

Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide

First Published: 2024-09-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

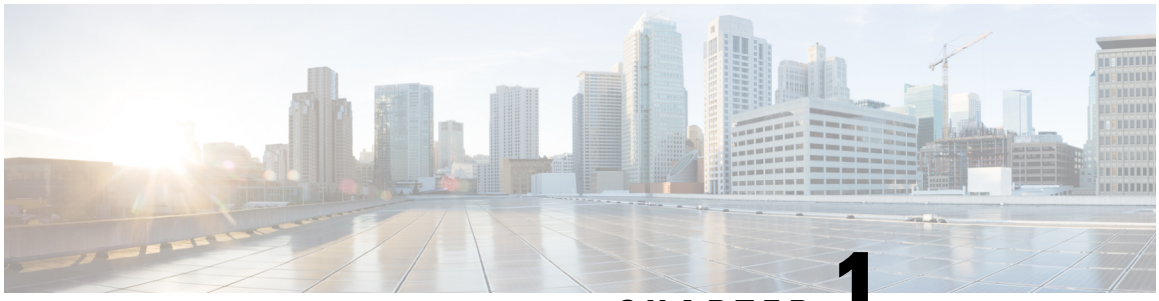
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Introduction to Integrating Secure Firewall Threat Defense and Cisco XDR

- About Secure Firewall Threat Defense and Cisco XDR Integration, on page 1
- Regional Clouds, on page 2
- Supported Event Types, on page 3
- Comparison of Methods for Sending Events to the Cloud, on page 3

About Secure Firewall Threat Defense and Cisco XDR Integration

Integrate Secure Firewall Threat Defense with Cisco Extended Detection and Response (Cisco XDR) to connect Cisco's integrated security portfolio and your firewall deployment for a consistent experience that unifies visibility, enables automation, and strengthens your security across network.

About Cisco XDR

Cisco XDR is a cloud-based solution that unifies visibility by correlating detections across multiple telemetry sources, and enables security teams to detect, prioritize, and respond to the most sophisticated threats.

By integrating your firewall deployment with Cisco XDR, you can:

- Correlate and analyze the firewall events to determine end-to-end incidents and promote incident on the basis of risk to enable analysts to focus on what needs to be addressed with urgency.
- Enhances threat detection and response capabilities through clear prioritization of alerts and providing the shortest path from detection to response.
- Remediate threats confidently using automation and guided response recommendations.

For more information about Cisco XDR, see Cisco XDR Help Center.

Note Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses required for Cisco Secure Firewall products. For more information, see Cisco XDR Licenses.

Regional Clouds

Table 1: URLs of the Regional Clouds

Region	Link to the Cloud	Supported Integration Methods and Firewall Threat Defense Device Version
North America	• api-sse.cisco.com • mx*.sse.itd.cisco.com • eventing-ingest.sse.itd.cisco.com • us.manage.security.cisco.com	• Direct integration: Version 6.4 and later • Integration using syslog: Version 6.3 and later
Europe	• api.eu.sse.itd.cisco.com • mx*.eu.sse.itd.cisco.com • eventing-ingest.eu.sse.itd.cisco.com • eu.manage.security.cisco.com	• Direct integration: Version 6.5 and later • Integration using syslog: Version 6.3 and later
Asia (APJC)	• api.apj.sse.itd.cisco.com • mx*.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com • apj.manage.security.cisco.com	• Direct integration: Version 6.5 and later • Integration using syslog: Version 6.3 and later
Australia	• api.aus.sse.itd.cisco.com • mx*.aus.sse.itd.cisco.com • eventing-ingest.aus.sse.itd.cisco.com • aus.manage.security.cisco.com	• Direct integration: Version 6.5 and later • Integration using syslog: Version 6.3 and later
India	• api.in.sse.itd.cisco.com • mx*.in.sse.itd.cisco.com • eventing-ingest.in.sse.itd.cisco.com • in.manage.security.cisco.com	• Direct integration: Version 6.5 and later • Integration using syslog: Version 6.3 and later

Guidelines and Limitations for Choosing a Regional Cloud

While choosing a regional cloud, keep in mind that:

- Choosing a regional cloud depends on your Firewall Threat Defense device versions, and integration method (syslog or direct).

For a list of regional clouds and their URLs, see Regional Clouds.

- When possible, use the regional cloud nearest to your deployment.
- You cannot merge or aggregate data in different regional clouds. To aggregate data from multiple regions, devices in all the regions must send data to the same regional cloud.
- You can create an account on each regional cloud, and the data on each cloud remains separate.
- The regional cloud you select is also used for the Cisco Support Diagnostics and Cisco Support Network capabilities. This setting also governs the cloud region for the Secure Network Analytics cloud using Security Analytics and Logging (SaaS).

Supported Event Types

The Firewall Threat Defense and Cisco XDR integration supports the following event types:

Table 2: Supported Event Types for Sending Events to the Security Cloud Control

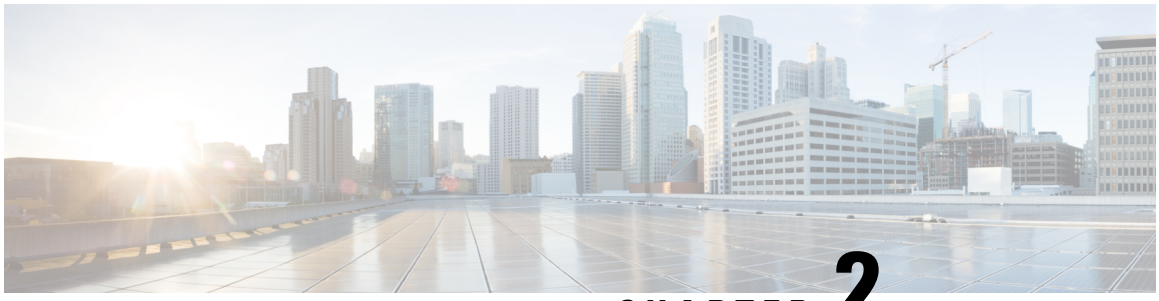
Event Type	Supported Firewall Threat Defense Device Version for Direct Integration	Supported Firewall Threat Defense Device Version for Syslog Integration
Intrusion events	6.4 and later	6.3 and later
Following high-priority connection events: • Security-related connection events. • Connection events related to file and malware events. • Connection events related to intrusion events.	6.5 and later	Not supported
File and malware events	6.5 and later	Not supported

Comparison of Methods for Sending Events to the Cloud

The Firewall Threat Defense devices send events to the cloud through the Security Services Exchange portal, either using syslog or directly.

Sending Events Directly	Sending Events Using Syslog
Supports only Firewall Threat Defense devices running supported versions of software.	Supports all devices running supported versions of software.
Supports version 6.4 and later.	Supports version 6.3 and later.

Sending Events Directly	Sending Events Using Syslog
Supports all event types listed.	Supports only intrusion events.
Threat defense devices must be connected to the internet.	Devices do not need to be connected to the internet.
Your deployment cannot be using a Smart Software Manager on-premises server (formerly known as a Smart Software Satellite Server).	Your deployment can be using a Smart Software Manager on-premises server.
No need to set up and maintain an on-premises proxy server.	Requires an on-premises virtual Cisco Security Service Proxy server. More information about this proxy server, see Cisco Security Services Proxy. To access Security Services Exchange, see Access Security Service Exchange.



CHAPTER 2

Account Requirements

- Account Required for Cisco XDR Integration, on page 5
- Get an Account for Enabling Cisco XDR Integration, on page 5
- Manage Access to Your Cloud Accounts, on page 6

Account Required for Cisco XDR Integration

To integrate the Firewall Management Center with Security Cloud Control and send events to Cisco XDR, you must have one of these regional cloud accounts:

- Security Cloud Sign On account.
- Secure Endpoint account.
- Secure Malware Analytics account.
- Security Cloud Control account.

Important If you or your organization already has any of the above accounts on the regional cloud, use the existing account. Do not create a new account. Remember that the data associated with an account is available only to that account.

If you do not have an account, see Get an Account for Enabling Cisco XDR Integration, on page 5.

For direct integration, you require a Security Cloud Control organization to register your management center and the managed devices. If you do not already have a Security Cloud Control organization, request one. For more information, refer to Provision Security Cloud Control Firewall Management.

Get an Account for Enabling Cisco XDR Integration

Before you begin

If you or your organization already has an account on the regional cloud you want to use, do not create a new account. Use the existing account for sending firewall event data to Cisco XDR. For supported account types, see Account Required for Cisco XDR Integration, on page 5. If anyone else in your organization already

has an account for that regional cloud, then have the administrator of that account add an account for you. For instructions, see Manage Access To Your Security Cloud Control Account, on page 6.

Procedure

Step 1 Determine which regional cloud you want to use. For more information, refer to Guidelines and Limitations for Choosing a Regional Cloud, on page 2.

Step 2 If you do not have a Security Cloud Sign On account and you want to create one, go to your chosen regional cloud. For a list of regional clouds and their URLs, refer to Regional Clouds, on page 2.

Step 3 Click **Sign up now**.

For more information about creating a security cloud sign on account, refer to Provision Security Cloud Control Firewall Management.

Manage Access to Your Cloud Accounts

Managing user accounts varies based on the type of cloud account you have.

Note If you access the cloud using a Secure Malware Analytics or Secure Endpoint account, see the documentation for those products.

Manage Access To Your Security Cloud Control Account

If you are using Security Cloud Control account to access the Security Cloud Control, use this procedure to manage users.

Before you begin

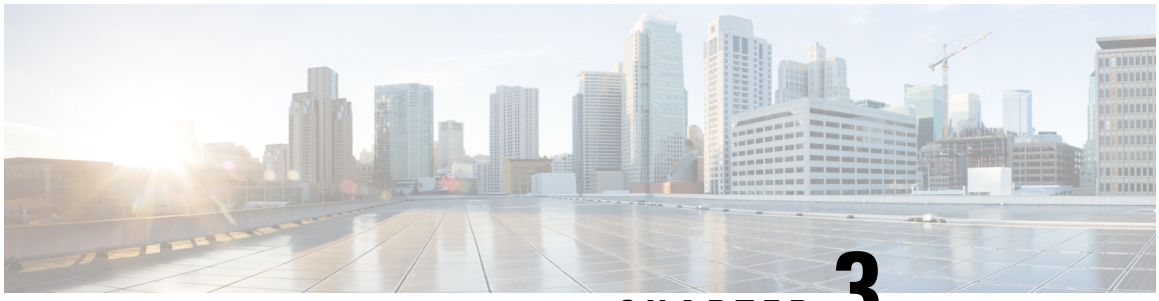
You must have **Super Admin** privileges in Security Cloud Control to perform this task.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 From the Security Cloud Control navigation bar, click **Settings** > **User Management**.

See the Security Cloud Control online help to know more about the user management in Security Cloud Control.



CHAPTER 3

Send Events to the Cloud Directly

- About Direct Integration, on page 7
- Requirements for Direct Integration, on page 7
- High Availability Deployment and Security Cloud Control Integration, on page 11
- How to Send Events Directly to the Security Cloud Control and Integrate with Cisco XDR, on page 12
- Troubleshoot a Direct Integration, on page 23

About Direct Integration

Starting from Firewall Threat Defense release 6.4, you can configure your Firewall Threat Defense devices to send supported firewall events directly to the Security Cloud Control. The devices send events to the Security Services Exchange, from where the events can be promoted to various cloud services, including Cisco XDR, to improve your event analysis and investigations.

Requirements for Direct Integration

Requirement Type	Requirement
Secure Firewall Version	• Firewall Threat Defense version 6.4 or later for US cloud. • Firewall Threat Defense version 6.5 or later for Europe, APJC, India, and Australia clouds. • Firewall Management Center version from 7.0.2 to 7.0.x, or version 7.2.0 and later.

Requirement Type	Requirement
Licensing	• Your firewall deployment must be licensed to generate the events that you want to send to Security Cloud Control For details, see Cisco Secure Firewall Licensing Information. • Your environment cannot be using a Cisco Smart Software Manager On-Prem server (formerly known as Smart Software Satellite Server) or be deployed in an air-gapped environment. • Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses for Cisco Secure Firewall products. For more information, see Cisco XDR Licenses. • If you were already sending events to the Security Cloud Control using a SecureX subscription, you can continue to send events to Cisco XDR. However, if you now register your Firewall Management Center to the cloud tenancy using your Security Cloud Control account, your Security Cloud Control account must have a Security Analytics and Logging license to send events to Cisco XDR.

Requirement Type	Requirement
Connectivity	

Requirement Type	Requirement

	The Firewall Management Center and the managed devices must be able to connect outbound on port 443 to the Security Cloud Control at the following addresses:
	• 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
	• 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
	• Asia (APJC) 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.manage.security.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.manage.security.cisco.com

Requirement Type	Requirement
	• 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.manage.security.cisco.com
General	Your firewall deployment is generating events as expected.

High Availability Deployment and Security Cloud Control Integration

The following describes the guidelines for integrating firewall high availability deployment with Security Cloud Control.

- To integrate Firewall Threat Defense high availability or cluster deployment with Security Cloud Control, you must integrate all peers with Security Services Exchange.
- Security Services Exchange integration requires all Firewall Threat Defense devices in the high availability deployment to have connectivity to the internet.
- When integrating a Firewall Management Center high availability deployment with Security Cloud Control, you must enable Security Cloud Control integration in the active peer.
- If you promote the standby Firewall Management Center peer to the active role, the Security Cloud Control integration gets transferred between the active and standby peers.
- If you break Firewall Management Center high availability deployment, both the peers remain integrated with Security Cloud Control.

For more information about configuring and managing a high availability deployment, see the High Availability section in *Cisco Secure Firewall Management Center Administration Guide*.

How to Send Events Directly to the Security Cloud Control and Integrate with Cisco XDR

	Do This	More Information
Step 1	Decide the following: • Types of events you want to send to the cloud. • The method of sending events. • The regional cloud to use for sending the events.	See About Secure Firewall Threat Defense and Cisco XDR Integration, on page 1.
Step 2	Meet the requirements for direct integration.	See Requirements for Direct Integration, on page 7.
Step 3	Access Security Services Exchange, the cloud portal that you will use for managing devices and filtering events for the Cisco XDR integration.	See Access Security Services Exchange, on page 22.
Step 4	In Security Services Exchange, enable the eventing service.	Click **Cloud Services** and enable the following options: • **Cisco SecureX threat response or Cisco XDR** • **Eventing**
Step 5	If you are using Security Cloud Control to manage configurations on your Firewall Threat Defense device or to register your devices with Security Cloud Control, merge your Security Cloud Control account with the Security Services Exchange account you use for this integration.	See Link Your Security Cloud Control and Security Services Exchange Accounts, on page 13.
Step 6	If you are using Smart Licensing account to register your devices with Security Cloud Control, link your Smart Licensing account with the Security Services Exchange account you use for this integration.	See Link Smart Licensing Accounts with Security Services Exchange, on page 14.
Step 7	In your firewall manager, enable integration with the Security Cloud Control.	• For devices managed by the Firewall Device Manager, see: Configure the Firewall Device Manager to Send Events Directly, on page 15 • For devices managed by the Firewall Management Center, see: Configure Firewall Management Center to Send Events Directly, on page 16

	Do This	More Information
Step 8	In Security Services Exchange, configure the system to automatically promote significant events.	**Important** If you do not automate event promotion, you may need to manually review and promote events in order to view them in Security Services Exchange. For more information, see *About Promoting Events to Incidents* in the Security Services Exchange Online Help
Step 9	(Optional) In Security Services Exchange, configure automatic deletion of certain non-significant events.	For more information, see *Events* in the Security Services Exchange Online Help
Step 10	Verify that your integration is set up correctly. If necessary, troubleshoot issues.	See: • Verify that Events Reach Security Services Exchange Using Direct Connection, on page 23 • Troubleshoot a Direct Integration, on page 23
Step 11	In Cisco XDR, verify that promoted events appear as expected in the Incident Manager.	For instructions, see Cisco XDR Help Center.

Link Your Security Cloud Control and Security Services Exchange Accounts

If your register your Firewall Threat Defense device with Security Cloud Control using Security Cloud Control account and you want to send events to Security Services Exchange, you must link your Security Cloud Control account with the Security Services Exchange account.

Note that only one Security Cloud Control account can be linked with one Security Services Exchange account. If you have tenant accounts on more than one regional cloud, you must link tenant accounts separately for each regional cloud.

Note This operation is not reversible.

Before you begin

- You must be able to sign in to Security Cloud Control and to the applicable regional cloud with your Security Cloud Sign On account.
- Your Security Cloud Control account must have **Admin** or **Super Admin** privileges.
- Your Security Services Exchange account must have **Admin** privileges.

Procedure

Step 1 Sign in to the Security Cloud Control account that contains the tenant you wish to link with Security Services Exchange.

Step 2 Choose the tenant to link with Security Services Exchange.

Step 3 Generate a new API token for your account:

a) From the user menu on the top-right corner of the window, select **Settings**.

b) In the **My Tokens** section, click **Generate API Token** or **Refresh**.

c) Copy the token.

For more information about API tokens, see API Tokens.

Step 4 In Security Services Exchange, click the **Tools** () icon on the top-right and click **Link CDO Account**.

Step 5 Paste the token that you copied from Security Cloud Control.

Step 6 Verify that you are linking the tenant that you intended to link.

Step 7 Click **Link CDO Account**.

Step 8 Sign out of your Security Cloud Control account, and then sign back in.

What to do next

- Events generated by devices before linking tenants will have a different device ID than events generated by the same device after linking tenants.
- If you do not need to map events to the devices that generated them, you can delete the "Unregistered" device entries for devices that are now associated with the linked tenant.

Link Smart Licensing Accounts with Security Services Exchange

To integrate products registered under different Smart Licensing accounts into a single view in the cloud, you must link those Smart Licensing accounts to the Security Services Exchange tenant.

Before you begin

To link Smart Licensing accounts, you must have administrator-level privileges for all of the Smart Licensing accounts and the Security Services Exchange tenant that you are using for this integration.

Procedure

Step 1 In the top right corner of any page in Security Services Exchange, click the **Tools** button () and choose **Link Smart/Virtual Accounts**.

Step 2 Click **Link more accounts**.

Step 3 Select the accounts to integrate with this cloud account.

Step 4 Click **Link Smart/Virtual Accounts**.

Step 5 Click **OK**.

Configure the Firewall Device Manager to Send Events Directly

Note Available options depend on your **Firewall Device Manager** version. Skip any step that is not applicable to your version. For example, the ability to select region and event types are version-dependent.

Before you begin

- Register the device with cloud services before you continue with this procedure. For more information, see *Configuring Cloud Services* section in *Cisco Secure Firewall Device Manager Configuration Guide*.
- If you are using Security Cloud Control register your device with cloud services, link your Security Cloud Control account with the Security Services Exchange tenant. For more information, see Link Your Security Cloud Control and Security Services Exchange Accounts, on page 13.
- If you are using Smart License to register your device with cloud services, link your Smart Licensing account with the Security Services Exchange tenant. For more information, see Link Smart Licensing Accounts with Security Services Exchange, on page 14
- In the Firewall Device Manager:
  - Make sure that your device has a unique name. If not, click **Devices** > **System Settings** > **Hostname** and assign a name.
  - Verify that the Firewall Threat Defense device is successfully generating events.
- Make sure you have your Cisco Security Cloud Sign On credentials and can sign in to the regional cloud on which your account was created.

Procedure

Step 1 In the Firewall Device Manager: Click **Device**, then click the **System Settings** > **Cloud Services** link.

Step 2 Click **Enable** for the **Send Events to the Cisco Cloud** option.

Step 3 Select the types of events to send to the cloud and click **OK**. Later, you can change the event selection by clicking **Edit** next to the list of selected events.

If you choose to send connection events, only security-related connection events are used in this integration.

Step 4 Verify that your device has registered successfully in Security Services Exchange:

a) If you do not already have Firewall Device Manager open in a browser window, see Access Security Services Exchange, on page 22.

b) In Security Services Exchange, click **Devices**.

c) Verify that your Firewall Threat Defense device appears in the list.

Note
The description shown for the Firewall Threat Defense device in the **Devices** list is the serial number, which matches the serial number shown if you run the **show running-config** command in the command-line interface of the device.

Configure Firewall Management Center to Send Events Directly

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

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

Note Your Firewall Management Center must be between version 7.0.2 and 7.0.x, or version 7.2 and later to integrate Firewall Management Center with Security Cloud Control.

For more information about integrating Firewall Management Center with Security Cloud Control, see Integrate Firewall Management Center With Security Cloud Control, on page 16.

Integrate Firewall Management Center With Security Cloud Control

This procedure describes how to integrate the Firewall Management Center with Security Cloud Control. By enabling Security Cloud Control integration, your management center gets registered to the Cisco cloud tenancy. This allows you to send firewall events to the Cisco cloud and use the various cloud services, such as Cisco XDR, to view and analyze the events.

Before you begin

- Security Cloud Control uses Security Cloud Sign On as its identity provider and Duo for multifactor authentication. Ensure that you have your Security Cloud Sign On credentials and can sign in to the Cisco regional cloud where your account was created. For the regional cloud URLs, refer to Regional Clouds, on page 2.
- You need a Security Cloud Control organization to integrate the Firewall Management Center with Security Cloud Control. If you do not already have a Security Cloud Controlorganization, create one. For more information, refer to Provision Security Cloud Control Firewall Management.
- Link your Security Cloud Control tenant, the one you want to use for onboarding the Firewall Management Center, to your Security Services Exchange account. For more information, refer to Link Your Security Cloud Control and SecureX or Cisco XDR Tenant Accounts.
- Ensure that you are modifying the configuration from the global domain.

- Ensure that **Cisco SecureX threat response or Cisco XDR** and **Eventing** services are enabled in Security Services Exchange. Verify this setting under **Cloud Services**.
- Your Firewall Management Center must be between version 7.0.2 and 7.0.x, or version 7.2 and later to perform this procedure.

Procedure

Step 1 Depending on the version of your Firewall Management Center:

- Click **Integration** > **SecureX** if your Firewall Management Center is between versions 7.0.2 and 7.0.x, or between versions 7.2.0 and 7.4.x.
- Click **Integration** > **Cisco Security Cloud** if your Firewall Management Center version is between 7.6.0 and 7.7.x.
- Click **Integration** > **Security Cloud Control** if your Firewall Management Center version is 10.0.0 and later.

Step 2 (Optional) Choose a Cisco regional cloud from the **Current Region** drop-down list.

Note

- The regional cloud you choose here is also used for the Cisco Success Network and Cisco Support Diagnostics capabilities. This setting also governs the cloud region for the Secure Network Analytics cloud using Security Analytics and Logging (SaaS).
- If you have already registered the Firewall Management Center with Smart License, the region selected by default will correspond to your Smart Licensing region. In such scenario, you don't have to change the region.

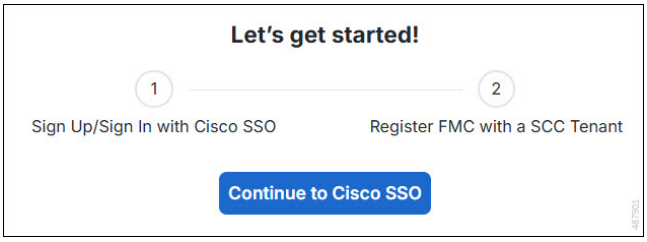
Step 3 Depending on the version of your Firewall Management Center:

- Click **Enable SecureX** for Firewall Management Center versions between 7.0.2 and 7.0.x, or between versions 7.2.0 and 7.4.x.
- Click **Enable Cisco Security Cloud** for Firewall Management Center version between 7.6.0 and 7.7.x.
- Click **Enable Security Cloud Control** for Firewall Management Center version 10.0.0 and later.

A separate browser tab opens to log you in to your Security Cloud Control account. Make sure this page is not blocked by a pop-up blocker.

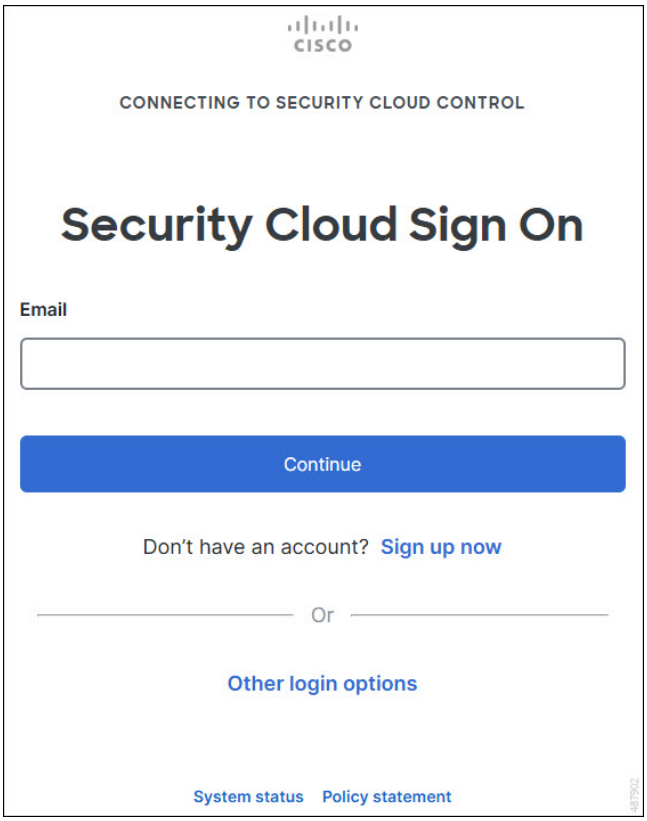
Step 4 Click **Continue to Cisco SSO**.

Figure 1: Security Cloud Control Welcome Page



Step 5 Log in to your Security Cloud Control organization.

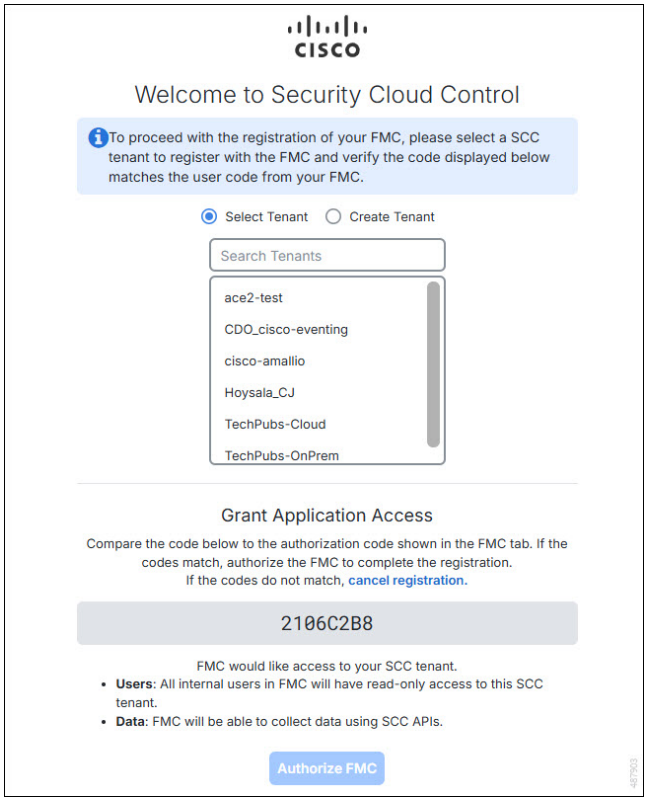
Figure 2: Cisco Security Cloud Sign On



If you do not have a Security Cloud Sign On account to log in to Security Cloud Control and you want to create one, click **Sign up now** in the **Security Cloud Sign On** page. For more information, refer to Provision Security Cloud Control Firewall Management.

Step 6 Choose a Security Cloud Control tenant that you want to use for this integration. The Firewall Management Center and the managed devices get onboarded to the Security Cloud Control tenant that you choose here.

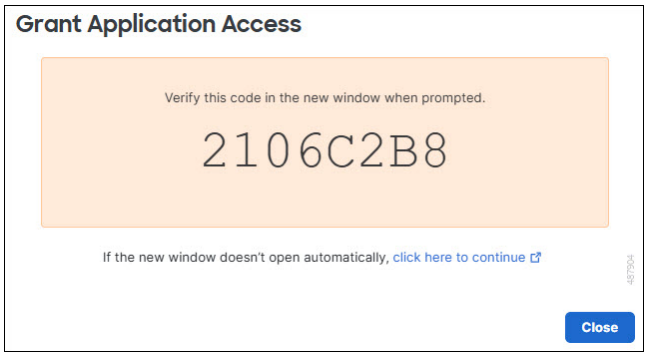
Figure 3: Choose the Security Cloud Control Tenant



If you do not already have a Security Cloud Control organization or if you want to use a new organization for this integration, create a new organization. For more information, refer to Provision Security Cloud Control Firewall Management.

Step 7 Verify that the code displayed in the Security Cloud Control login page matches the code provided by the Firewall Management Center.

Figure 4: Verification Code in the Firewall Management Center



Step 8 Click **Authorize FMC**.

Step 9 In the Firewall Management Center UI, click **Save** to save the configuration.

You can view the task progress under **Notifications** > **Tasks**.

The registration task can take up to 90 second to complete. If you must use Firewall Management Center while the registration task is in progress, open the Firewall Management Center in a new window.

Enable Sending Events to the Cloud

Configure your Firewall Management Center to have the managed devices send events directly to Security Cloud Control. 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

- In the Firewall Management Center:
  - Go to the **System > Configuration** page and give your Firewall Management Center a unique name to clearly identify it in the **Devices** list in the cloud.
  - Add your Firewall Threat Defense devices to the Firewall Management Center, assign licenses to them, and ensure that the system is working correctly. Ensure that you have created necessary policies and the generated events are displayed as expected in the Firewall Management Center UI under the **Analysis** menu.
  - Register the Firewall Management Center with the Smart License or enable Security Cloud Control integration.
- Determine the Cisco regional cloud you want to use for sending firewall events. For more information, see Guidelines and Limitations for Choosing a Regional Cloud, on page 2.
- If you are using Security Cloud Control integration to register your devices with cloud services, you must link your Security Cloud Control account with the Security Services Exchange tenant. For more information, see Link Your Security Cloud Control and Security Services Exchange Accounts, on page 13.



Important If you were already sending events to Security Cloud Control using a SecureX subscription, you can continue to send events to Cisco XDR. However, if you now register your Firewall Management Center to the cloud tenancy using your Security Cloud Control account, your Security Cloud Control account must have a Security Analytics and Logging license to forward events to Cisco XDR.

- If you are using Smart License to register your devices with cloud services, you must link your Smart Licensing account with the Security Services Exchange tenant. For more information, see Link Smart Licensing Accounts with Security Services Exchange, on page 14.
- Ensure that you can sign-in to the regional cloud using your Security Cloud Sign On credentials.
- Link your smart account or the Security Cloud Control tenant to your Security Services Exchange account.
- Disable sending events to the cloud using syslog to avoid duplication.

Procedure

Step 1 Depending on the version of your Firewall Management Center:

- Click **Integration** > **SecureX** if your Firewall Management Center is between versions 7.0.2 and 7.0.x, or between versions 7.2.0 and 7.4.x.
- Click **Integration** > **Cisco Security Cloud** if your Firewall Management Center version is between 7.6.0 and 7.7.x.
- Click **Integration** > **Security Cloud Control** if your Firewall Management Center version is 10.0.0 and later.

Step 2 (Optional) Choose a regional cloud from the **Current Region** drop-down list.

Step 3 Check the **Send events to the cloud** check box.

Step 4 Choose 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
Security Analytics and Logging (SaaS)	All	High priority connection events include: • Security-related connection events. • Connection events related to file and malware events. • Connection events related to intrusion events.
Cisco XDR	Depending on your version: • Security-related connection events. • Intrusion events. • File and malware events.	Even if you send all connection events, Cisco XDR support only security-related connection events. **Note** Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses required for Cisco Secure Firewall products. For more information, see Cisco XDR Licenses.

Note

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

Step 5 Click **Save**.

Analyze and Respond to Threats Using Cisco XDR Automation

Enable this setting to allow the automated workflows created by Cisco XDR users to interact with your Firewall Management Center resources.

Cisco XDR automation provides a no-to-low code approach for building automated workflows and they can be set to run in response to different schedules and events. Cisco XDR automation helps you to automate data collection and incident generation. You can rectify threats using automation and guided response recommendations across all relevant control points.

For more information about the Cisco XDR automation capabilities, see the Cisco XDR documentation.

Procedure

Step 1 Depending on the version of your Firewall Management Center:

- Click **Integration** > **Cisco Security Cloud** if your Firewall Management Center version is between 7.6.0 and 7.7.x.
- Click **Integration** > **Security Cloud Control** if your Firewall Management Center version is 10.0.0 and later.

Step 2 Check the **Enable Cisco XDR Automation** check box.

Step 3 Choose the Firewall Management Center user role that you want to assign to the Cisco XDR automation workflows.

The **Access Admin** role is set as the default, allowing access to access control policy and associated functionality in the **Policies** menu.

Step 4 Click **Save**.

Access Security Services Exchange

Before you begin

In your browser, disable pop-up blocking.

Procedure

Step 1 In a browser window, go to the Security Services Exchange admin portal using the URL: https://admin.sse.itd.cisco.com.

Step 2 Sign in using the credentials for your Cisco security cloud sign on, Secure Endpoint , Secure Malware Analytics, or Cisco Security account.

Note that your account credentials are specific to the regional cloud.

Verify that Events Reach Security Services Exchange Using Direct Connection

Before you begin

Verify that the events you expect appear in device as expected.

Procedure

Step 1 Login to your Security Services Exchange account. For more information, see Access Security Services Exchange, on page 22.

Step 2 In Security Services Exchange, click **Events**.

Step 3 Look for events from your device.

If you do not see expected events, see Troubleshoot a Direct Integration, on page 23.

Troubleshoot a Direct Integration

Problems accessing the cloud

- If you activate your cloud account immediately before attempting to configure this integration and you encounter problems implementing this integration, wait for an hour or two and then log in to your cloud account.
- Make sure you are accessing the correct URL for the regional cloud associated with your account.

Device managed by the Firewall Management Center is not listed correctly on the Security Services Exchange Devices page

(Releases earlier than 6.4.0.4) Manually give the device a unique name: Click the **Edit** icon for each row in the Devices list. Suggestion: Copy the IP address from the Description.

This change is valid only for this Devices list; it does not appear anywhere in your deployment.

(Releases from 6.4.0.4 to 6.6) Device name is sent from the Firewall Management Center to Security Services Exchange only at initial registration to Security Services Exchange and is not updated on Security Services Exchange if the device name changes in the Firewall Management Center.

Expected events are missing from the Events list

- Make sure you are looking at the correct regional cloud and account.
- Make sure that your devices can reach the cloud and that you have allowed traffic through your firewall to all required addresses.

- Click the **Refresh** button on the **Events** page to refresh the list and verify that the expected events appear.
- Check your configurations for automatic deletion (filtering out events) in the **Eventing** settings on the **Cloud Services** page in Security Services Exchange.
- For more troubleshooting tips, see the online help in Security Services Exchange.

Some events are missing

- If you send all connection events to the cloud, Cisco XDR uses only security connection events.
- If you are using custom Security Intelligence objects in the Firewall Management Center including global block or allow lists and Threat Intelligence Director, you must configure Security Services Exchange to auto-promote events that are processed using those objects. For more information, see the Security Services Exchange online help.

Failed to save the Security Cloud Control configuration

If the Firewall Management Center page fails to save the Security Cloud Control configuration,

- Verify that the Firewall Management Center has connectivity to the cloud.
- Ensure that you modify Security Cloud Control configuration from the global domain.

Security Cloud Control integration failed due to timeout

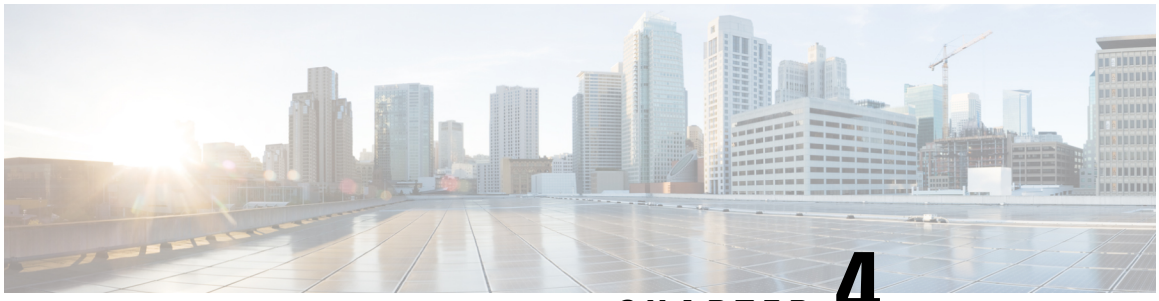
After starting the configuration, Firewall Management Center page waits 15 minutes to receive the authorization before it times out. Ensure that you complete the authorization within 15 minutes. Click **EnableSecurity Cloud Control** to start a new authorization request after a timeout.

Failed to register Firewall devices to Security Services Exchange using the Security Cloud Control Account

When Firewall Management Center fails to register managed devices to Security Services Exchange using the Security Cloud Control account, a message appears under **Notification** > **Tasks**. The Firewall Management Center restores the original configuration. When device registration fails, verify the following:

- Your Security Cloud Control account has administrator privileges.
- Firewall Management Center has connectivity to Security Services Exchange.

Disable and enable the Security Cloud Control configuration to register firewall devices to Security Services Exchange again.



CHAPTER 4

Send Events to the Cloud Using Syslog

- About Integration via Syslog, on page 25
- Requirements for Integration Using Syslog, on page 25
- How to Send Events to the Security Cloud Control Using Syslog and Integrate with Cisco XDR, on page 26
- Troubleshoot a Syslog Integration, on page 28

About Integration via Syslog

From Firewall Threat Defense release 6.3 onwards, you can use syslog to send supported events to the Cisco cloud from devices. You can set up an on-premises Cisco Security Services Proxy (CSSP) server and configure your devices to send syslog messages to this proxy.

Every 10 minutes, the proxy forwards collected events to Security Services Exchange from where the events can be promoted to various Security Cloud Control services, including Cisco XDR, to enrich your event analysis and investigations.

Requirements for Integration Using Syslog

Requirement Type	Requirement
Firewall Threat Defense device version	6.3 or later.
Account on the regional cloud that you will use	See Account Required for Cisco XDR Integration, on page 5.

Requirement Type	Requirement
Licensing	• Your Secure Firewall deployment must be licensed to generate the events that you want to send to the Cisco cloud. For details, see the Licensing Information. • This integration is not supported under an evaluation license. • Your environment cannot be deployed in an air-gapped environment. • Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses for Cisco Secure Firewall products. For more information, see Cisco XDR Licenses.
General	Your Firewall Threat Defense device is generating events as expected.

How to Send Events to the Security Cloud Control Using Syslog and Integrate with Cisco XDR

Note If your devices are already sending events to the Security Cloud Control, you do not need to configure sending them again.

Step	Do This	More Information
Step 1	Decide the following: • Types of events you want to send to the cloud. • The method of sending events. • The regional cloud to use for sending the events.	See About Secure Firewall Threat Defense and Cisco XDR Integration, on page 1.
Step 2	Meet the requirements for syslog integration.	See Requirements for Integration Using Syslog, on page 25.
Step 3	Access Security Services Exchange, the cloud portal that you will use for managing devices and filtering events for Cisco XDR integration.	See Access Security Services Exchange, on page 22.
Step 4	Install and configure a Cisco Security Services Proxy server.	Download the free installer and instructions from Security Services Exchange: In Security Services Exchange, from the **Tools** icon near the top-right of the browser window, select **Downloads**.

Step	Do This	More Information
Step 5	In Security Services Exchange, enable features.	Click **Cloud Services** and enable the following options: • **Cisco SecureX threat response or Cisco XDR** • **Eventing**
Step 6	Configure your devices to send syslog messages for supported events to the proxy server.	• For devices managed by the Firewall Device Manager, see the *Configuring Syslog for Intrusion Events* section in *Cisco Secure Firewall Device Manager Configuration Guide*. • For devices managed by the Firewall Management Center, see the *Event Analysis Using External Tools* section in *Cisco Secure Firewall Management Center Administration Guide*.
Step 7	In your product, ensure that the messages identify the device that generated each event.	• In the Firewall Device Manager: Specify a hostname in **Device** > **Hostname**. • In the Firewall Management Center: Under the Platform Settings **Syslog Settings** tab, **Enable Syslog Device ID**, and specify an identifier.
Step 8	In Security Services Exchange, configure the system to automatically promote significant events.	**Important** If you do not automate event promotion, you must manually review, and promote events to view them in Cisco XDR. See information in the online help in Security Services Exchange about promoting events. To access Security Services Exchange, see Access Security Services Exchange, on page 22.
Step 9	(Optional) In Security Services Exchange, configure automatic deletion of certain non significant events.	For more information on filtering events, see Security Services Exchange online help. To access Security Services Exchange, see Access Security Services Exchange, on page 22.
Step 10	Verify that your events appear as expected in Security Services Exchange and troubleshoot if necessary.	See: • Verify that Events Reach Security Services ExchangeUsing Syslog, on page 28. • Troubleshoot a Syslog Integration, on page 28.

Access Security Services Exchange

Before you begin

In your browser, disable pop-up blocking.

Procedure

Step 1 In a browser window, go to the Security Services Exchange admin portal using the URL: https://admin.sse.itd.cisco.com.

Step 2 Sign in using the credentials for your Cisco security cloud sign on, Secure Endpoint , Secure Malware Analytics, or Cisco Security account.

Note that your account credentials are specific to the regional cloud.

Verify that Events Reach Security Services ExchangeUsing Syslog

Before you begin

Verify that the events appear in the device as you expected.

Procedure

Step 1 Wait for about 15 minutes after your device has detected a supported event to allow messages to be forwarded from the proxy to Security Services Exchange.

Step 2 Login to your Security Services Exchange account. For more information, see Access Security Services Exchange, on page 22.

Step 3 In Security Services Exchange, click **Events**.

Step 4 Look for events from your device.

If you do not see the expected events, see Troubleshoot a Syslog Integration, on page 28.

Troubleshoot a Syslog Integration

Events are not reaching Cisco Security Services Proxy

Make sure your devices can reach Cisco Security Services Proxy on the network.

Problems accessing the cloud

- If you activate your cloud account immediately before attempting to configure this integration and you encounter problems implementing this integration, try waiting an hour or two and then log in to your cloud account.
- Make sure you are accessing the correct URL for the regional cloud associated with your account.

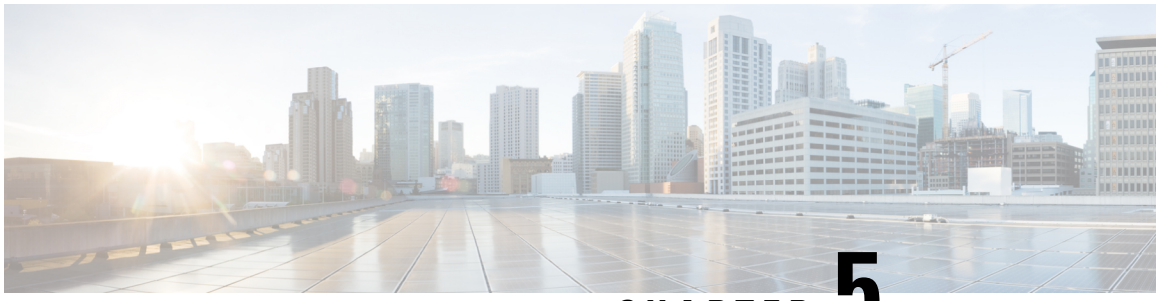
Expected events are missing from the events list

Check the following:

- Verify that the expected events appear on the device.
- In Security Services Exchange, check your configurations for automatic deletion (filtering out events) in the **Eventing** settings on the **Cloud Services** page.
- Make sure you are viewing the regional cloud to which you are sending your events.

Questions about Syslog Fields

For syslog fields and descriptions, see the Threat Defense Syslog Messages.



CHAPTER 5

Additional References

- More Information About Using Cisco XDR, on page 31
- About Using Security Services Exchange, on page 31

More Information About Using Cisco XDR

For more information about using Cisco XDR and for troubleshooting, see Cisco XDR Help Center. For information about the Cisco XDR product, see Cisco XDR product page.

For Cisco XDR FAQ, see Frequently Asked Questions.

About Using Security Services Exchange

For information about using Security Services Exchange or Cisco Security Services Proxy, see

Security Services Exchange's Online Help.