device IP address.
- Splunk integration does not support analytics devices managed by another Firewall Management Center, for example, cdFMC.

Configure Splunk in Secure Firewall Management Center

Before you begin:

- Ensure that the Splunk server can be reached by both Firewall Management Center and Firewall Threat Defense device.
- Configure the Cisco Secure Firewall App in Splunk. You need a valid Splunk server license and Cisco Secure Cloud account. For configuration information, see [Configure Secure Firewall App in Splunk, on page 33](#).
- The Cisco Secure Firewall App in Splunk does not support TLS. Hence, if you choose to use the TLS protocol to send events to Splunk, configure TLS on the Splunk server. For TLS configuration instructions, see the section *Configure Splunk indexing and forwarding to use TLS certificates* under *Manage Users and Security* in the [Splunk Administer](#) guide.
- Create required objects such as host, security zone, interface group, certificate, and so on, before starting the configuration procedure. Although you can navigate from the **Splunk integration** wizard to create objects, having them in advance will provide a smoother integration experience.
- Connection events from Firewall Management Center or Firewall Threat Defense device will be sent to the configured Splunk server or SIEM syslog server only when the logging destination is appropriately selected in the Access Control policy rules page. For more information, see [Creating and Edit Access Control Rules](#).

The Splunk integration wizard allows you to create a profile that enables you to stream events and syslog from the Firewall Management Center and its managed devices to a specific server.

You can create multiple profiles to configure any number of servers for various combinations of devices and events. For example, you can create multiple profiles to send events from Firewall Threat Defense devices to one server, while directing events from the Firewall Management Center to another. Another scenario where multiple profiles can be created is when you have to send a specific set of events to one server and all the remaining events to a different server. Each profile is independent, but they all apply additively.

To open the **Splunk integration** wizard, go to **Integrations > Splunk**.

The steps for configuring Splunk integration in Secure Firewall Management Center are listed in this table.

	Do This	More Information
Step 1	Configure Splunk or similar SIEM tool server.	See Configure Splunk Server, on page 29 .
Step 2	Choose the event types that you want to send to the Splunk server.	See Select Event Types, on page 30 .
Step 3	Specify the devices and the interfaces from which you want to send syslog events to Splunk.	See Select Devices and Interfaces, on page 31 .
Step 4	(Optional) Specify the device certificate to be used for sending events securely to Splunk.	See Configure Firewall Certificates, on page 32 .
Step 5	View the summary of the profile that is being created.	See Summary, on page 32 .

Configure Splunk Server

In this step, provide networking information about the Splunk syslog server, and specify the protocols, and ports for receiving syslog events.

Procedure

-
- Step 1** In the **Configure Splunk server** page, from the **Host object or IP address** drop-down, choose the host object or enter an IP address of the Splunk server. To create a host object, click the **Create** link in the drop-down list.
- Step 2** Click the **Protocol** (UDP, TCP, or TLS) that you want the Splunk server to use for communicating with Firewall Management Center and Firewall Threat Defense device.
- Step 3** In the **Port** field, enter the port number applicable for the selected protocol:
- UDP: Enter the port number **514**, or a number between **1025** and **65535**. The default UDP port is **514**.
 - TCP: Enter the port number between **1025** and **65535**. The default TCP port is **1470**.
 - TLS: Enter the port number between **1** and **65535**. The default TLS port is **6514**.

- Step 4** (Optional) If you selected **TLS**, specify the trusted CA name to securely establish the connection on the Splunk server. From the **Trusted certificate authority** drop-down list, choose the CA. (To import a new CA object, click the **Create** link in the drop-down list.)
- Step 5** To forward the events logged by a facility, from the **Facility** drop-down list, choose the corresponding facility.
- Step 6** To forward the events with a specific severity, from the **Severity** drop-down list, choose the severity level.
- Step 7** (Optional) In the **Tag** field, enter an alphanumeric string by which to identify the message in the server.
- Step 8** (Optional) To cancel the creation of the Splunk profile, click **Cancel**.
- Step 9** To move to the next step in the Splunk configuration, click **Next**.

Select Event Types

In this step, you can specify the type of events that you want to send to Splunk. The recommended event types are selected by default. However, you can modify the default source for the event types.

Procedure

- Step 1** To specify the event source for the event types, from the **Source** drop-down list, choose **FTD** or **FMC**, as applicable. The system default event sources are listed in this table.

Event type	Source (Default)	Applicable sources (Firewall Threat Defense, Firewall Management Center, or both)
Connection—Security or All <ul style="list-style-type: none"> • Security connection events implies sending only high-priority connection events • All implies sending all connection events. 	Firewall Threat Defense	Both Important Sending connection events from the Management Center may cause performance issues.
Intrusion	Firewall Management Center	Both Note Sending intrusion events from the Threat Defense devices will not include impact flags.
AMP/Retrospective	Firewall Management Center	Firewall Management Center
File/Malware	Firewall Threat Defense	Both
User activity	Disabled	Firewall Management Center
Correlation	Disabled	Firewall Management Center

Event type	Source (Default)	Applicable sources (Firewall Threat Defense, Firewall Management Center, or both)
Discovery	Disabled	Firewall Management Center
Intrusion packet	Disabled	Both

Step 2 After selection, to reset to default settings, click **Revert to system defaults**.

Step 3 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 4 (Optional) To go back to the previous step, click **Back**.

Step 5 To move to the next step in the Splunk configuration, click **Next**.

Select Devices and Interfaces

In this step, you can specify the Firewall Threat Defense devices and interfaces from which you want to send syslog events to Splunk. To send events from multiple interfaces, use security zones or interface groups.



Note

If you are using security zones or interface groups, only routed, management, switched, and loopback zones and groups are allowed.

Procedure

Step 1 Under **Select devices**, click the relevant options:

- **Use management interface:** Click this button to configure the management interface of Firewall Threat Defense device to send the events to Splunk. When this option is chosen, all the devices in the current domain also receive the Splunk configuration.
- **Use security zones and interface groups to specify devices and interfaces:** Click this button to configure the interfaces of corresponding devices in the selected security zones and interface groups to send their respective events to Splunk.
 - From the **Security zones and interface groups** drop-down list, choose the required zones and groups.
 - To create a security zone or interface group for the device's interfaces, click **Create** in the **Certificates** drop-down list.
- **Manually select devices and interfaces:** Click this button to send the events from the deployed device to Splunk. From the **Interface** drop-down list, choose the configured interface through which you want the events to be sent to Splunk. You can choose only security zones that include this device.

Note

- Virtual Tunnel Interface (VTI) and Dynamic Virtual Tunnel Interface (DVTI) are excluded from Splunk configuration.

- To encrypt syslog events over TLS, use the management interface to add a certificate. Encryption is not supported for data interfaces configured for TLS.
- Click the **Send events from this device** toggle button corresponding to the device and its selected interface.
- To create a security zone or interface group for the device's interfaces, click **Create**.

Step 2 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 3 (Optional) To go back to the previous step, click **Back**.

Step 4 To move to the next step in the Splunk configuration, click **Next**.

Configure Firewall Certificates

In this step, you can specify the device certificate to be used for sending events securely to Splunk. This step is optional. It is applicable only if you use the TLS protocol to send events to Splunk.

Before you begin

You can configure the certificates when you have set TLS protocol while configuring the Splunk server. Add certificate object for these clients:

- For Firewall Management Center, use internal certificate objects for authentication.
- For Firewall Threat Defense, use a certificate enrollment object. First, create the object at **Objects > PKI > Certificate Enrollment**. Then, enroll the certificate on a device at **Devices > Certificates**.

Procedure

-
- Step 1** From the **Firewall Management Center client certificate** drop-down list, choose the certificate. To create an internal certificate, click **Create**.
- Step 2** In the **Firewall Threat Defense certificates** box, use the search box to choose the device whose certificate you want to assign.
- Step 3** From the **Certificates** drop-down list, choose the certificate. Only successfully enrolled device certificates are listed. To enroll a new device certificate, click **Create**.
- Step 4** (Optional) To cancel the creation of the Splunk profile, click **Cancel**.
- Step 5** (Optional) To go back to the previous step, click **Back**.
- Step 6** To move to the next step in the Splunk configuration, click **Next**.
-

Summary

You can view the selections made for the Splunk configuration profile.

Procedure

Step 1 Under **Profile Name**, a system-generated name is displayed. Edit the value in the **Name** field, if you want to use a different name.

Note

The name must start with a letter, a number, or an underscore (_). The name can contain include letters, numbers, and special characters: period (.), hyphen (-), underscore (_), and plus (+).

Step 2 To change a value from a previous Splunk server configuration, click **Edit** next to the attribute.

Step 3 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 4 (Optional) To go back to the previous step, click **Back**.

Step 5 To save the Splunk profile, click **Submit**.

Step 6 If you have configured Threat Defense events to be sent to Splunk, click **Deploy**.

Note

When you configure Management Center events to be sent to Splunk, eventing files are generated immediately after the profile is saved. You will be able to view the events sent from Management Center in Splunk. Deploy is not needed for events from Management Center.

Configure Secure Firewall App in Splunk

To ensure that the Splunk server is reachable by Firewall Management Center and Firewall Threat Defense, and to receive the events from the device, configure the Cisco Secure Firewall App in Splunk.

Before you begin

- Ensure that you have obtained a Splunk server license and a Cisco Security Cloud account.

Procedure

Step 1 Download and install the Splunk server using the instructions provided in [Splunk Enterprise Installation Manual](#).

Step 2 To install Splunk license, log in to your Splunk server's web interface.

Step 3 Go to **Settings > Licensing > Add license**. Use the license received by email.

Note

Make sure to restart Splunk to complete license registration.

Step 4 Download Cisco Security Cloud from [Splunkbase Apps](#).

Step 5 To install Cisco Security Cloud, log in to your Splunk server's web interface.

Step 6 Go to **Apps > Manage Apps > Install app from file**.

- Step 7** Click **Browse** and select the downloaded application file and upload.
- Step 8** To configure the server to receive the syslog events from the Firewall Management Center and Firewall Threat Defense, go to **Apps > Cisco Security Cloud > Secure Firewall > Configure Application**, and then click the **Syslog** tab.
- Step 9** In the **Input Name** field, enter any name.
- Step 10** In the **Input Type** field, enter UDP or TCP.
- TLS is not supported in the Cisco Security Cloud application. Use rsyslog or syslog-ng to establish TLS on Splunk server. For detailed procedures, see [Configure TLS on Splunk Server](#).
- Step 11** In the **Port** field, enter a value between 1025 and 65535. The default port is 514.
- Step 12** Leave the **Host** field blank. This will allow the Splunk to process events from any Firewall Management Center and Firewall Threat Defense.
- Step 13** In the **Source Type** field, enter *cisco:ftd:syslog*.
- Step 14** In the **Interval** field, enter 600 seconds.

Event Analysis in IBM QRadar

You can use the Cisco Firepower app for IBM QRadar as an alternate way to display event data and help you analyze, hunt for, and investigate threats to your network.

eStreamer is required. This is an advanced functionality. See [eStreamer Server Streaming, on page 23](#).

For more information, see <https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html>.

History for Analyzing Event Data Using External Tools

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Improved threat detection with inclusion of packet data for the intrusion events.	10.0.0	10.0.0	<p>Introduced automatic inclusion of packet data with intrusion events when sent to the Security Cloud Control. This enhancement enables Cisco Talos to analyze the packet and better distinguish between true and false threats, improving overall threat detection accuracy and operational efficiency.</p> <p>For more information, see Enable Sending Events to the Security Cloud Control, on page 2.</p> <p>Upgrade impact: If Intrusion events were already configured to be sent to Security Cloud Control before the upgrade, the feature will automatically enable the transmission of packet data along with these events after the upgrade.</p>

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Register your management center with the Security Cloud Control using your Cisco Security Cloud Sign On account.	7.6.0	Any	<p>You can now authorize the management center to register to the Security Cloud Control using your Cisco Security Cloud Sign On account and CDO tenant. Registering the management center to the Security Cloud Control gives you access to the latest Cisco cloud services such as the Cisco AI Assistant for Security, Policy Analyzer and Optimizer, Zero-Touch Provisioning, and more.</p> <p>New/Modified Screen: Integration > Cisco Security Cloud.</p> <p>Upgrade Impact: Cisco Security Cloud integration is set to disabled by default.</p>
Deprecated: SecureX Ribbon	Any	Any	<p>SecureX Ribbon is deprecated.</p> <p>If you have installed the Cisco SecureX Ribbon browser extension in your Firefox browser and are experiencing compatibility errors while using Firewall Management Center, remove the SecureX Ribbon extension.</p> <p>To remove the extension, open Firefox, go to the browser's add-ons or extensions manager, locate the Cisco SecureX Ribbon extension, and remove or disable it. Restart Firefox to apply the changes.</p>
Deprecated: SecureX Integration	7.6.0	Any	<p>SecureX integration is deprecated. You can now register your Firewall Management Center and its managed devices to the Security Cloud Control using your Cisco Security Cloud Sign-On account and your Security Cloud Control tenant.</p> <p>New/modified screen: Integration > Cisco Security Cloud.</p> <p>Deprecated screen: Integration > SecureX.</p>
SecureX ribbon	7.0	Any	<p>The SecureX ribbon pivots into SecureX for instant visibility into the threat landscape across your Cisco security products.</p> <p>To display the SecureX ribbon in Firewall Management Center, see the <i>Firepower and SecureX Integration Guide</i> at https://cisco.com/go/firepower-securex-documentation.</p> <p>New/Modified screens: New page: System > SecureX.</p>
Send all connection events to the Cisco cloud	7.0	Any	<p>You can now send all connection events to the Cisco cloud, rather than just sending high-priority connection events.</p> <p>New/Modified screens: New option on the System > Integration > Cloud Services page.</p>

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Cross-launch to view data in Secure Network Analytics	6.7	Any	<p>This feature introduces a quick way to create multiple entries for your Secure Network Analytics appliance on the Analysis > Contextual Cross-Launch page. These entries allow you to right-click a relevant event to cross-launch Secure Network Analytics and display information related to the data point from which you cross-launched.</p> <p>New menu item: System > Logging > Security Analytics and Logging.</p> <p>New page to configure sending events to Secure Network Analytics.</p>
Contextual cross-launch from additional field types	6.7	Any	<p>You can now cross-launch into an external application using the following additional types of event data:</p> <ul style="list-style-type: none"> • Access control policy • Intrusion policy • Application protocol • Client application • Web application • Username (including realm) <p>New menu options: Contextual-cross launch options are now available when right-clicking the above data types for events in Dashboard widgets and event tables on pages under the Analysis menu.</p> <p>Supported platforms: Secure Firewall Management Center</p>
Integration with IBM QRadar	6.0 and later	Any	<p>IBM QRadar users can use a new Firepower-specific app to analyze their event data.</p> <p>Available functionality is affected by your Firepower version.</p> <p>See Event Analysis in IBM QRadar, on page 34.</p>

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Enhancements to integration with SecureX Threat Response	6.5	Any	<ul style="list-style-type: none"> • Support for regional clouds: <ul style="list-style-type: none"> • United States (North America) • Europe • Support for additional event types: <ul style="list-style-type: none"> • File and malware events • High-priority connection events <p>These are connection events related to the following:</p> <ul style="list-style-type: none"> • Intrusion events • Security Intelligence events • File and malware events <p>Modified screens: New options on System > Integration > Cloud Services.</p> <p>Supported Platforms: All devices supported in this release, either via direct integration or syslog.</p>
Syslog	6.5	Any	The AccessControlRuleName field is now available in intrusion event syslog messages.
Integration with Cisco Security Packet Analyzer	6.5	Any	Support for this feature was removed.
Integration with SecureX Threat Response	6.3 (via syslog, using a proxy collector) 6.4 (direct)	Any	<p>Integrate Firepower intrusion event data with data from other sources for a unified view of threats on your network using the powerful analysis tools in SecureX Threat Response.</p> <p>Modified screens (version 6.4): New options on System > Integration > Cloud Services.</p> <p>Supported Platforms: Secure Firewall Threat Defense devices running version 6.3 (via syslog) or 6.4.</p>
Syslog support for File and Malware events	6.4	Any	<p>Fully-qualified file and malware event data can now be sent from managed devices via syslog.</p> <p>Modified screens: Policies > Access Control > Access Control > Logging.</p> <p>Supported Platforms: All managed devices running version 6.4.</p>

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Integration with Splunk	Supports all 6.x versions	Any	<p>Splunk users can use a new, separate Splunk app, Cisco Secure Firewall app for Splunk, to analyze events.</p> <p>Available functionality is affected by your Firepower version.</p> <p>See Event Analysis in Splunk, on page 27.</p>
Integration with Cisco Security Packet Analyzer	6.3	Any	<p>Feature introduced: Instantly query Cisco Security Packet Analyzer for packets related to an event, then click to examine the results in Cisco Security Packet Analyzer or download them for analysis in another external tool.</p> <p>New screens:</p> <p>System > Integration > Packet Analyzer</p> <p>Analysis > Advanced > Packet Analyzer Queries .</p> <p>New menu options: Query > Packet Analyzer menu item when right-clicking on an event on Dashboard pages and event tables on pages under the Analysis menu.</p> <p>Supported platforms: Secure Firewall Management Center</p>
Contextual cross-launch	6.3	Any	<p>Feature introduced: Right-click an event to look up related information in predefined or custom URL-based external resources.</p> <p>New screens: Analysis > Advanced > Contextual Cross-Launch.</p> <p>New menu options: Multiple options when right-clicking on an event on Dashboard pages and event tables on pages under the Analysis menu.</p> <p>Supported platforms: Secure Firewall Management Center</p>
Syslog messages for connection and intrusion events	6.3	Any	<p>Ability to send fully-qualified connection and intrusion events to external storage and tools via syslog, using new unified and simplified configurations. Message headers are now standardized and include event type identifiers, and messages are smaller because fields with unknown and empty values are omitted.</p> <p>Supported Platforms:</p> <ul style="list-style-type: none"> • All new functionality: Firewall Threat Defense devices running version 6.3. • Some new functionality: Non-Firewall Threat Defense devices running version 6.3. • Less new functionality: All devices running versions older than 6.3. <p>For more information, see the topics under About Sending Syslog Messages for Security Events, on page 9 and subtopics.</p>
eStreamer	6.3	Any	Moved eStreamer content from the Host Identity Sources chapter to this chapter and added a summary comparing eStreamer to syslog.