



CISCO Secure Firewall Threat Defense User Guide

[Home](#) » [Cisco](#) » CISCO Secure Firewall Threat Defense User Guide 

Contents

- 1 CISCO Secure Firewall Threat Defense
- 2 Specifications
- 3 About Cisco SecureX Threat Response and This Integration
- 4 Cisco SecureX Threat Response Regional Clouds
- 5 Guidelines and Limitations for Choosing a Regional Cloud
- 6 Supported Event Types
- 7 Comparison of Methods for Sending Events to the Cloud
- 8 Best Practices
- 9 Documents / Resources
 - 9.1 References
- 10 Related Posts



CISCO Secure Firewall Threat Defense



Specifications

- Supported Integration Methods: Sending Events Directly, Sending Events Using Syslog Through a Proxy Server
- Supported Event Types: Threat defense (NGFW) devices, Intrusion events, Security Intelligence connection events

Supported Regions

- North America: <https://visibility.amp.cisco.com>
- Europe: <https://visibility.eu.amp.cisco.com>
- Asia (APJC): <https://visibility.apjc.amp.cisco.com>
- Management Center Version: 6.3 and later (via syslog)
- Device Manager Version: 6.3 and later (via syslog)

Important Information About Integrating Secure Firewall Threat Defense and Cisco SecureX Threat Response

- About Cisco SecureX Threat Response and This Integration, on page 1
- Cisco SecureX Threat Response Regional Clouds, on page 2
- Supported Event Types, on page 2
- Comparison of Methods for Sending Events to the Cloud, on page 3
- Best Practices, on page 4

About Cisco SecureX Threat Response and This Integration

- Cisco SecureX threat response (formerly Cisco Threat Response or CTR) is the platform in the Cisco cloud that helps you detect, investigate, analyze, and respond to threats using data aggregated from multiple products and sources.
- This integration sends supported events from devices to Cisco SecureX threat response for analysis alongside data from your other products and other sources.
- For more information about Cisco SecureX threat response, see Cisco SecureX Threat Response product page. For videos about the use and benefits of the application on YouTube, see <http://cs.co/CTRvideos>.
- If you do not already have a Cisco SecureX threat response account, you can create one using Cisco Defense Orchestrator (CDO). To create a Cisco SecureX threat response account from CDO, follow the instructions here.
- For more information about this integration, see the at http://cs.co/ctr_firepower_faq and the online help in Cisco SecureX threat response, including the release notes.

Cisco SecureX Threat Response Regional Clouds

Region	Link to Cloud	Supported Integration Methods
North America	https://visibility.amp.cisco.com	<ul style="list-style-type: none"> • Direct integration: Release 6.4 and later • Integration via syslog: Release 6.3 and later
Europe	https://visibility.eu.amp.cisco.com	<ul style="list-style-type: none"> • Direct integration: Release 6.5 and later • Integration via syslog: Release 6.3 and later
Asia (APJC)	https://visibility.apjc.amp.cisco.com	<ul style="list-style-type: none"> • 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 Cisco SecureX Threat Response 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 Cisco SecureX threat response 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 Cisco SecureX threat response 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
<p>No need to set up and maintain an on-premises proxy server.</p>	<ul style="list-style-type: none"> • 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.
- **For integration using syslog**
See How to Send Events to the Cisco Cloud Using Syslog.

Documents / Resources

	<p>CISCO Secure Firewall Threat Defense [pdf] User Guide Secure Firewall Threat Defense, Firewall Threat Defense, Threat Defense, Defense</p>
---	---

References

- [User Manual](#)