Cisco Security Analytics and Logging and Cisco XDR Integration

First Published: 2021-07-02

Objective and Assumptions

The objective of this document is to explain the benefit of merging your Security Cloud Control tenant and your Cisco Extended Detection and Response (XDR) tenant so that you can analyze all your firewall events in Cisco XDR. The document assumes that you have an existing Security Cloud Control tenant.

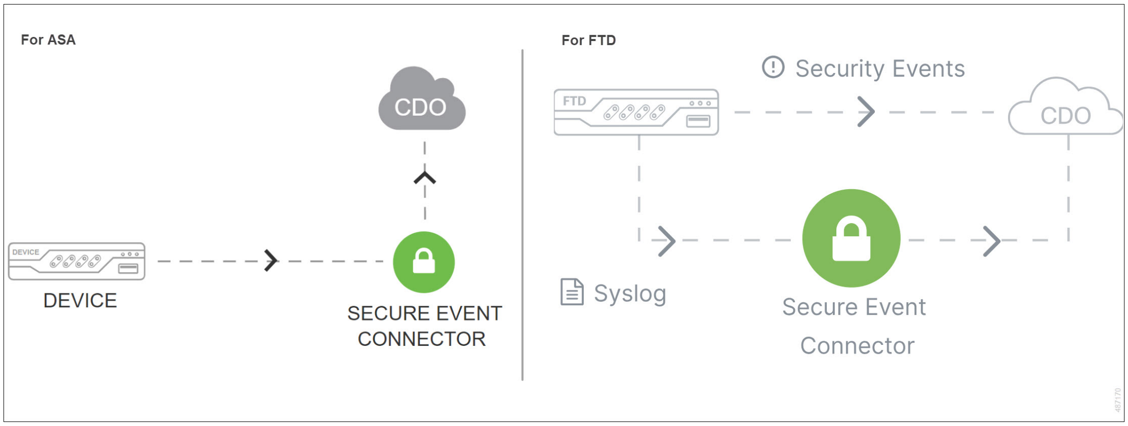
If you already have a Cisco XDR tenant, a Security Cloud Control Tenant, you have configured Secure Logging Analytics, and you just want the instructions to merge the tenants, see Link Your Security Cloud Control and Cisco XDR Tenant Accounts.

Cisco Security Analytics and Logging and Cisco XDR Overviews

Cisco Security Analytics and Logging allows you to capture connection, intrusion, file, malware, and Security-relared connection events from all your threat defense devices, and all syslog and Netflow Secure Event Logging (NSEL) events from your Adaptive Security Appliances (ASA) and view them in Security Cloud Control. The events are stored in the Cisco Security Cloud and viewable from the **Event Logging** page in Security Cloud Control, where you can filter and review them to gain a clear understanding of what security rules are triggering in your network.

With additional licensing, after you capture events reported by your firewalls, you can cross-launch from Security Cloud Control to a Secure Cloud Analytics portal which can make observations about the events you stored. These observations characterize network traffic as typical or atypical of the device type that generated it.

Figure 1: How Sending Events to the Cloud Works



ASA devices managed by Adaptive Security Device Manager (ASDM), Cisco Security Manager (CSM), or Security Cloud Control can all send events to the Cisco Security Cloud by way of a Secure Event Connector (SEC). The SEC is installed on a virtual machine and you configure the ASA to send events to the SEC as it if were a syslog server. The SEC forwards the events securely to the Cisco Security Cloud.

The threat defense devices managed by firewall device manager, management center, or Security Cloud Control can also send events to the Cisco Security Cloud. They can be sent through the SEC or they can be sent directly to the Cisco Security Cloud.

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 Security Cloud Control tenant 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.

.

Cisco Tenancy and Registered Devices

Your ASA and FDM-managed devices are registered with either the Virtual Account cloud tenant or the Security Cloud Control cloud tenant depending on how they are licensed and how they communicate with the Cisco Security Cloud infrastructure.

The tenants are isolated from each other and do not share event data.

Virtual Account Tenant

The threat defense devices that are "smart-licensed," and are not onboarded to Security Cloud Control account are registered to the Cisco Virtual Account tenant. The Virtual Account tenant has no automatic connection to the Cisco XDR tenant or the Security Cloud Control tenant, therefore, events are not automatically forwarded to Cisco XDR.

Cisco Defense Orchestrator Tenant

Devices that have been onboarded to Security Cloud Control are registered to the Security Cloud Control tenant. Those devices can send events directly to the Cisco Security Cloud or through the SEC to the Cisco Security Cloud. Secure Cloud Analytics is part of the Security Cloud Control tenant. The Security Cloud Control tenant has no automatic connection to the Cisco XDR tenant or the Virtual Account Tenant, therefore, events are not automatically forwarded to Cisco XDR.

Cisco XDR Tenant

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.

You cannot log in to Cisco XDR using your Cisco Security Account or Cisco Secure Malware Analytics credentials.

The Cisco XDR tenant does not automatically receive events from the Security Cloud Control tenant or Virtual account tenant unless those tenants are merged with it.

Security Services Exchange

These tenants are all separate but all reside in the Security Services Exchange (SSE). The SSE is a secure intermediary cloud service that handles cloud-to-cloud and premises-to-cloud identification, authentication, and data storage for use in Cisco cloud security products.

Merge Security Cloud Control and Cisco XDR Tenants to Display Events in Cisco XDR

To maximize the benefit of Cisco XDR and Security Analytics and Logging, merge your Cisco XDR tenant and Security Cloud Control tenant. After the merge, Cisco XDR can analyze these high-priority events from your FDM-managed devices: intrusion, file, malware, Security-related connection events and associated connection events.

Secure Logging Analytics continues to store and process all FTD and ASA events that are sent to the Cisco Security Cloud.

Procedure

Step 1 Request a Cisco XDR Tenant. For instructions on setting up your Cisco XDR tenant, see Cisco XDR Help Center.

Step 2 Configure Security Analytics and Logging on your Security Cloud Control Tenant.

Use these different instructions to configure Security Analytics and Logging for different devices:

Device type and Device Manager	Documentation
ASA managed by Security Cloud Control and sending events to the Cisco Security Cloud using an SEC.	Cisco Security Analytics and Logging (SaaS) for ASA Devices
ASA managed by ASDM and CLI and sending events to the Cisco Security Cloud using an SEC.	Integrating Cisco ASA and Cisco Security Analytics and Logging (SaaS) using CLI and ASDM
ASA managed by Cisco Security Manager and sending events to the Cisco Security Cloud using an SEC.	Integrating Cisco ASA and Cisco Security Analytics and Logging (SaaS) using CSM
FTD managed by Security Cloud Control and sending events to the Cisco Security Cloud using an SEC.	Cisco Security Analytics and Logging (SaaS) for FTD Devices
FTD 7.0+ device, managed by FDM and sends events directly to the Cisco Security Cloud.	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0 > System Settings
FTD 7.0+ device managed by FMC.	Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide

Step 3 Merge your Security Cloud Control Tenant with your Cisco XDR Tenant.

If you want events generated by your secure firewalls and other supported Cisco products to be available in Cisco XDR, merge your tenants. See Link Your Security Cloud Control and Cisco XDR Tenant Accounts for instructions.