Introduction to Integrating Secure Firewall Threat Defense and Cisco XDR

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 Threat Defense Device Version
North America	• api-sse.cisco.com • mx*.sse.itd.cisco.com • eventing-ingest.sse.itd.cisco.com • defenseorchestrator.com • edge.us.cdo.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 • defenseorchestrator.eu • edge.eu.cdo.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.cdo.cisco.com • edge.apj.cdo.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.cdo.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.cdo.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 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 threat defense and Cisco XDR integration supports the following event types:

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

Event Type	Supported Threat Defense Device Version for Direct Integration	Supported 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 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 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.
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.