Cisco Secure Logging Analytics and Cisco SecureX Integration

First Published: 2021-07-02

Objective and Assumptions

The objective of this document is to explain the benefit of merging your Cisco Defense Orchestrator tenant and your SecureX tenant so that you can analyze all your firewall events in SecureX. The document assumes that you have an existing Cisco Defense Orchestrator tenant.

If you already have a SecureX tenant, a CDO Tenant, you have configured Secure Logging Analytics, and you just want the instructions to merge the tenants, see (FTD Managed by FDM Only) Merge Your CDO and Security Accounts for instructions.

Cisco Secure Logging Analytics and Cisco SecureX Overviews

Cisco Secure Logging Analytics allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all your Firepower Threat Defense (FTD) devices, and all syslog and Netflow Secure Event Logging (NSEL) events from your Adaptive Security Appliances (ASA) and view them in Cisco Defense Orchestrator (CDO). The events are stored in the Cisco cloud and viewable from the event logging page in CDO, 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 CDO 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.

ASAs managed by Adaptive Security Device Manager (ASDM), Cisco Security Manager (CSM), or CDO can all send events to the Cisco 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 cloud.

Firepower Threat Defense (FTD) devices managed by Firepower Device Manager (FDM), Firepower Management Center (FMC) or CDO can also send events to the Cisco cloud. They can be sent through the SEC or they can be sent directly to the Cisco cloud.

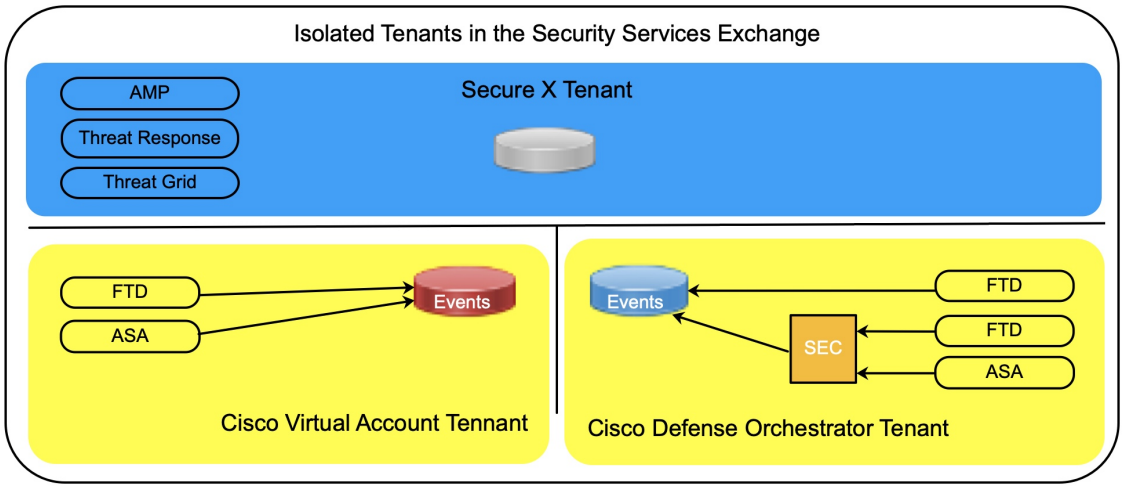
SecureX is a security platform that aggregates all your security intelligence from Cisco and third-party applications. With that intelligence, it analyzes the observations, event information, and threat intelligence gathered from integrated applications. You will be able to defend against instances of malware or other attacks by tuning security policies or identifying compromised computers.

Cisco Tenancy and Registered Devices

Your ASA and FTD devices are registered with either the Virtual Account cloud tenant or the Cisco Defense Orchestrator cloud tenant depending on how they are licensed and how they communicate with the Cisco cloud infrastructure.

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

Figure 1: Isolated Tenants in the Security Services Exchange



Virtual Account Tenant

Devices such as Firepower Threat Defense devices, that are "smart-licensed," and are not onboarded to Cisco Defense Orchestrator account are registered to the Cisco Virtual Account tenant. The Virtual Account tenant has no automatic connection to the SecureX tenant or the CDO tenant, therefore, events are not automatically forwarded to SecureX.

Cisco Defense Orchestrator Tenant

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

SecureX Tenant

If you have licenses for Cisco security products such as AMP, Cisco Threat Response, or Cisco Threat Grid, these products are part of the SecureX tenant. SecureX is an aggregator of security intelligence and analyzer of threat data. As long as you have one Cisco security product, SecureX is free to you.

The SecureX tenant does not automatically receive events from the CDO tenant or Virtual account tenant unless those tenants are merged with it.

Security Services Exchange

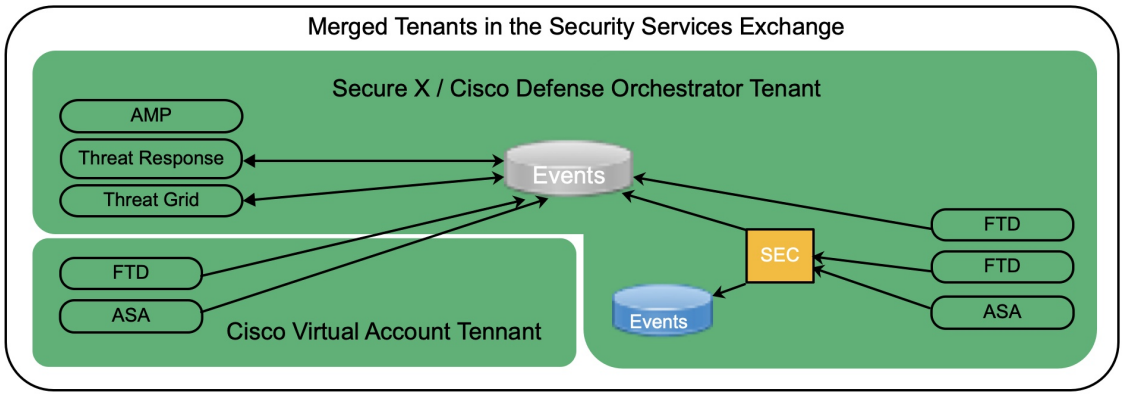
These tenants are all separate but all reside in the Security Services Exchange (SSE). The SSE is a secure intermediary cloud service that handles cloud-to-cloud and premises-to-cloud identification, authentication, and data storage for use in Cisco cloud security products.

Merge CDO and SecureX Tenants to Display Events in SecureX

To maximize the benefit of SecureX and Security Analytics and Logging, merge your SecureX tenant and CDO tenant. After the merge, SecureX can analyze these high-priority events from your FTD devices: intrusion, file, malware, Security Intelligence and associated connection events.

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

Figure 2: Merged Tenants in the Security Services Exchange



Procedure

Step 1 Request a SecureX Tenant. See See the Cisco SecureX Sign-On Quick Start Guide for instructions on setting up your SecureX account.

Step 2 Configure Security Analytics and Logging on your CDO Tenant.

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

Device type and Device Manager	Documentation
ASA managed by CDO and sending events to the Cisco 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 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 cloud using an SEC	Integrating Cisco ASA and Cisco Security Analytics and Logging (SaaS) using CSM
FTD managed by CDO and sending events to the Cisco 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 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 CDO Tenant with your SecureX Tenant.

If you want events generated by your secure firewalls and other supported Cisco products to be available in SecureX, merge your tenants. See (FTD Managed by FDM Only) Merge Your CDO and Security Accounts for instructions on how to merge these tenants.