Important Information About Integrating Secure Firewall Threat Defense and SecureX

About Threat Defense and SecureX

View data from all of your Cisco security products through SecureX, a unified portal that is included with your Cisco security product purchase.

SecureX is a simplified platform experience, connecting Cisco's integrated security portfolio with your existing infrastructure to unify visibility, enable automation, and strengthen security across your network, endpoints, cloud, and applications.

For more information about SecureX, see 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.

To view and work with your data in the SecureX portal, follow the instructions in this document. If you manage your threat defense devices using management center version 7.0.2, 7.2, or higher, follow the instructions in Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide.

SecureX Regional Clouds

Region	Link to Cloud	Supported Integration Methods
North America	https://securex.us.security.cisco.com	• Direct integration: Release 6.4 and later • Integration via syslog: Release 6.3 and later
Europe	https://securex.eu.security.cisco.com	• Direct integration: Release 6.5 and later • Integration via syslog: Release 6.3 and later
Asia (APJC)	https://securex.apjc.security.cisco.com	• Direct integration: Release 6.5 and later • Integration via syslog: Release 6.3 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, on page 2 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 threat defense and SecureX integration supports the following event types:

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

Feature	Devices Managed by Secure Firewall Management Center Version (Direct integrations)	Devices Managed by Secure Firewall Device Manager Version (Direct integrations)	Syslog
Intrusion (IPS) events	6.3 and later (via syslog) 6.4 and later (via direct connection)	6.3 and later (via syslog) 6.4 and later (via direct connection)	Supported
Security Intelligence connection events	6.5 and later	6.5 and later	Not supported
File and malware events	6.5 and later	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 Supported Event Types, on page 2.	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.

Sending Events Directly	Sending Events Using Syslog Through a Proxy Server
No need to set up and maintain an on-premises proxy server.	Requires an on-premises virtual Cisco Security Services Proxy (CSSP) server. More information about this proxy server is available from the online help in Security Services Exchange (SSE). To access SSE, see Access Security Services 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 and Integrate with SecureX.

- For integration using syslog:

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