Introduction to Integrating Secure Firewall Management Center and SecureX

About Secure Firewall Management Center and SecureX

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.

If you do not have a SecureX account and want to use this feature, create a SecureX account using your CDO tenant. For more information, follow the instructions here.

Integrating SecureX with management center provides you a complete overview of all the data from the management center.

Follow the instructions in this document to use your SecureX portal to view and work with firewall event data from devices managed by management center versions 7.0.2, 7.2 or later. If your management center version is 7.1 or lower (except 7.0.2), follow the instruction is Cisco Secure Firewall Threat Defense and SecureX Integration Guide to integrate management center with SecureX.

SecureX Regional Clouds

Region	Link to Cloud	Supported Integration Methods and Managed Device Version	Supported Management Center Version
North America	https://securex.us.security.cisco.com	• Direct integration: Version 6.4 and later • Integration using syslog: Version 6.3 and later	Version 7.0.2, version 7.2 and later
Europe	https://securex.eu.security.cisco.com	• Direct integration: Version 6.5 and later • Integration using syslog: Version 6.3 and later	Version 7.0.2, version 7.2 and later
Asia (APJC)	https://securex.apjc.security.cisco.com	• Direct integration: Version 6.5 and later • Integration using syslog: Version 6.3 and later	Version 7.0.2, version 7.2 and later

Guidelines and Limitations for Choosing a Regional Cloud

Before choosing a regional cloud, consider these important points:

- Selecting regional cloud depends on your version and integration method (syslog or direct).

  See SecureX Regional Clouds for specifics.

- When possible, use the regional cloud nearest to your deployment.
- You cannot merge or aggregate data in different regional clouds.
- If you need to aggregate data from multiple regions, devices in all 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 region you select in your product is also used for the Cisco Support Diagnostics and Cisco Support Network features, if applicable and enabled. For more information about these features, see the online help for your product.

Supported Event Types

The Secure Firewall Management Center and SecureX integration supports the following event types:

Table 1: Version Support for Sending Events to the Cisco Cloud

Event Type	Threat Defense Device Version (Direct Integration)	Syslog
Intrusion (IPS) events	6.4 and later	6.3 and later
Security connection 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

Devices make events available to SecureX through the Security Services Exchange portal, either using syslog or directly.

Sending Events Directly	Sending Events Using Syslog Through a Proxy Server
Supports only threat defense (NGFW) 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.
Supports all event types listed in.	Supports only intrusion events.
Supports SecureX tiles that show system status information such as whether your appliances and devices are running the optimal software versions.	System status features are not supported with syslog-based integrations.
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 (CSSP) server. More information about this proxy server is available from the online help in Security Services Exchange. To access Security Services Exchange, see Access Security Service Exchange.

Best Practices

Follow guidelines and setup instructions in the following topics precisely, including Requirements topics and Before You Begin sections in referenced procedure topics:

- For all integrations:

  See Guidelines and Limitations for Choosing a Regional Cloud, on page 2.

- For direct integration:

  See How to Send Events Directly to the Cisco Cloud.

- For integration using syslog:

  See How to Send Events to the Cisco Cloud Using Syslog.