Event Analysis Using External Tools

- Integrate with Cisco SecureX, on page 1
- Event Analysis with SecureX Threat Response, on page 9
- Event Investigation Using Web-Based Resources, on page 9
- Configure Cross-Launch Links for Secure Network Analytics, on page 12
- About Sending Syslog Messages for Security Events, on page 14
- eStreamer Server Streaming, on page 27
- Event Analysis in Splunk, on page 30
- Event Analysis in IBM QRadar, on page 31
- History for Analyzing Event Data Using External Tools, on page 31

Integrate with Cisco SecureX

View and work with data from all of your Cisco security products and more through a single pane of glass, the SecureX cloud portal. Use the tools available via SecureX to enrich your threat hunts and investigations. SecureX can also provide useful appliance and device information such as whether each is running an optimal software version.

For more information about SecureX, see Cisco SecureX page.

Enable SecureX Integration

The Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio and your infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications. For more information about SecureX, see the Cisco SecureX product page.

Integrating SecureX with the management center provides you a complete overview of all the data from the management center. For more information about integrating the management center with SecureX, see the Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide.

Before you begin

You need a SecureX account that belongs to an organization. If you don't have a SecureX account, create a SecureX account using your CDO tenant. See Create a SecureX Account Using CDO for more information.

Procedure

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

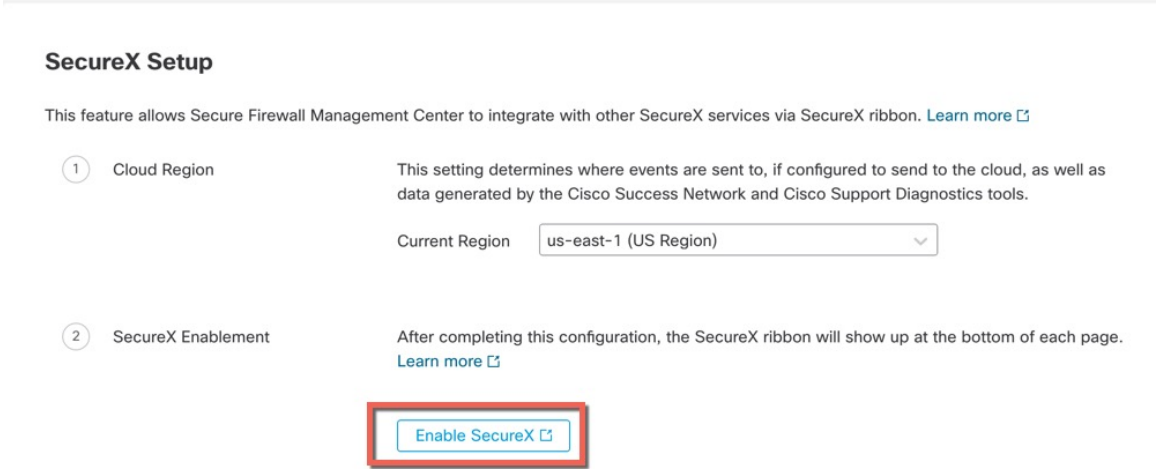
Step 2 (Optional) For the **Cloud Region**, choose your **Current Region**.

The region selected by default matches your Smart Licensing region, so you probably do not need to change the region.

Step 3 In **SecureX Enablement**, perform the following steps.

a) Click **Enable SecureX**.

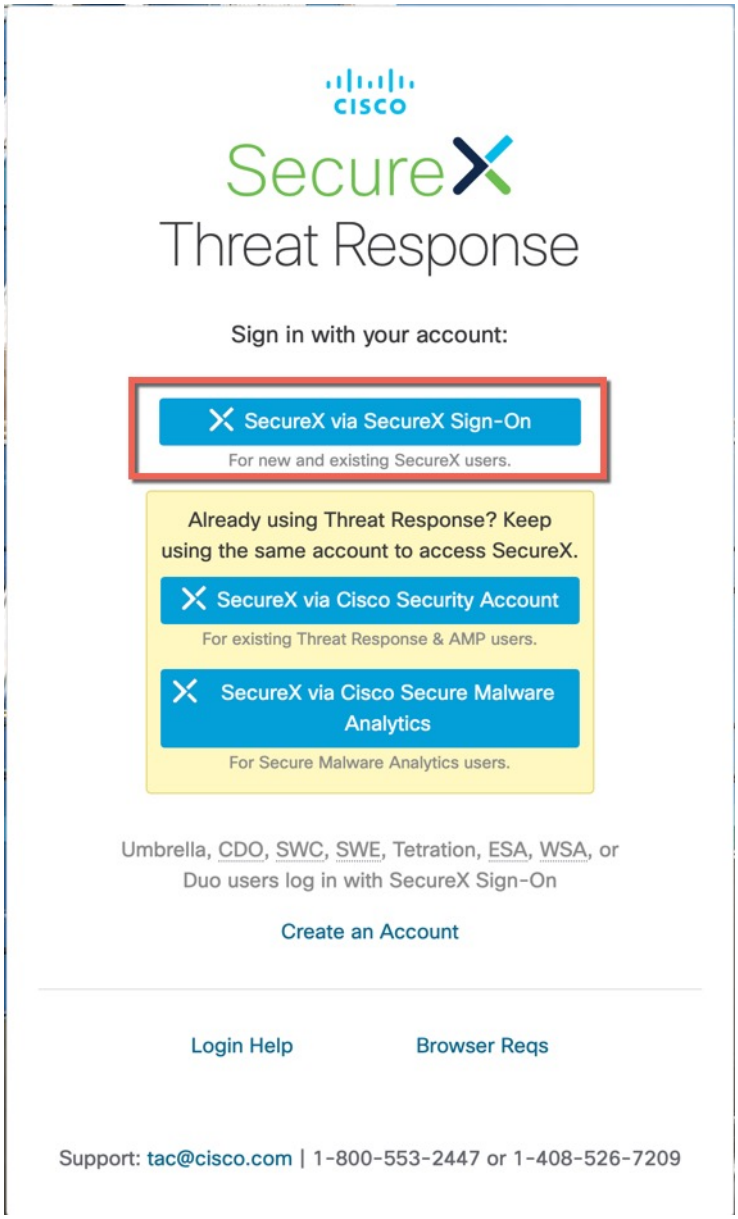
Figure 1: Enable SecureX



b) Log into SecureX.

A separate browser tab or window opens to log you into your SecureX account. Make sure this page is not blocked by a pop-up blocker.

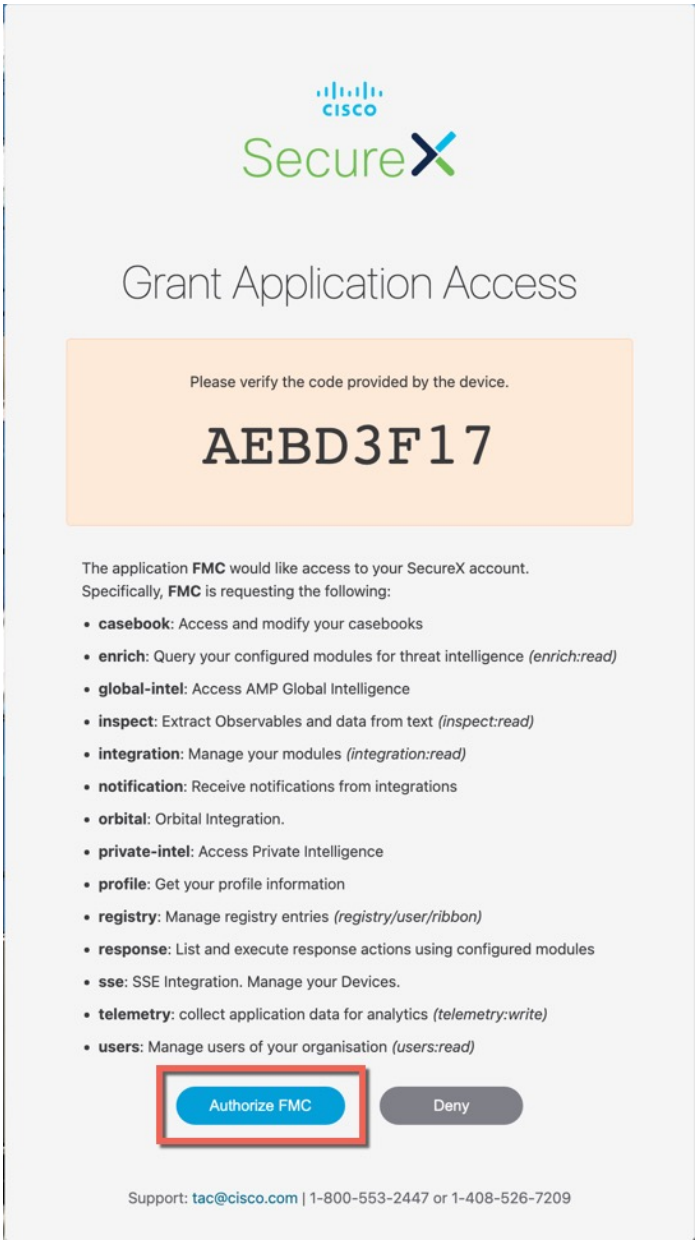
Figure 2: SecureX Sign-In



c) Click **Authorize FMC**.

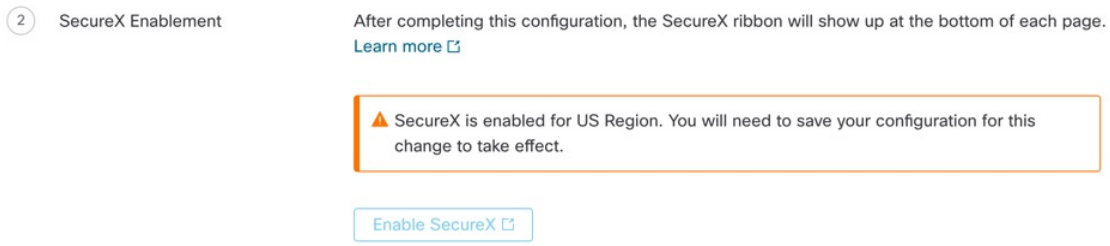
You are shown a code that should match the code shown in the management center.

Figure 3: Grant Application Access



d) After the management center integrates with SecureX, you see a success message. Click **Save**.

Figure 4: Success Message



Configure the Management Center to Send Events to the Cisco Security Cloud

Configure your management center to have the managed threat defense devices send events directly to Cisco Security Cloud. The cloud region and event types that you configure in this page can be used for multiple integrations when applicable and enabled.

Before you begin

- Ensure that you register the management center with the Smart License (**System** (⚙) > **Smart License**) or enable Cisco Security Cloud integration to allow your devices to send firewall events to the Cisco cloud.
- In the management center:
  - Go to the **System** > **Configuration** page and give your management center a unique name to clearly identify it in the **Devices** list in the cloud.
  - Add your threat defense devices to the management center, assign licenses to them, and ensure that the system is working correctly. Ensure that you have created the necessary policies and the generated events are displayed as expected in the management center UI under the **Analysis** menu.
- Ensure that you have your Cisco security cloud sign on credentials and can sign in to the SecureX regional cloud in which your account was created.

  For more information on SecureX regional cloud URLs and supported device versions, see Cisco Secure Firewall Management Center and SecureX Integration Guide.
- If you are currently sending events to the cloud using syslog, disable it to avoid duplication.

Procedure

Step 1 Determine the Cisco regional cloud you want to use for sending firewall events. For more information for choosing a regional cloud, see Cisco Secure Firewall Management Center and SecureX Integration Guide.

Note If SecureX is enabled and the management center is registered to the selected regional cloud, changing the regional cloud disables SecureX. You can enable the SecureX again after changing the regional cloud.

Step 2 In your management center, click **Integration** > **SecureX**.

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 following table.

Integration	Supported Event Options	Notes
Cisco Security Analytics and Logging (SaaS)	All	High-priority connection events include: • Security Intelligence connection events • Connection events related to file and malware events • Connection events related to intrusion events
Cisco SecureX and Cisco SecureX threat response	Depending on your version: • Security-related connection events. • Intrusion events. • File and malware events.	Even if you send all the connection events, Cisco SecureX and Cisco SecureX threat response supports only security-related connection events.

Note
- If you enable **Intrusion Events**, the management center sends events along with the impact flag.
- If you enable **File and Malware Events**, in addition to the events sent from the threat defense devices, the management center sends retrospective events.

Step 6 Click **Save**.

Configure Cisco Success Network Enrollment

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

- To inform you of available, but unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that are available for your product.
- (If you integrate with SecureX) To summarize appliance and device status in SecureX tiles and know whether all your devices are running optimal software versions.
- To help Cisco improve its products.

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

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

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

Note

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

Before you begin

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

Procedure

Step 1 Click **Integration** > **SecureX**.

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

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

Step 3 Click **Save**.

Configure Cisco Support Diagnostics Enrollment

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

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

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

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

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

Before you begin

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

Procedure

Step 1 Click **Integration** > **SecureX**.

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

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

Step 3 Click **Save**.

Access SecureX Using the Ribbon

The ribbon appears at the bottom of every page in the management center web interface. You can use the ribbon to quickly pivot to other Cisco security products and work with threat data from multiple sources.

Before you begin

- If you do not see the SecureX ribbon at the bottom of management center web interface pages, do not use this procedure.

  Instead, see the Cisco Secure Firewall Threat Defense and SecureX Integration Guide.

- If you don't already have a SecureX account, obtain one from your IT department.

Procedure

Step 1 In management center, click the ribbon at the bottom of any management center page.

Step 2 Click **Get SecureX**.

Step 3 Sign in to SecureX.

Step 4 Click the link to authorize access.

Step 5 Click the ribbon to expand and use it.

What to do next

For information about ribbon features and how to use them, see the online help in SecureX.

Event Analysis with SecureX Threat Response

SecureX threat response was formerly known as Cisco Threat Response (CTR.)

Rapidly detect, investigate, and respond to threats using SecureX threat response, the integration platform in the Cisco Cloud that lets you analyze incidents using data aggregated from multiple products, including Secure Firewall.

- For general information about SecureX threat response, see:

  Cisco SecureX Threat Response product page.

- For detailed instructions for integrating Secure Firewall with SecureX threat response, see:
- See Cisco Secure Firewall Threat Defense and Cisco SecureX Threat Response Integration Guide.

View Event Data in SecureX Threat Response

Before you begin

- Set up the integration as described in the Cisco Secure Firewall Threat Defense and Cisco SecureX Threat Response Integration Guide.
- Review the online help in SecureX threat response to learn how to find, investigate, and take action on threats.
- You will need your credentials to access SecureX threat response.

Procedure

Step 1 In Secure Firewall Management Center, do the following:

- To pivot to SecureX threat response from a specific event:

  a. Navigate to a page under the **Analysis** > **Intrusions** menu that lists a supported event.

  b. Right-click a source or destination IP address and choose **Thereat Response IP**.

Step 2 Sign in to SecureX threat response as prompted.

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 **Analysis > 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 12.

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 11.

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 10.
- 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 **Analysis** > **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 (**Overview** > **Dashboards**), 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 Secure Firewall Threat Defense to related data in your Secure Network Analytics appliance. For more information about the Secure Network Analytics product, see Cisco Security Analytics and Logging product page.

For general information about contextual cross-launching, see Investigate Events Using Contextual Cross-Launch, on page 12.

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 11, but those links remain independent of the auto-created resources and you must manage them manually.

Before you begin

- You must have a deployed and running Secure Network Analytics appliance.
- If you are currently using syslog to send events to Secure Network Analytics from device versions that support sending events directly, disable syslog for those devices (or assign those devices an access control policy that does not include syslog configurations) to avoid duplicate events on the remote volume.
- You must have the following:
  - 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 Secure 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 .

Step 2 You have two options for Secure Network Analytics deployment:

- Manager Only—Deploy a standalone Manager to receive and store events, and from which you can review and query events.
- Data Store—Deploy a Cisco Secure Network Analytics Flow Collector to receive events, a Secure Network Analytics Data Store to store events, and a Manager from which you can review and query events.

Choose the deployment option and click **Start**.

Step 3 Complete the wizard. For more information, see the Secure Firewall Management Center Configuration section of Cisco Security Analytics and Logging Firewall Event Integration Guide.

Step 4 Verify your new cross-launch links: Select **Analysis** > **Advanced** > **Contextual Cross-launch**.

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 management center event viewer or dashboard, right-click a relevant event's table cell and choose the appropriate option.

It may take some time to process the queries, depending on the amount of data to process, speed of and demand on the Secure Network Analytics Manager, and so on.

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.

About Configuring the System to Send Security Event Data to Syslog

In order to configure the system to send security event syslogs, you will need to know the following:

- Best Practices for Configuring Security Event Syslog Messaging, on page 14
- Configuration Locations for Security Event Syslogs, on page 19
- *Threat Defense Platform Settings that Apply to Security Event Syslog Messages* in the Cisco Secure Firewall Management Center Device Configuration Guide
- If you make changes to syslog settings in any policy, you must redeploy for 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.

Device and Version	Configuration Location
Secure Firewall Threat Defense	**1.** Do the following to configure threat defense platform settings: (**Devices** > **Platform Settings** > **Threat Defense Settings** > **Syslog**.) **a.** Click **Devices** > **Platform Settings**. **b.** Edit the threat defense settings policy. **c.** In the left navigation pane, click **Syslog**. See also *Threat Defense Platform Settings That Apply to Security Event Syslog Messages* in the Cisco Secure Firewall Management Center Device Configuration Guide. **2.** In your access control policy Logging tab, opt to use the threat defense platform settings. **3.** (For intrusion events) Configure intrusion policies to use the settings in your access control policy Logging tab. (This is the default.) Overriding any of these settings is not recommended. For essential details, see Send Security Event Syslog Messages from Threat Defense Devices, on page 15.
All other devices	**1.** Create an alert response. **2.** Configure access control policy Logging to use the alert response. **3.** (For intrusion events) Configure syslog settings in intrusion policies. For complete details, see Send Security Event Syslog Messages from Classic Devices, on page 18.

Send Security Event Syslog Messages from 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 threat defense devices.

Note Many 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 threat defense device:

a) Click **Devices > Platform Settings**.
b) **Edit** the platform settings policy associated with your threat defense device.
c) In the left navigation pane, click **Syslog**.
d) 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.

e) Click **Syslog Settings** and configure the following settings:

- **Enable timestamp on syslog messages**
- **Timestamp Format**
- **Enable syslog device ID**

f) Click **Logging Setup**.
g) On the **Basic Logging Settings**, select whether or not to **Send syslogs in EMBLEM format**.
h) Click **Save**, to save your settings.

Step 2 Configure general logging settings for the access control policy (including file and malware logging):

a) Click **Policies > Access Control**.
b) Edit the applicable access control policy.
c) Click **More** > **Logging**.
d) Threat Defense 6.3 and later: Select **Use the syslog settings configured in the Threat Defense Platform Settings policy deployed on the device**.
e) (Optional) Select a **Syslog Severity**.
f) If you want to send file and malware events, select **Send Syslog messages for File and Malware events**.
g) Click **Save**.

Step 3 Enable logging for Security Intelligence events for the access control policy:

a) In the same access control policy, click the **Security Intelligence** tab.
b) 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**.

c) Click **Save**.

Step 4 Enable syslog logging for each rule in the access control policy:

a) In the same access control policy, click the **Access Control** > **Add Rule**.
b) Select a rule to edit.
c) Click the **Logging** tab in the rule.

d) 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.)

e) If you want to log file events, select **Log Files**.
f) Enable **Syslog Server**.
g) Verify that the rule is "**Using default syslog configuration in Access Control Logging**."
h) Click **Confirm**.
i) Repeat for each rule in the policy.

Step 5 If you send intrusion events:

a) Navigate to the intrusion policy associated with your access control policy.
b) In your intrusion policy, click **Advanced Settings** > **Syslog Alerting** > **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. 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.

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 policies and rules.

  See the applicable table rows in Configuration Locations for Syslogs for Connection and Security Intelligence Events (All Devices), on page 19.

  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 18.

- 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** > **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, click **Advanced Settings** > **Syslog Alerting** > **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 19. 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 threat defense devices, see Send Security Event Syslog Messages from Threat Defense Devices, on page 15.

Configuration Locations for Security Event Syslogs

- Configuration Locations for Syslogs for Connection and Security Intelligence Events (All Devices), on page 19
- Configuration Locations for Syslogs for Intrusion Events (Threat Defense Devices), on page 21
- Configuration Locations for Syslogs for Intrusion Events (Devices Other than Threat Defense), on page 22
- Configuration Locations for Syslogs for File and Malware Events, on page 22

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**	This option applies only to threat defense devices. 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. See Cisco Secure Firewall Management Center Device Configuration Guide.

Configuration Location	Description and More Information
Policies > **Access Control**, <each policy>, **Logging**	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. Recommended setting for threat defense devices: Use Threat Defense Platform Settings. For information, see Cisco Secure Firewall Management Center Device Configuration Guide. Required setting for all other devices: Use a syslog alert. If you specify a syslog alert, see Creating a Syslog Alert Response. For more information about the settings on the Logging tab, see Cisco Secure Firewall Management Center Device Configuration Guide.
Policies > **Access Control**, <each policy>, **Rules**, **Default Action** row, **Logging** ( )	Logging settings for the default action associated with an access control policy. See information about logging in Cisco Secure Firewall Management Center Device Configuration Guide and Logging Connections with a Policy Default Action.
Policies > **Access Control**, <each policy>, **Rules**, <each rule>, **Logging**	Logging settings for a particular rule in an access control policy. See information about logging in Cisco Secure Firewall Management Center Device Configuration Guide.
Policies > **Access Control**, <each policy>, **Security Intelligence**, **Logging** ( )	Logging settings for Security Intelligence Block lists. Click these buttons to configure: • DNS Block List Logging Options • URL Block List Logging Options • Network Block List Logging Options (for IP addresses on the blocked list) See Cisco Secure Firewall Management Center Device Configuration Guide
Policies > **SSL**, <each policy>, **Default Action** row, **Logging** ( )	Logging settings for the default action associated with an SSL policy. See Logging Connections with a Policy Default Action.
Policies > **SSL**, <each policy>, <each rule>, **Logging**	Logging settings for SSL rules. See Cisco Secure Firewall Management Center Device Configuration Guide.
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.

Configuration Location	Description and More Information
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 > **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 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 (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 > **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.
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 > **Access Control** > **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 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 threat defense are not configured there, syslogs will not be sent for devices other than 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 Threat Defense Platform Settings, you must also create an alert response. See Creating a Syslog Alert Response.
In Threat Defense Platform Settings: **Devices** > **Platform Settings**, Threat Defense Settings policy, **Syslog**	These settings apply only to threat defense devices running supported versions, and only if you configure the Logging tab in the access control policy to use 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 Threat Defense Platform Settings, you must also create an alert response. See Creating a Syslog Alert Response.

Anatomy of Security Event Syslog Messages

Example security event message from Threat Defense (Intrusion Event)

```
 0        1              2              3        4   5     6
___   ___________   ___________   _______   ___  __  ______

<37>2018-06-27 192.168.0.81 SFIMS : %FTD-5-43000
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 339
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Re
Message: "DCE2_EVENT   SMB_INVALID_DSIZE", Classi
Potentially Bad Traffic, User: No Authentication
Client: NetBIOS-ssn (SMB) client, ApplicationPro
(SMB), ACPolicy: test, NAPPolicy: Balanced Secur
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 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.

Item Number in Sample Message	Header Element	Description
1	Timestamp	Date and time the syslog message was sent from the device. • (Syslogs sent from 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. To configure the timestamp setting in Threat Defense Platform Settings, see Cisco Secure Firewall Management Center Device Configuration Guide.
2	Device or interface from which the message was sent. This can be: • IP address of the interface • Device hostname • Custom device identifier	(For syslogs sent from threat defense devices) 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. Otherwise, this element is not present in the header. To configure this setting in Threat Defense Platform Settings, see Cisco Secure Firewall Management Center Device Configuration Guide.
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

Item Number in Sample Message	Header Element	Description
5	Severity	The severity specified in the syslog settings for the policy that triggered the message. For severity descriptions, see *Severity Levels* in the Cisco Secure Firewall Management Center Device Configuration Guide or Syslog Severity Levels.
6	Event type identifier	• 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
--	Facility	See Facility in Security Event Syslog Messages, on page 25.
--	Remainder of message	Fields and values separated by colons. Fields with empty or unknown values are omitted from messages. For field descriptions, see: • Connection and Security Intelligence Event Fields. • Intrusion Event Fields • File and Malware Event Fields **Note** Field description lists include both syslog fields and fields visible in the event viewer (menu options under the Analysis menu in the management center web interface.) Fields available via syslog are labeled as such. 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.

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
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 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 management center	Stream Audit Logs to Syslog and the Audit and Syslog chapter
Device health and network-related logs from threat defense devices	Cisco Secure Firewall Management Center Device Configuration Guide
Connection, security intelligence, and intrusion event logs from threat defense devices	About Configuring the System to Send Security Event Data to Syslog, on page 14.
Connection, security intelligence, and intrusion event logs from Classic devices	About Configuring the System to Send Security Event Data to Syslog, on page 14
Logs for file and malware events	About Configuring the System to Send Security Event Data to Syslog, on page 14
IPS Settings	Send Syslog messages for IPS events. Configuration Locations for Syslogs for Intrusion Events (Threat Defense Devices), on page 21

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. For more information, see *Secure Firewall Management Center Event Streamer Integration Guide*.

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
Correlation and Allow List Events	correlation and compliance allow list events
Impact Flag Alerts	impact alerts generated by the 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 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 27.
Some event data can be sent only from management center. See Data Sent Only via eStreamer, Not via Syslog, on page 28.	Includes data that cannot be sent via syslog directly from devices. See Data Sent Only via eStreamer, Not via Syslog, on page 28.

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 27.
- 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 27.

    - 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 management center.

Procedure

Step 1 Choose **Integration** > **Other Integrations**.

Step 2 Click **eStreamer**.

Step 3 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 27.

Step 4 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 management center.

Procedure

Step 1 Choose **Integration** > **Other Integrations**.

Step 2 Click **eStreamer**.

Step 3 Click **Create Client**.

Step 4 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 5 If you want to encrypt the certificate file, enter a password in the **Password** field.

Step 6 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 7 Click **Download** ( ) next to the client hostname to download the certificate file.

Step 8 Save the certificate file to the appropriate directory used by your client for SSL authentication.

Step 9 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 (f.k.a. Firepower) app for Splunk (formerly known as the Cisco Firepower App for Splunk) as an external tool to display and work with Secure Firewall event data, to hunt and investigate threats on your network.

eStreamer is required. This is an advanced functionality. See eStreamer Server Streaming, on page 27.

For more information, see User Guide for Cisco Secure Firewall (f.k.a. Firepower) App for Splunk.

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 27.

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 Management Center	Minimum Threat Defense	Details
SecureX ribbon	7.0	Any	The SecureX ribbon pivots into SecureX for instant visibility into the threat landscape across your Cisco security products. To display the SecureX ribbon in management center, see the *Firepower and SecureX Integration Guide* at https://cisco.com/go/firepower-securex-documentation. New/Modified screens: New page: System > SecureX
Send all connection events to the Cisco cloud	7.0	Any	You can now send all connection events to the Cisco cloud, rather than just sending high-priority connection events. New/Modified screens: New option on the System > Integration > Cloud Services page
Cross-launch to view data in Secure Network Analytics	6.7	Any	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. New menu item: System > Logging > Security Analytics and Logging New page to configure sending events to Secure Network Analytics.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Contextual cross-launch from additional field types	6.7	Any	You can now cross-launch into an external application using the following additional types of event data: • Access control policy • Intrusion policy • Application protocol • Client application • Web application • Username (including realm) 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. Supported platforms: Secure Firewall Management Center
Integration with IBM QRadar	6.0 and later	Any	IBM QRadar users can use a new Firepower-specific app to analyze their event data. Available functionality is affected by your Firepower version. See Event Analysis in IBM QRadar, on page 31.

Enhancements to integration with SecureX threat response	6.5	Any	• Support for regional clouds:
			  • United States (North America)
			  • Europe
			
			• Support for additional event types:
			  • File and malware events
			  • High-priority connection events
			  These are connection events related to the following:
			  • Intrusion events
			  • Security Intelligence events
			  • File and malware events
			
			Modified screens: New options on **System** > **Integration** > **Cloud Services**.
			
			Supported Platforms: All devices supported in this release, either via direct integration or syslog.

Syslog	6.5	Any	The AccessControlRuleName field is now available in intrusion event syslog messages.

Feature	Minimum Management Center	Minimum Threat Defense	Details
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	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. Modified screens (version 6.4): New options on **System > Integration > Cloud Services**. Supported Platforms: Secure Firewall Threat Defense devices running version 6.3 (via syslog) or 6.4.
Syslog support for File and Malware events	6.4	Any	Fully-qualified file and malware event data can now be sent from managed devices via syslog. Modified screens: **Policies > Access Control > Access Control > Logging**. Supported Platforms: All managed devices running version 6.4.
Integration with Splunk	Supports all 6.x versions	Any	Splunk users can use a new, separate Splunk app, Cisco Secure Firewall (f.k.a. Firepower) app for Splunk, to analyze events. Available functionality is affected by your Firepower version. See Event Analysis in Splunk, on page 30.
Integration with Cisco Security Packet Analyzer	6.3	Any	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. New screens: **System** > **Integration** > **Packet Analyzer** **Analysis** > **Advanced** > **Packet Analyzer Queries** 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. Supported platforms: Secure Firewall Management Center
Contextual cross-launch	6.3	Any	Feature introduced: Right-click an event to look up related information in predefined or custom URL-based external resources. New screens: **Analysis** > **Advanced** > **Contextual Cross-Launch** New menu options: Multiple options when right-clicking on an event on Dashboard pages and event tables on pages under the Analysis menu. Supported platforms: Secure Firewall Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Syslog messages for connection and intrusion events	6.3	Any	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. Supported Platforms: • All new functionality: threat defense devices running version 6.3. • Some new functionality: Non-threat defense devices running version 6.3. • Less new functionality: All devices running versions older than 6.3. For more information, see the topics under About Sending Syslog Messages for Security Events, on page 14 and subtopics.
eStreamer	6.3	Any	Moved eStreamer content from the Host Identity Sources chapter to this chapter and added a summary comparing eStreamer to syslog.