

Monitor Cloud-Delivered Firewall Management Center-Managed Threat Defense Device Events

View events from Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center in Security Cloud Control.

- About Security Analytics and Logging, on page 1
- Comparison of SAL Remote Event Storage and Monitoring Options, on page 2
- About SAL (OnPrem), on page 2
- Manage SAL (OnPrem) for Security Cloud Control-Managed Firewall Threat Defense Devices, on page 3
- Configure SAL (OnPrem) Integration, on page 5
- Security Analytics and Logging for Firewall Threat Defense, on page 8
- Configure the SAL (SaaS) Integration, on page 8

About Security Analytics and Logging

Security Analytics and Logging (SAL) is a central log management and advanced threat detection service which delivers scalable Cisco firewall logging and correlated analytics. Central logging helps in providing visibility, helps troubleshoot network access issues including disruptions, and enables device and overall network health monitoring. Analytics provide detection against advanced threats.

The SAL service is available in the following two methods:

- Security Analytics and Logging (SaaS)—A hosted software as a service (SaaS) which stores events and provides data for security analytics. This service connects the Security Analytics and Logging cloud data store to the firewall cloud manager, Security Cloud Control (Security Cloud Control).

  In this documentation, this method is also referred to as SAL (SaaS).

- Security Analytics and Logging (On Premises)—A service that runs on the Secure Network Analytics appliances to store event logs at the customer's own premises. This service connects the Security Analytics and Logging (On Premises) data to the on-premises manager, Secure Firewall Management Center.

  In this documentation, this method is also referred to as SAL (OnPrem).

For more information about Security Analytics and Logging, see https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html.

Comparison of SAL Remote Event Storage and Monitoring Options

SAL integration shows similar options for storing event data externally to a Firewall Management Center and Security Cloud Control:

	SAL (OnPrem)	SAL (SaaS)
Why choose this solution?	You want to increase your on-premises firewall event data storage capacity, retain this data for a longer period, and export your event data to the Secure Network Analytics appliance.	You want to send firewall events to the Cisco cloud for storage and optionally make your firewall event data available for security analytics using integrated cloud services such as Cisco XDR.
Licensing	Purchase license and set-up the storage system behind your firewall. For more information, see Licensing for SAL (OnPrem), on page 3	Purchase license and a data storage plan and send your data to the Cisco cloud. For more information, see Licensing for SAL (SaaS), on page 8
Supported event types	• Connection • File and Malware • Intrusion • LINA • Security Intelligence	• Connection • File and Malware • Intrusion • Security Intelligence
Supported methods to send events	Supports both, syslog and direct integration.	Supports both, syslog and direct integration.
Event viewing	• View events on the Secure Network Analytics Manager. • Cross-launch from the Firewall Management Center event viewer to view events on the Secure Network Analytics Manager. • View remotely stored connection and security intelligence events in the management center.	View events in Security Cloud Control or Secure Network Analytics Manager, depending on your license. Cross-launch from the Firewall Management Center event viewer.

About SAL (OnPrem)

You can configure SAL (OnPrem) to store firewall event data for increased storage at a larger retention period. By deploying Secure Network Analytics appliances and integrating them with your firewall deployment, you can export your event data to a Secure Network Analytics appliance.

This provides you with the following capabilities:

- Store events on the Secure Network Analytics appliance.
- Specify this remote data source to view these events in the management center.
- Review event data from the Secure Network Analytics Manager (formerly Stealthwatch Management Console) Web App UI using the *Event Viewer*.
- Cross-launch from the management center UI to the *Event Viewer* to view additional context on the information from which you cross-launched.

Licensing for SAL (OnPrem)

You must obtain the Logging and Troubleshooting smart license to use SAL (OnPrem). You can obtain the license based on the amount of data you anticipate while sending the syslog data from your firewall deployment to your Secure Network Analytics appliance on a daily basis.

For information on licensing the Secure Network Analytics appliances, see Secure Network Analytics Smart Software Licensing Guide.

For information on the available SAL (OnPrem) licensing options, see the Cisco Security Analytics and Logging Ordering Guide.

Note For license calculation purposes, the amount of data is reported to the nearest whole GB. For example, If you send 4.9 GB in a day, it is reported as 4 GB.

Manage SAL (OnPrem) for Security Cloud Control-Managed Firewall Threat Defense Devices

Starting with Secure Firewall Threat Defense(formerly Firepower Threat Defense) version 7.2, you can choose to send fully qualified events that are generated by Security Cloud Control-managed Firewall Threat Defense devices to the Firewall Management Center. The Firewall Management Center receives and displays data analytics for these events. The Firewall Management Center receiving and displaying the event data is also referred to as an analytics-only management center. .

If your devices are enabled to send connection events to a Secure Network Analytics Manager using SAL (OnPrem), you can view and work with these remotely stored events in the management center event viewer and context explorer, and include them when generating reports. By deploying the Secure Network Analytics appliance and integrating it with the firewall deployment, you can export the event data to the Secure Network Analytics appliance. This allows you to view and manage the events in the management center UI. From the management center interface, you can also cross-launch to Secure Network Analytics Manager to view and manage the events data.

The management center can receive and display event analytics for the following Security Cloud Control-managed Firewall Threat Defense devices:

- New or existing Firewall Threat Defense devices onboarded to Security Cloud Control

For information on onboarding a Firewall Threat Defense device to Security Cloud Control, see Requirements: Prerequisites to onboard a device to Cloud-Delivered Firewall Management Center.

The workflow is as follows:

1. Onboard a Firewall Threat Defense device to Security Cloud Control.

   Onboard the Firewall Threat Defense devices using the onboarding methods that are described in Requirements: Prerequisites to onboard a device to Cloud-Delivered Firewall Management Center. The onboarding process includes assigning policies and choosing the appropriate licenses.

2. Register this Firewall Threat Defense device in the appropriate management center.

   For the management center to display events generated by a Security Cloud Control-managed Firewall Threat Defense device, you must register the Firewall Threat Defense device in the management center. To register this device in the Firewall Management Center, enable the device to be registered using the **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address*}*reg_key*[*nat_id*] CLI, and then add the device to the Firewall Management Center using the **Security Cloud Control Managed Device** check box.



Note The registration key and the NAT ID must be unique from those used while onboarding the device to Security Cloud Control.

   For more information, see *Add a Device to the Management Center* and *Complete the Threat Defense Initial Configuration Using the CLI* in Firepower Management Center Device Configuration Guide.

3. View events in the management center or cross-launch to a configured Secure Network Analytics Manager.

   To view and work with the events in the management center event viewer. If the Secure Network Analytics appliance is deployed and integrated with the firewall deployment, you can export the event data to the Secure Network Analytics appliance. This allows you to cross-launch from the management center UI to the Secure Network Analytics Manager to view and manage the events data.

   For more information, see *Events and Assets* and *Event Analysis Using External Tools*.

- Existing Firewall Threat Defense devices on the management center.

  You can change the management of the Firewall Threat Defense devices from management center to Security Cloud Control using the change threat defense manager functionality. The change threat defense manager functionality provides you to ability to change the management of Firewall Threat Defense devices from management center to Security Cloud Control. While changing the manager, you can choose to retain the events data generated by these threat defense devices on the management center. If you choose to retain the events data on the management center, a copy of the Firewall Threat Defense device in an analytics-only mode is retained on the management center.

  For more information, see Migrate Secure Firewall Threat Defense to Cloud.

  The workflow is as follows:

  1. Onboard the management center to Security Cloud Control

     To onboard the existing Firewall Threat Defense devices from management center to Security Cloud Control, you must onboard the appropriate management center to Security Cloud Control.

For more information, see Onboard an FMC.

2. Complete the change threat defense management process

   During the change threat defense management process, while changing the device manager, you can choose to retain events data generated by these Firewall Threat Defense devices on the management center.

   For more information, see Migrate Secure Firewall Threat Defense to Cloud.

3. View events in the management center or cross-launch to configured Secure Network Analytics appliance.

   To view and work with the events in the management center event viewer. If the Secure Network Analytics appliance is deployed and integrated with the firewall deployment, you can export the event data to the Secure Network Analytics appliance. This allows you to cross-launch from the management center UI to the Secure Network Analytics Manager to view and manage the events data.

   For more information, see Events and Assets and Event Analysis Using External Tools.

Configure SAL (OnPrem) Integration

Configure Security Cloud Control to send events to the Secure Network Analytics appliance.

Deploy a Cisco Secure Network Analytics Flow Collector to receive events, a Cisco Secure Network Analytics Data Store (containing 3 Cisco Secure Network Analytics Data Nodes) to store events, and a manager. The Firewall Threat Defense devices send event data to the flow collector from where the events are sent to the Data Store for storage. From the Cloud-Delivered Firewall Management Center user interface, you can cross-launch the manager to view more information about the stores events.

Starting with Firewall Threat Defense Version 7.2, you can choose to associate different flow collectors to different devices.

Configure a Secure Network Analytics Manager

Configure the Secure Network Analytics Manager deployment to integrate SAL (OnPrem) with Security Cloud Control-managed Firewall Threat Defense devices.

Before you begin

Ensure the following:

- You have a provisioned Security Cloud Control tenant and have the following Security Cloud Control user roles:
  - Admin
  - Super admin
- Your Firewall Threat Defense devices are working as expected and are generating events.
- If you are currently using syslog to send events to the Secure Network Analytics Manager 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 duplicating events on the remote volume.

- You have the hostname or the IP address of your Secure Network Analytics Manager.

Note You may be logged out of the Secure Network Analytics Manager during the registration process; complete any work in progress before you start with the deployment wizard.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 From the Security Cloud Control menu, navigate **Administration** > **Firewall Management Center** to open the **Services** page.

Step 3 Select **Cloud-Delivered FMC** and then click **Configuration**.

Step 4 Navigate to **Integration** > **Security Analytics & Logging**.

Step 5 In the **Secure Network Analytics Manager Only** widget, click **Start**.

Step 6 Enter the hostname or the IP address and port number of the Secure Network Analytics Manager and click **Next**.

Step 7 Deploy the changes to the managed devices.

The event data is not logged to the SAL (OnPrem) until the logging policy changes are deployed to the registered Firewall Threat Defense devices.

Note If you must change any of these configurations, run the wizard again. If you disable the configuration or run he wizard again, all settings except the account credentials are retained.

You can view and work with these remotely stored events in the event viewer and context explorer in the management center, and include them when generating reports. You can also cross-launch from an event in the management center to view related data on your Secure Network Analyticss appliance.

For more information, see the online help for the management center.

Step 8 Click **OK**.

Configure a Secure Network Analytics Data Store

Configure a Secure Network Analytics data store deployment to integrate SAL (OnPrem) with Firewall Threat Defense devices that are Security Cloud Control-managed.

Before you begin

Ensure the following:

- You have a provisioned Security Cloud Control tenant and have the following Security Cloud Control user roles:
  - Admin
  - Super admin
- Your Firewall Threat Defense devices are working as expected and generating events.
- If you are currently using syslog to send events to the Secure Network Analytics appliance 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.
- Gather the following information:
  - The hostname or the IP address of your Secure Network Analytics Manager.
  - The IP address of your flow collector.

Note You may be logged out of the Secure Network Analytics Manager during the registration process; complete any work in progress before you start with the deployment wizard.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 From the Security Cloud Control menu, navigate **Administration** > **Firewall Management Center** to open the **Services** page.

Step 3 Choose **Cloud-Delivered FMC** and click **Configuration**.

Step 4 Navigate to **Integration** > **Security Analytics & Logging**.

Step 5 In the **Secure Network Analytics Data Store** widget, click **Start**.

Step 6 Enter the hostname or the IP address and port number of the flow collector.

To add more flow collectors, click **+Add another Flow Collector**.

Step 7 If you have configured more than one flow collector, associate the managed devices with different flow collectors:

Note By default, all the managed devices are assigned to the default flow collector.

a) Click **Assign Devices**.
b) Select the managed devices that you want to assign.
c) From the reassign device drop-down list, choose the flow collector.

If you do not want a managed device to send event data to any of the flow collectors, select that device, and choose **Do not log to flow collector from the reassign device drop-down list.**

You can change the default flow collector by hovering over the intended flow collector and clicking **Set default**.

d) Click **Apply Changes**.
e) Click **Next**.

Step 8 Click **Next**.

Step 9 Deploy the changes to the registered managed devices.

The event data is not logged to the SAL (OnPrem) until the logging policy changes are deployed to the registered Firewall Threat Defense devices.

Note If you must change any of these configurations, run the wizard again. If you disable the configuration or run he wizard again, all settings except the account credentials are retained.

You can view and work with these remotely stored events in the event viewer and context explorer in the management center, and include them when generating reports. You can also cross-launch from an event in the management center to view related data on your Secure Network Analytics Manager.

For more information, see the online help for the management center.

Security Analytics and Logging for Firewall Threat Defense

SAL (SaaS) is a cloud-based security service that

- captures connection, intrusion, file, malware, and Security Intelligence events from all Firewall Threat Defense devices
- stores events in the Cisco cloud for centralized viewing in Security Cloud Control, and
- provides filtering and review capabilities through the **Event Logging** page to help understand what security rules are triggering in your network.

Additional capabilities

Licensing for SAL (SaaS)

The SAL (SaaS) licenses allows you to use a Security Cloud Control tenant to view firewall logs from all your managed devices at one place. For details on the available SAL (SaaS) licensing options, see the Cisco Security Analytics and Logging Ordering Guide.

Configure the SAL (SaaS) Integration

To deploy this integration, you must set up event data storage in SAL (SaaS) using either syslog or a direct connection.

- Send Cloud-Delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog, on page 11
- Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection, on page 13

Requirements and guidelines

Requirements: Cisco Secure Firewall Threat Defense

Ensure that your environment meets these device and system requirements for Firewall Threat Defense integration.

- Security Cloud Control-managed standalone Firewall Threat Defense devices, Version, 7.2 and later.
- To send events using syslog, you must have Firewall Threat Defense device, Version 6.4 or later.
- To send events directly, you must have Firewall Threat Defense device, Version 7.2 or later.
- To optionally exclude individual Firewall Threat Defense devices from sending events directly, you must have Firewall Threat Defense device, Version 7.4.1 or later.
- Your firewall system must be deployed and successfully generating events.

Requirements: regional cloud configuration

Select the appropriate regional cloud for your event management and ensure consistency across your security integrations.

- Determine the regional cloud that you want to send events to.
- Events cannot be viewed from or moved between different regional clouds.
- If you use a direct connection to send events to the Cisco Security Cloud for integration with Cisco SecureX, or Cisco SecureX threat response, or Cisco XDR, you must use the same cloud region for this integration.
- If you send events directly, the regional cloud you specify in Security Cloud Control must match the region of your Security Cloud Control tenant.

Requirements: Security Analytics and Logging subscription plan

Obtain and configure the appropriate Security Analytics and Logging subscription plan for your event volume requirements.

- You must have a valid Security Analytics and Logging subscription plan. For more information about the subscription plans, see Security Analytics and Logging Licenses.
- If your do not have a Security Analytics and Logging plan subscribed, you can request a 90-day trial by logging in to Security Cloud Control and navigating to **Events & Logs** > **Events** > **Event Logging** tab. You can purchase the desired subscription plan by following the instructions in the Security Cloud Control Firewall Management Ordering Guide.
- You must buy a data plan that reflects the number of events the Cisco cloud receives from your threat defense devices daily. This is called your daily ingest rate.

- Use the Logging Volume Estimator Tool to estimate your data storage requirements.

Requirements: account configuration

When you purchase a license for this integration, you are provided with a Security Cloud Control tenant account to support the integration.

Requirements: connectivity

The Firewall Threat Defense devices must be able to connect outbound on port 443 to the Cisco Security Cloud at the addresses specified for your regional cloud.

- US region:
  - api-sse.cisco.com
  - mx*.sse.itd.cisco.com
  - dex.sse.itd.cisco.com
  - eventing-ingest.sse.itd.cisco.com
  - registration.US.sse.itd.cisco.com
  - US.manage.security.cisco.com
  - edge.US.cdo.cisco.com
- EU region:
  - api.EU.sse.itd.cisco.com
  - mx*.EU.sse.itd.cisco.com
  - dex.EU.sse.itd.cisco.com
  - eventing-ingest.EU.sse.itd.cisco.com
  - registration.EU.sse.itd.cisco.com
  - EU.manage.security.cisco.com
  - edge.EU.cdo.cisco.com
- Asia (APJ) region:
  - api.APJ.sse.itd.cisco.com
  - mx*.APJ.sse.itd.cisco.com
  - dex.APJ.sse.itd.cisco.com
  - eventing-ingest.APJ.sse.itd.cisco.com
  - registration.APJ.sse.itd.cisco.com
  - APJ.cdo.cisco.com
  - edge.APJ.cdo.cisco.com

- Australia region:
  - api.aus.sse.itd.cisco.com
  - mx*.aus.sse.itd.cisco.com
  - dex.au.sse.itd.cisco.com
  - eventing-ingest.aus.sse.itd.cisco.com
  - registration.au.sse.itd.cisco.com
  - aus.cdo.cisco.com
- India region:
  - api.in.sse.itd.cisco.com
  - mx*.in.sse.itd.cisco.com
  - dex.in.sse.itd.cisco.com
  - eventing-ingest.in.sse.itd.cisco.com
  - registration.in.sse.itd.cisco.com
  - in.cdo.cisco.com

Send Cloud-Delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog

This task enables your Cloud-Delivered Firewall Management Center-managed devices to send security events (connection, security intelligence, intrusion, file, and malware events) directly to SAL (SaaS) using syslog messages.

This procedure provides information about the configuration for sending syslog messages for security events (connection, security intelligence, intrusion, file, and malware events) from devices managed by Security Cloud Control.

Before you begin

- Configure policies to generate security events, and verify that the events you expect to see are displayed in the applicable tables under the **Events & Logs** menu.
- Gather information relating to the syslog server IP address, port, and protocol (UDP or TCP).
- Ensure that your devices can reach the syslog server.

Procedure

Step 1 In the left pane, click **Administration** > **Firewall Management Center** to open the **Services** page.

Step 2 Click and select **Cloud-Delivered FMC** and then click **Configuration**.

Step 3 Configure the syslog settings for your threat defense device:

a) Click **Devices** > **Platform Settings** and edit the platform settings policy that is associated with your threat defense device.

b) In the left-side navigation pane, click **Syslog** and configure the syslog settings as follows:

Click this UI Element...	To Do the Following:
Logging Setup	Enable logging, specify FTP server settings, and the Flash usage.
Logging Destination	Enable logging to specific destinations and to specify filtering by message severity level, event class, or by a custom event list.
E-mail Setup	Specify the email address that is used as the source address for syslog messages that are sent as emails.
Events Lists	Define a custom event list that includes an event class, a severity level, and an event ID.
Rate Limit	Specify the volume of messages being sent to all the configured destinations and define the message severity level to which you want to assign the rate limits.
Syslog Settings	Specify the logging facility, enable the inclusion of a time stamp, and enable other settings to set up a server as a syslog destination.
Syslog Servers	Specify the IP address, protocol that is used, format, and security zone for the syslog server that is designated as a logging destination.

c) Click **Save**.

Step 4 Configure the general logging settings for the access control policy (including file and malware logging):

a) Click **Policies** > **Access Control** and then edit the access control policy that is associated with your threat defense device.

b) Click **More** and then choose **Logging**. Configure the general logging settings for the access control policy (including file and malware logging) as follows:

Click this UI Element...	To Do the Following:
Send using specific syslog ALERT	Select a syslog ALERT from the list of existing predefined alerts or add one by specifying the name, logging host, port, facility, and severity.
Use the syslog settings configured in the FTD Platform Settings policy deployed on the device	Unify the syslog configuration by configuring it in **Platform Settings** and reuse the settings in the access control policy. The selected severity is applied to all the connection and intrusion events. The default severity is **ALERT**.

Click this UI Element...	To Do the Following:
Send Syslog messages for IPS events	Send events as syslog messages. The default syslog settings are used unless you override them.
Send Syslog messages for File and Malware events	Send file and malware events as syslog messages. The default syslog settings are used unless you override them.

c) Click **Save**.

Step 5 Enable logging for security intelligence events for the access control policy:

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

b) Click the logging icon and enable security intelligence logging using these criteria:

- By Domain Name: Click the logging icon next to the **DNS Policy** drop-down list.
- By IP address: Click the logging icon next to **Networks**.
- By URL: Click the logging icon next to **URLs**.

c) Click **Save**.

Step 6 Enable syslog logging for each rule in the access control policy:

a) In the same access control policy, click the **Access Control** tab, and click a rule to edit.

b) Click the **Logging** tab in the rule.

c) Check the **Log at beginning of connection** and **Log at end of connection** check boxes.

d) If you want to log file events, check the **Log Files** check box.

e) Check the **Syslog Server** check box.

f) Verify that the rule is **Using default syslog configuration in Access Control Logging**.

g) Click **Confirm**.

h) Click **Apply** to save the rule.

i) Repeat steps 7.a through 7.h for each rule in the policy and click **Save** to save the policy.

Step 7 If you have made all the required changes, deploy your changes to the managed devices.

Your Cloud-Delivered Firewall Management Center-managed devices now send intrusion, file, malware, and connection events to SAL (SaaS) using syslog messages. Security events should appear in the configured syslog server.

Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection

This task enables the Cloud-Delivered Firewall Management Center to send events directly to SAL (SaaS) by configuring the Cisco cloud event global setting.

This procedure enables the Cisco cloud event global setting in the Cloud-Delivered Firewall Management Center. When needed, you can exclude individual Firewall Threat Defense devices from sending event logs to SAL (SaaS). For more information, see Enable or Disable Threat Defense Devices to Send Event logs to SAL (SaaS) Using a Direct Connection.

Before you begin

- Onboard devices to the Cloud-Delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Administration** > **Firewall Management Center**.

Step 3 Click **Cloud-Delivered FMC**, and in the **System** pane that is located at the right-side, click **Cisco Cloud Events**.

Step 4 In the **Configure Cisco Cloud Events** widget, do the following:

a. Click the **Send Events to the Cisco Cloud** toggle button to enable the overall configuration.

b. Check the **Send Intrusion Events to the cloud** check box to send the intrusion events to the cloud.

Note When you enable sending intrusion events, the Firewall Threat Defense device sends the captured packet data to the cloud along with the intrusion events. Cisco 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.

c. Check the **Send File and Malware Events to the cloud** check box to send the file and malware events to the cloud.

d. Choose an option to send the connection events to the cloud:

- Click the **None** radio button to not send connection events to the cloud.
- Click the **Security Events** radio button to send only security intelligence events to the cloud.
- Click the **All** radio button to send all the connection events to the cloud.

e. Click **Save**.

The Cloud-Delivered Firewall Management Center is now configured to send the selected event types directly to SAL (SaaS).

Enable individual threat defense devices to send events to SAL (SaaS) using a direct connection

Enable or disable FTD devices managed by the Cloud-Delivered Firewall Management Center to send events directly to SAL (SaaS). This device-level control allows you to optionally exclude specific FTD devices from

sending event logs to the Cisco cloud to reduce traffic or to maintain a combination of SAL and on-premises event log storage.

Note

- To enable or disable sending events to the Cisco cloud from the FTD devices, enable the Cisco cloud event global setting in the Cloud-Delivered Firewall Management Center. For more information on enabling the Cisco cloud event global setting, see Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection, on page 13.

  Sending events to the Cisco cloud is enabled by default for all FTD devices when the Cisco cloud event global setting is enabled in the Cloud-Delivered Firewall Management Center.

- The option to enable or disable FTD devices to send event logs to the cloud is supported on FTD Version 7.4.1 or later.

Before you begin

- Onboard devices to the Cloud-Delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

Step 1 Log in to Security Cloud Control.
Step 2 From the left pane, click **Security Devices**.
Step 3 Click the **Devices** tab to view the device.
Step 4 Click the **FTD** tab to view FTD devices.
Step 5 Choose the FTD devices whose configurations you want to edit, from the **Security Devices** list.
Step 6 In the **Device Management** pane, click **Cloud Events**.
Step 7 Click the **Send Events to the Cisco Cloud** toggle button to enable or disable the configuration.
Step 8 Click **Save**.

The FTD device configuration is updated to enable or disable sending events directly to SAL (SaaS).

View and Work with Events in Security Cloud Control

Procedure

Step 1 Log in to Security Cloud Control.
Step 2 From the Security Cloud Control menu, choose **Events & Logs** > **Events** > **Event Logging**.
Step 3 Use the **Historical** tab to view all historical events data. By default, the viewer displays this tab.

Step 4 To view the live events, click the **Live** tab.

What to do next

For more information about what you can do on this page, see the Security Cloud Control online help.

View AI Defense Events in Security Cloud Control

View AI Defense events in Security Cloud Control to monitor activities within your AI environment, including prompts submitted, responses generated, and any triggered AI Defense policy violations.

AI Defense events record activities within your AI environment. They capture interactions such as prompts submitted, responses generated, and any triggered AI Defense policy violations. Each event includes key information, such as the application and AI model involved, the specific rule triggered, and the action taken.

Before you begin

- Enable the AI Defense service in your Security Cloud Control tenant. For information on enabling the AI Defense service, see the AI Defense User Guide.
- You must be managing Firewall Threat Defense devices with Version 10.0 or higher.
- Enable your Firewall Threat Defense device to send events to the cloud. For more information, see Send Cloud-Delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection, on page 13.

Follow these steps to view AI Defense events in Security Cloud Control:

Procedure

Step 1 In the navigation pane, choose **Events & Logs** > **Events** > **Event Logging**.

Step 2 Click the filter icon ( ).

Step 3 Check the **AI Defense** check box.

AI Defense events are displayed in the event logging interface, showing activities within your AI environment including prompts, responses, and policy violations.