



Cisco Security Analytics and Logging

- [About Security Analytics and Logging \(SaaS\) in Cisco Defense Orchestrator, on page 2](#)
- [Event Types in CDO, on page 2](#)
- [Secure Logging Analytics for FDM-Managed Devices, on page 8](#)
- [Implementing Secure Logging Analytics \(SaaS\) for FDM-Managed Devices, on page 14](#)
- [Send FDM Events to Cisco Defense Orchestrator Events Logging, on page 17](#)
- [Send FDM-Managed Events Directly to the Cisco Cloud, on page 17](#)
- [Implementing SAL \(SaaS\) for Cloud-Delivered Firewall Management Center-Managed Devices, on page 18](#)
- [Requirements, Guideline, and Limitations for the SAL \(SaaS\) Integration, on page 18](#)
- [Send Cloud-delivered Firewall Management Center-Managed Events to SAL \(SaaS\) Using Syslog, on page 19](#)
- [Send Cloud-delivered Firewall Management Center-Managed Event Logs to SAL \(SaaS\) Using a Direct Connection, on page 21](#)
- [Enable or Disable Threat Defense Devices to Send Event logs to SAL \(SaaS\) Using a Direct Connection, on page 22](#)
- [Secure Event Connectors, on page 23](#)
- [Installing Secure Event Connectors, on page 24](#)
- [Deprovisioning Cisco Security Analytics and Logging \(SaaS\), on page 44](#)
- [Remove the Secure Event Connector, on page 44](#)
- [Provision a Cisco Secure Cloud Analytics Portal, on page 45](#)
- [Review Sensor Health and CDO Integration Status in Secure Cloud Analytics, on page 46](#)
- [Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting, on page 47](#)
- [Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 48](#)
- [Cisco Secure Cloud Analytics and Dynamic Entity Modeling, on page 49](#)
- [Working with Alerts Based on Firewall Events, on page 50](#)
- [Modifying Alert Priorities, on page 56](#)
- [Viewing Live Events, on page 56](#)
- [Show and Hide Columns on the Event Logging Page, on page 59](#)
- [Customizable Event Filters, on page 62](#)
- [Event Attributes in Security Analytics and Logging, on page 63](#)
- [Searching for and Filtering Events in the Event Logging Page, on page 92](#)
- [Download a Background Search, on page 101](#)
- [Data Storage Plans, on page 101](#)

- [Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics \(SaaS\), on page 103](#)

About Security Analytics and Logging (SaaS) in Cisco Defense Orchestrator

Cisco Security Analytics and Logging (SAL) allows you to capture connection, intrusion, file, malware, security intelligence, syslog, and Netflow Secure Event Logging (NSEL) events from all of your ASA and Secure Firewall Threat Defense devices and view them in one place 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 these events, you can cross-launch from CDO to a Secure Cloud Analytics portal provisioned for you. Secure Cloud Analytics is a software as a service (SaaS) solution that tracks the state of your network by performing a behavioral analysis on events and network flow data. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Terminology Note: In this documentation, when Cisco Security Analytics and Logging is used with the Secure Cloud Analytics portal (a software as a service product) you will see this integration referred to as Cisco Security Analytics and Logging (SaaS) or SAL (SaaS).

Event Types in CDO

When filtering ASA and Secure Firewall Threat Defense events logged by Secure Logging Analytics (SaaS), you can choose from a list of ASA and FTD event types that CDO supports. From the CDO menu, navigate **Analytics > Event Logging** and click the filter icon to choose events. These event types represent groups of syslog IDs. The table that follows shows which syslog IDs are included in which event type. If you want to learn more about a specific syslog ID, you can search for it in the [Cisco ASA Series Syslog Messages](#) or the [Cisco Secure Firewall Threat Defense Syslog Messages](#) guides.

Some syslog events have the additional attribute "EventName." You can filter the events table to find events using the EventName attribute by filtering by attribute:value pairs. See [EventName Attributes for Syslog Events](#).

Some syslog events will have the additional attributes "EventGroup" and "EventGroupDefinition". You will be able to filter the events table to find events using these additional attributes by filtering by attribute:value pairs. See [EventGroup and EventGroupDefinition Attributes for Some Syslog Messages](#).

The NetFlow events are different from syslog events. The **NetFlow** filter searches for all NetFlow event IDs that resulted in an NSEL record. Those NetFlow event IDs are defined in the [Cisco ASA NetFlow Implementation Guide](#).

The following table describes the event types that CDO supports and lists the syslog or NetFlow event numbers that correspond to the event types:

Filter Name	Description	Corresponding Syslog Event or Netflow Event
AAA	These are events that the system generates when failed or invalid attempts happen to authenticate, authorize, or use up resources in the network, when AAA is configured.	109001-109035 113001-113027
BotNet	These events get logged when a user attempts to access a malicious network, which might contain a malware-infected host, possibly a BotNet, or when the system detects traffic to or from a domain or an IP address in the dynamic filter block list.	338001-338310
Failover	These events get logged when the system detects errors in stateful and stateless failover configurations or errors in the secondary firewall unit when a failover occurs.	101001-101005, 102001, 103001-103007, 104001-104004, 105001-105048 210001-210022 311001-311004 709001-709007
Firewall Denied	These events get generated when the firewall system denies traffic of a network packet for various reasons, ranging from a packet drop because of the security policy to a drop because the system received a packet with the same source IP and destination IP, which could potentially mean an attack on the network. Firewall Denied events may be contained in a NetFlow and may be reported with NetFlow event IDs as well as syslog IDs.	106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Firewall Traffic	<p>These are events that get logged depending on the various connection attempts in the network, user identities, time stamps, terminated sessions, and so on.</p> <p>Firewall Traffic events may be contained in a NetFlow and may be reported with NetFlow event IDs as well as syslog IDs.</p>	<p>106001-106100, 108001-108007, 110002-110003</p> <p>201002-201013, 209003-209005, 215001</p> <p>302002-302304, 302022-302027, 303002-303005, 313001-313008, 317001-317006, 324000-324301, 337001-337009</p> <p>400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001</p> <p>500001-500005, 508001-508002</p> <p>607001-607003, 608001-608005, 609001-609002, 616001</p> <p>703001-703003, 726001</p>
IPsec VPN	These events are logged in an IPsec VPN-configured firewall when mismatches occur in IPsec security associations or when the system detects an error in the IPsec packets it receives.	402001-402148, 602102-602305, 702304-702307
NAT	These events are logged in a NAT-configured firewall when NAT entries are created or deleted and when all the addresses in a NAT pool are used up and exhausted.	201002-201013, 202001-202011, 305005-305012
SSL VPN	These events are logged in an SSL VPN-configured firewall when WebVPN sessions get created or terminated, user access errors, and user activities.	716001-716060, 722001-722053, 723001-723014, 724001-724004, 725001-725015
NetFlow	These events are logged around the IP network traffic as network packets enter and exit the interfaces, timestamps, user identities, and the amount of data transferred.	0, 1, 2, 3, 5

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Connection	<p>You can generate events for connections as users generate traffic that passes through the system. Enable connection logging on access rules to generate these events. You can also enable logging on Security Intelligence policies and SSL decryption rules to generate connection events.</p> <p>Connection events contain data about the detected sessions. The information available for any individual connection event depends on several factors, but in general includes:</p> <ul style="list-style-type: none">• Basic connection properties: timestamp, source and destination IP address, ingress and egress zones, the device that handled the connection, and so on.• Additional connection properties discovered or inferred by the system: applications, requested URLs, or users associated with the connection, and so on.• Metadata about why the connection was logged: which configuration handled the traffic, whether the connection was allowed or blocked, details about encrypted and decrypted connections, and so on.	430002, 430003

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Intrusion	The system examines the packets that traverse your network for malicious activity that could affect the availability, integrity, and confidentiality of a host and its data. When the system identifies a possible intrusion, it generates an intrusion event, which is a record of the date, time, type of exploit, and contextual information about the source of the attack and its target. Intrusion events are generated for any intrusion rule set to block or alert, regardless of the logging configuration of the invoking access control rule.	430001
File	<p>File events represent files that the system detected, and optionally blocked, in network traffic based on your file policies. You must enable file logging on the access rule that applies the file policy to generate these events.</p> <p>When the system generates a file event, the system also logs the end of the associated connection regardless of the logging configuration of the invoking access control rule.</p>	430004

Filter Name	Description	Corresponding Syslog Event or Netflow Event
Malware	<p>The system can detect malware in network traffic as part of your overall access control configuration. AMP for Firepower can generate a malware event, containing the disposition of the resulting event, and contextual data about how, where, and when the malware was detected. You must enable file logging on the access rule that applies the file policy to generate these events.</p> <p>The disposition of a file can change, for example, from clean to malware or from malware to clean. If AMP for Firepower queries the AMP cloud about a file, and the cloud determines the disposition has changed within a week of the query, the system generates retrospective malware events.</p>	430005
Security Intelligence	<p>Security Intelligence events are a type of connection event generated by the Security Intelligence policy for each connection that is blocked or monitored by the policy. All Security Intelligence events have a populated Security Intelligence Category field.</p> <p>For each of these events, there is a corresponding "regular" connection event. Because the Security Intelligence policy is evaluated before many other security policies, including access control, when a connection is blocked by Security Intelligence, the resulting event does not contain the information that the system would have gathered from subsequent evaluation, for example, user identity.</p>	430002, 430003

Secure Logging Analytics for FDM-Managed Devices

Cisco Security Analytics and Logging (SaaS) allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all of your FDM-managed devices and view them in one place in Cisco Defense Orchestrator.

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. The **Logging and Troubleshooting** package gives you these capabilities.

With the **Logging Analytics and Detection** package (formerly **Firewall Analytics and Logging** package), the system can apply Secure Cloud Analytics dynamic entity modeling to your FDM-managed device events, and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a **Total Network Analytics and Monitoring** package, the system applies dynamic entity modeling to both your FDM-managed device events and your network traffic, and generates observations and alerts. You can cross-launch from CDO to a Cisco Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.

How FDM Events are Displayed in the CDO Events Viewer

Connection, intrusion, file, malware, and Security Intelligence events are generated when an individual rule is configured to log events and network traffic matches the rule criteria. After the events are stored in the Cisco cloud, you can view them in CDO. There are two methods of configuring your FDM-managed device to send events to the Cisco cloud:

- You can install multiple Secure Event Connectors (SECs) and send events generated by a rule, on any device, to any of the SECs as if it were a syslog server. The SEC then forwards the event to the Cisco cloud.
- If your FDM-managed device was onboarded to CDO using a registration key, you can send events directly to the Cisco cloud using a control in the Secure Firewall device manager.

How an Event is Sent to the Cisco Cloud Using the Secure Event Connector

With the basic **Logging and Troubleshooting** license, this is how a Secure Firewall device manager event reaches the Cisco cloud:

1. You onboard your FDM-managed device to CDO using username and password or by using a registration key.
2. You configure individual rules, such as access control rules, Security Intelligence rules, and SSL decryption rules, to forward events to any one of your SECs as if it were a syslog server. In access control rules, you can also enable file and malware policies, and intrusion policies, and forward events generated by those policies to the SEC.
3. You configure File/Malware logging in **System Settings > Logging** for file events.
4. You configure Intrusion Logging in **System Settings > Logging** for intrusion events.
5. The SEC forwards the events to the Cisco cloud where the events are stored.
6. CDO displays events from the Cisco cloud in its Events Logging page based on the filters you set.

With the **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, the following also occur:

1. Cisco Secure Cloud Analytics applies analytics to the Secure Firewall device manager connection events stored in the Cisco cloud.
2. Generated observations and alerts are accessible from the Secure Cloud Analytics portal associated with your CDO portal.
3. From the CDO portal, you can cross-launch your Secure Cloud Analytics portal to review these observations and alerts.

How Events are Sent Directly from an Secure Firewall device manager to the Cisco Cloud

With the basic **Logging and Troubleshooting** license, this is how Secure Firewall device manager events reach the Cisco cloud:

1. You onboard your FDM-managed device to CDO using a registration token.
2. You configure individual rules, such as access control rules, Security Intelligence rules, and SSL decryption rules, to log events but you don't specify a syslog server for them to be sent to. In access control rules, you can also enable file and malware policies and intrusion policies, and forward events generated by those policies to the Cisco cloud.
3. File events and Intrusion events are sent to the Cisco cloud if file and malware policies and intrusion policies are configured in the access control rules to log connection events.
4. You activate Cloud Logging on the Secure Firewall device manager and the events logged in the various rules are sent to the Cisco cloud.
5. CDO pulls events from the Cisco cloud based on the filters you set and displays them in its Events viewer.

With the **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, the following also occur:

1. Cisco Secure Cloud Analytics applies analytics to the Secure Firewall device manager connection events stored in the Cisco cloud.
2. Generated observations and alerts are accessible from the Secure Cloud Analytics portal associated with your CDO portal.
3. From the CDO portal, you can cross-launch your Secure Cloud Analytics portal to review these observations and alerts.

Configuration Comparison

Here is a summary of the CDO configuration differences between sending events to the Cisco cloud through an SEC and sending events directly to the Cisco cloud.

FDM-Managed Device Configuration	When Sending Events through a Secure Event Connector (SEC)	When Sending Events Directly to Cisco Cloud
CDO onboarding method for FDM-Managed Device	Credentials (Username and password) Registration token	Registration token Serial Number

FDM-Managed Device Configuration	When Sending Events through a Secure Event Connector (SEC)	When Sending Events Directly to Cisco Cloud
Version Support	Version 6.4+	Registration Token - Version 6.5+ Serial Number - Version 6.7+
Cisco Security Analytics and Logging (SaaS) Licenses	Logging and Troubleshooting Logging Analytics and Detection (optional) Total Network Analytics and Monitoring (optional)	Logging and Troubleshooting Logging Analytics and Detection (optional) Total Network Analytics and Monitoring (optional)
Licenses	license -If you want to collect connection events from intrusion rules, file control rules, or security intelligence filtering. Malware-If you want to collect connection events from file control rules.	license -If you want to collect connection events from intrusion rules, file control rules, or security intelligence filtering. Malware-If you want to collect connection events from file control rules.
Secure Event Connector	Required	N/A
Data Compression*	Events are compressed*	Events are not compressed*
Data Plan	Required	Required



Note Data subscriptions and your Historical Monthly Usage are based on the amount uncompressed data you use.

Components in the Solution

Cisco Security Analytics and Logging (SaaS) uses these components to deliver events to CDO:

Secure Device Connector (SDC)-The SDC connects CDO to your FDM-managed devices. The login credentials for the FDM-managed devices are stored on the SDC. See [Secure Device Connector](#) for more information.

Secure Event Connector (SEC)-The SEC is an application that receives events from your FDM-managed devices and forwards them to the Cisco cloud. Once in the Cisco cloud, you can view the events on CDO's Event Logging page or analyze them with Cisco Secure Cloud Analytics. You may have one or more SECs associated with your tenant. Depending on your environment, you install the Secure Event Connector on a Secure Device Connector or a CDO Connector VM.

Secure Firewall device manager-The FDM-managed device is Cisco's next generation firewall. Beyond stateful inspection of network traffic and access control, the FDM-managed device provides capabilities such as protection from malware and application-layer attacks, integrated intrusion prevention, and cloud-delivered threat intelligence.

If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, Cisco Security Analytics and Logging (SaaS) uses Cisco Secure Cloud Analytics to further analyze events delivered to CDO.

Cisco Secure Cloud Analytics-Secure Cloud Analytics applies dynamic entity modeling to events, generating detections based on this information. This provides a deeper analysis of telemetry gathered from your network, allowing you to identify trends and examine anomalous behavior in your network traffic.

Licensing

To configure this solution you need the following accounts and licenses:

Cisco Defense Orchestrator. You must have a CDO tenant.

Secure Device Connector. There is no separate license for a SDC.

Secure Event Connector. There is no separate license for a SEC.

Secure Logging Analytics (SaaS). You need to buy the **Logging and Troubleshooting** license. The goal of this package is to provide network operations teams with real-time and historical events derived from their on-boarded FDM-managed devices for the purposes of troubleshooting and analyzing traffic in their network.

You can also buy a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license to apply Cisco Secure Cloud Analytics. The goal of these packages is to provide network operations teams additional insight into the events (and network traffic with the Total Network Analytics and Monitoring license) to better identify possible anomalous behavior and respond to it.

License Name	Provided Functionality	Available License Durations	Functionality Prerequisites
Logging and Troubleshooting	View events and event detail within CDO, both as a live feed and as a historical view	<ul style="list-style-type: none"> • 1 year • 3 years • 5 years 	<ul style="list-style-type: none"> • CDO • An on-premises deployment running version 6.4 or later • Deployment of one or more SECs to pass events to the cloud

License Name	Provided Functionality	Available License Durations	Functionality Prerequisites
Logging Analytics and Detection (formerly Firewall Analytics and Monitoring)	Logging and Troubleshooting functionality, plus: <ul style="list-style-type: none"> • Apply dynamic entity modeling and behavioral analytics to your FDM-managed device events • Open alerts in Secure Cloud Analytics based on event data, cross-launching from the CDO event viewer 	<ul style="list-style-type: none"> • 1 year • 3 years • 5 years 	<ul style="list-style-type: none"> • CDO • An on-premises deployment running version 6.4 or later. • Deployment of one or more SECs to pass events to the cloud. • A newly provisioned or existing Secure Cloud Analytics portal.
Total Network Analytics and Monitoring	Logging Analytics and Detection , plus: <ul style="list-style-type: none"> • Apply dynamic entity modeling and behavioral analytics to events, on-premises network traffic, and cloud-based network traffic. • Open alerts in Secure Cloud Analytics based on the combination of event data, on-premises network traffic flow data collected by Secure Cloud Analytics sensors, and cloud-based network traffic passed to Secure Cloud Analytics, cross-launching from the CDO event viewer. 	<ul style="list-style-type: none"> • 1 year • 3 years • 5 years 	<ul style="list-style-type: none"> • CDO • An on-premises deployment running version 6.4 or later • Deployment of one or more SECs to pass events to the cloud • Deployment of at least one Secure Cloud Analytics sensor version 4.1 or later to pass network traffic flow data to the cloud OR integrating Secure Cloud Analytics with a cloud-based deployment, to pass network traffic flow data to Secure Cloud Analytics. • A newly provisioned or existing Secure Cloud Analytics portal.

FDM-Managed Device. You need to have the following licenses to run the FDM-managed device and create rules that generate security events:

License	Duration	Granted Capabilities
Essentials(automatically included)	Perpetual	<p>All features not covered by the optional term licenses.</p> <p>You must also specify whether to Allow export-controlled functionality on the products registered with this token. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.</p>
	Term-based	<p>Intrusion detection and prevention-Intrusion policies analyze network traffic for intrusions and exploits and, optionally, drop offending packets.</p> <p>File control-File policies detect and, optionally, block users from uploading (sending) or downloading (receiving) files of specific types. AMP for Firepower, which requires a Malware license, allows you to inspect and block files that contain malware. You must have the Threat license to use any type of File policy.</p> <p>Security Intelligence filtering-Drop selected traffic before the traffic is subjected to analysis by access control rules. Dynamic feeds allow you to immediately drop connections based on the latest intelligence.</p>
Malware	Term-based	<p>File policies that check for malware, which use Cisco Advanced Malware Protection (AMP) with AMP for Firepower (network-based Advanced Malware Protection) and Cisco Threat Grid.</p> <p>File policies can detect and block malware in files transmitted over your network.</p>

Data Plans

You need to buy a data storage plan that reflects the number of events the Cisco cloud receives from your on-boarded FDM-managed devices on a daily basis. The best way to determine your ingest rate is to participate in a free trial of Secure Logging Analytics (SaaS) before you buy it. This will give you a good estimate of your event volume. In addition, you can use the [Logging Volume Estimator Tool](#).

**Caution**

It is possible to configure your FDM-managed device to send events to the Cisco cloud directly and by way of the SEC simultaneously. If you do this, the same event will be "ingested" twice and counted against your data plan twice, though it will only be stored in the Cisco cloud once. Be careful to send events to the Cisco cloud using one method or the other to avoid incurring unnecessary fees.

Data plans are available in 1 GB daily volumes increments, and in 1, 3 or 5 year terms. See the [Secure Logging Analytics \(SaaS\) Ordering Guide](#) for information about data plans.

**Note**

If you have a Security Analytics and Logging license and data plan, then obtain a different license at a later date, that alone does not require you to obtain a different data plan. If your network traffic throughput changes and you obtain a different data plan, that alone does not require you to obtain a different Security Analytics and Logging license.

30-day Free Trial

You can request a 30-day risk-free trial by logging in to CDO and navigating to **Analytics > Event Logging**. On completion of the 30-day trial, you can order the desired event data volume to continue the service from Cisco Commerce Workspace (CCW), by following the instructions in the [Secure Logging Analytics \(SaaS\) ordering guide](#).

What to do next?

Continue with [Implementing Secure Logging Analytics \(SaaS\) for FDM-Managed Devices](#), on page 14.

Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices

Before you Begin

- Review [Secure Logging Analytics for FDM-Managed Devices](#), on page 8 to learn about:
 - How events are sent to the Cisco cloud
 - Applications in the solution
 - Licenses you need
 - Data plan you need

- You have contacted your managed service provider or Cisco Defense Orchestrator Sales representative and you have a CDO tenant.
- Your tenant may or may not use an Secure Device Connector (SDC) for CDO to connect with your FDM-managed devices. Your tenant should have an SDC installed for those FDM-managed devices that you onboard with device credentials, [it is considered a best practice](#). If you onboard your FDM-managed devices with registration key or serial number you do not need an SDC.
- If you have installed an SDC for your tenant, ensure your SDC status is **Active** and has recorded a recent heartbeat.
- If you are installing an SDC, you use one of these methods for the installation:
 - Use [Deploy a secure device connector using CDO's vm image](#) to install an SDC using CDO's prepared VM image. This is the preferred and easiest way to deploy an SDC.
 - Use [Deploy a secure device connector using your own VM](#).
- You can [Installing an SEC Using a CDO Image](#) SEC for your tenant and you can send events from any Firewall device manager to any one SEC onboarded to your tenant.
- If you are sending events directly to the Cisco cloud from the firewall device manager, you have opened up outbound access on port 443 on the management interface.
- You have [established two-factor authentication](#) for users of your account.

New CDO Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud

1. [Onboard your FDM-Managed Devices](#). You can onboard the device with the admin username and password or with a registration token.
2. [Create a Syslog Server Object for Secure Logging Analytics \(SaaS\)](#).
3. [Configure the FDM-Managed Device Policy](#) to log connection events.
4. Configure your FDM-managed device to [Send FDM Events to Cisco Defense Orchestrator Events Logging](#).
5. Confirm events are visible in CDO. From the navigation bar, select **Analytics > Event Logging**. Click the Live tab to view live events.
6. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with [Analyzing Events in Cisco Secure Cloud Analytics](#).

New CDO Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events Directly to the Cisco Cloud

1. [Onboard your FDM-Managed Devices](#). You can only use a registration key.
2. [Configure the FDM-Managed Device Policy](#) to log connection events.
3. Configure your FDM-managed device to [Send FDM-Managed Events Directly to the Cisco Cloud](#).
4. Confirm events are visible in CDO. From the navigation bar, select **Analytics > Event Logging**. Click the Live tab to view live events.

5. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with [Analyzing Events in Cisco Secure Cloud Analytics](#).

Existing CDO Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud

1. [Onboard your FDM-Managed Devices](#). You can onboard the device with the admin username and password or with a registration token.
2. [Syslog Server Object for Secure Logging Analytics \(SaaS\)](#).
3. [Configure the FDM-Managed Device Policy](#) to log connection events.
4. [Send FDM Events to Cisco Defense Orchestrator Events Logging](#).
5. Confirm events are visible in CDO. From the navigation bar, select **Analytics > Event Logging**. Click the Live tab to view live events.
6. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with [Analyzing Events in Cisco Secure Cloud Analytics](#).

Existing CDO Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events Directly to the Cisco Cloud

1. [Onboard your FDM-Managed Devices](#). You can only use a registration key.
2. [Configure the FDM-Managed Device Policy](#) to log connection events.
3. Configure your FDM-managed device to [Send FDM-Managed Events Directly to the Cisco Cloud](#).
4. Confirm events are visible in CDO. From the navigation bar, select **Analytics > Event Logging**. Click the Live tab to view live events.
5. If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, continue with [Analyzing Events in Cisco Secure Cloud Analytics](#).

Analyzing Events in Cisco Secure Cloud Analytics

If you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, perform the following in addition to the previous steps:

1. [Provision a Cisco Secure Cloud Analytics Portal](#), on page 45.
2. Deploy one or more Secure Cloud Analytics sensors to your internal network if you purchased a **Total Network and Monitoring** license. See [Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting](#), on page 47.
3. Invite users to create Secure Cloud Analytics user accounts, tied to their Cisco Single Sign-On credentials. See [Viewing Cisco Secure Cloud Analytics Alerts from CDO](#), on page 48.
4. Cross-launch from CDO to Secure Cloud Analytics to monitor the Secure Cloud Analytics alerts generated from firewall device manager events. See [Viewing Cisco Secure Cloud Analytics Alerts from CDO](#), on page 48.

Reviewing Secure Cloud Analytics Alerts by Cross-launching from CDO

With a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, you can cross-launch from CDO to Secure Cloud Analytics to review the alerts generated by Secure Cloud Analytics, based on firewall device manager events.

Review these articles for more information:

- [Signing in to CDO](#)
- [Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 48](#)
- [Cisco Secure Cloud Analytics and Dynamic Entity Modeling, on page 49](#)
- [Working with Alerts Based on Firewall Events](#)

Secure Analytics and Logging (SaaS) Workflows

[Troubleshooting Using Security and Analytics Logging Events](#) describes using the events generated from Secure Logging Analytics (SaaS) to determine why a user can't access a network resource.

See also [Working with Alerts Based on Firewall Events](#).

Send FDM Events to Cisco Defense Orchestrator Events Logging

To view FDM-managed events from access control rules, security intelligence rules, and SSL decryption rules in the Event Logging viewer, you first need to send those events to the Cisco cloud.

- **Access Control Rules.** You can log [Event Types in CDO](#) at the beginning or end of a network connection. See [Configure the FDM Access Control Policy](#) and [Logging Settings in an FDM Access Control Rule](#) for more information about configuring logging for this rule type.
- **Security Intelligence Rules.** You can log [Event Types in CDO](#) generated by the Security Intelligence rules. If you enable logging, any matches to blocked list entries are logged. Matches to exception entries are not logged, although you get log messages if exempted connections match access control rules with logging enabled. See [Configure the Firepower Security Intelligence Policy](#) for more information about configuring logging.
- **SSL Decryption Rules.** You can log [Event Types in CDO](#) generated by SSL decryption rules.

If you are sending file and malware events or intrusion events to the Cisco cloud and you are using a Secure Event Connector, you need to [configure logging settings for the device](#).

Related Information:

- [Create a Syslog Server Object for Secure Logging Analytics \(SaaS\)](#)

Send FDM-Managed Events Directly to the Cisco Cloud

Starting with Firewall device manager Version 6.5, you can send connection events, intrusion, file, and malware events directly from your FDM-managed device to the Cisco cloud. Once in the Cisco cloud, you can monitor them with Cisco Defense Orchestrator (CDO) and analyze them with Cisco Secure Cloud Analytics. This

method does not require installing a Secure Event Connector (SEC) container on the Secure Device Connector (SDC) virtual machine.

Before you begin

Review these topics:

- [Secure Logging Analytics for FDM-Managed Devices, on page 8](#)
- [Implementing Secure Logging Analytics \(SaaS\) for FDM-Managed Devices](#)

Procedure

-
- Step 1** Log on to the Firewall device manager for the device from which you want to send events to the Cisco cloud.
- Step 2** Select **Device > System Settings > Cloud Services**.
- Step 3** In the Send Events to the Cisco Cloud pane, click **Enable**.
-

Implementing SAL (SaaS) for Cloud-Delivered Firewall Management Center-Managed Devices

To deploy this integration, you must set up event data storage in SAL (SaaS) using either syslog or a direct connection.

- [Send Cloud-delivered Firewall Management Center-Managed Events to SAL \(SaaS\) Using Syslog, on page 19](#)
- [Send Cloud-delivered Firewall Management Center-Managed Event Logs to SAL \(SaaS\) Using a Direct Connection, on page 21](#)

Requirements, Guideline, and Limitations for the SAL (SaaS) Integration

Type	Description
Cisco Secure Firewall Threat Defense	<ul style="list-style-type: none"> • CDO-managed standalone threat defense devices, Version, 7.2 and later. • To send events using syslog, you must have threat defense, Version 6.4 or later. • To send events directly, you must have threat defense Version, 7.2 or later. • Your firewall system must be deployed and successfully generating events.

Type	Description
Regional cloud	<ul style="list-style-type: none"> • Determine the regional cloud that you want to send events to. • Events cannot be viewed from or moved between different regional clouds. • If you use a direct connection to send events to the cloud for integration with Cisco SecureX or Cisco SecureX threat response, you must use the same cloud region for this integration. • If you send events directly, the regional cloud you specify in CDO must match the region of your CDO tenant.
Data plan	<ul style="list-style-type: none"> • You must buy a data plan that reflects the number of events the Cisco cloud receives from your threat defense devices daily. This is called your daily ingest rate. • Use the Logging Volume Estimator Tool to estimate your data storage requirements.
Accounts	When you purchase a license for this integration, you are provided with a CDO tenant account to support the integration.

Send Cloud-delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog

This procedure provides information about the configuration for sending syslog messages for security events (connection, security intelligence, intrusion, file, and malware events) from devices managed by CDO.

Before you begin

- Configure policies to generate security events, and verify that the events you expect to see are displayed in the applicable tables under the **Analysis** menu.
- Gather information relating to the syslog server IP address, port, and protocol (UDP or TCP).
- Ensure that your devices can reach the syslog server.

Procedure

-
- Step 1** Log in to CDO.
- Step 2** From the CDO menu, click **Tools & Services > Firewall Management Center** to open the **Services** page.
- Step 3** Click and select **Cloud-Delivered FMC** and then click **Configuration**.
- Step 4** Configure the syslog settings for your threat defense device:

- a) Click **Devices > Platform Settings** and edit the platform settings policy that is associated with your threat defense device.
- b) In the left-side navigation pane, click **Syslog** and configure the syslog settings as follows:

Click this UI Element...	To Do the Following:
Logging Setup	Enable logging, specify FTP server settings, and the Flash usage.
Logging Destination	Enable logging to specific destinations and to specify filtering by message severity level, event class, or by a custom event list.
E-mail Setup	Specify the email address that is used as the source address for syslog messages that are sent as emails.
Events Lists	Define a custom event list that includes an event class, a severity level, and an event ID.
Rate Limit	Specify the volume of messages being sent to all the configured destinations and define the message severity level to which you want to assign the rate limits.
Syslog Settings	Specify the logging facility, enable the inclusion of a time stamp, and enable other settings to set up a server as a syslog destination.
Syslog Servers	Specify the IP address, protocol that is used, format, and security zone for the syslog server that is designated as a logging destination.

- c) Click **Save**.

Step 5

Configure the general logging settings for the access control policy (including file and malware logging):

- a) Click **Policies > Access Control** and then edit the access control policy that is associated with your threat defense device.
- b) Click **More** and then choose **Logging**. Configure the general logging settings for the access control policy (including file and malware logging) as follows:

Click this UI Element...	To Do the Following:
Send using specific syslog alert	Select a syslog alert from the list of existing predefined alerts or add one by specifying the name, logging host, port, facility, and severity.
Use the syslog settings configured in the FTD Platform Settings policy deployed on the device	Unify the syslog configuration by configuring it in Platform Settings and reuse the settings in the access control policy. The selected severity is applied to all the connection and intrusion events. The default severity is ALERT .

Click this UI Element...	To Do the Following:
Send Syslog messages for IPS events	Send events as syslog messages. The default syslog settings are used unless you override them.
Send Syslog messages for File and Malware events	Send file and malware events as syslog messages. The default syslog settings are used unless you override them.

c) Click **Save**.

Step 6 Enable logging for security intelligence events for the access control policy:

- a) In the same access control policy, click the **Security Intelligence** tab.
- b) Click **Logging** and enable security intelligence logging using the following criteria:
 - By Domain Name—Click logging next to the **DNS Policy** drop-down list.
 - By IP address—Click logging next to **Networks**.
 - By URL—Click logging next to **URLs**.

c) Click **Save**.

Step 7 Enable syslog logging for each rule in the access control policy:

- a) In the same access control policy, click the **Rules** tab.
- b) Click a rule to edit.
- c) Click the **Logging** tab in the rule.
- d) Check the **Log at beginning of connection** and **Log at end of connection** check boxes.
- e) If you want to log file events, check the **Log Files** check box.
- f) Check the **Syslog Server** check box.
- g) Verify that the rule is **Using default syslog configuration in Access Control Logging**.
- h) Click **Save**.
- i) Repeat steps 7.a through 7.h for each rule in the policy.

What to do next

If you have made all the required changes, deploy your changes to the managed devices.

Send Cloud-delivered Firewall Management Center-Managed Event Logs to SAL (SaaS) Using a Direct Connection

Configure the cloud-delivered Firewall Management Center to send events directly to SAL (SaaS). Follow this procedure to enable the Cisco cloud event global setting in the cloud-delivered Firewall Management Center. When needed, you can exclude individual FTD devices from sending event logs to SAL (SaaS). For more information, see [Enable or Disable Threat Defense Devices to Send Event logs to SAL \(SaaS\) Using a Direct Connection](#).

Before you begin

- Onboard devices to the cloud-delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

-
- Step 1** Log in to CDO.
- Step 2** In the CDO menu, click **Tools & Services > Firewall Management Center**.
- Step 3** Click **Cloud-Delivered FMC**, and in the **System** pane that is located at the right-side, click **Cisco Cloud Events**.
- Step 4** In the **Configure Cisco Cloud Events** widget, do the following:
- a. Click the **Send Events to the Cisco Cloud** toggle button to enable the overall configuration.
 - b. Check the **Send Intrusion Events to the cloud** check box to send the intrusion events to the cloud.
 - c. Check the **Send File and Malware Events to the cloud** check box to send the file and malware events to the cloud.
 - d. Choose an option to send the connection events to the cloud:
 - Click the **None** radio button to not send connection events to the cloud.
 - Click the **Security Events** radio button to send only security intelligence events to the cloud.
 - Click the **All** radio button to send all the connection events to the cloud.
 - e. Click **Save**.
-

Enable or Disable Threat Defense Devices to Send Event logs to SAL (SaaS) Using a Direct Connection

Enable or disable the FTD devices managed by the cloud-delivered Firewall Management Center to send events directly to SAL (SaaS). This device-level control allows you to optionally exclude specific FTD devices from sending event logs to the Cisco cloud to reduce traffic or to maintain a combination of SAL and on-premises event log storage.

**Note**

- To enable or disable sending events to the Cisco cloud from the FTD devices, enable the Cisco cloud event global setting in the cloud-delivered Firewall Management Center. For more information on enabling the Cisco cloud event global setting, see [Send Cloud-delivered Firewall Management Center-Managed Event Logs to SAL \(SaaS\) Using a Direct Connection, on page 21](#).

Sending events to the Cisco cloud is enabled by default for all FTD devices when the Cisco cloud event global setting is enabled in the cloud-delivered Firewall Management Center.

- The option to enable or disable FTD devices to send event logs to the cloud is supported on FTD Version 7.4.1 or later.

Before you begin

- Onboard devices to the cloud-delivered Firewall Management Center, assign licenses to these devices, and configure these devices to send events directly to SAL (SaaS).
- Enable connection logging on a per-rule basis by editing a rule and choosing the **Log at Beginning of Connection** and **Log at End of Connection** options.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Log in to CDO. |
| Step 2 | In the CDO menu, click Inventory . |
| Step 3 | Click the Devices tab to locate the device. |
| Step 4 | Click the FTD tab. |
| Step 5 | Choose the FTD devices whose configurations you want to edit, from the inventory list. |
| Step 6 | In the Device Management pane, click Cloud Events . |
| Step 7 | Click the Send Events to the Cisco Cloud toggle button to enable or disable the configuration. |
| Step 8 | Click Save . |
-

Secure Event Connectors

The Secure Event Connector (SEC) is a component of the Security Analytics and Logging SaaS solution. It receives events from ASA, and FDM-managed devices and forwards them to the Cisco cloud. CDO displays the events on the Event Logging page so that administrators can analyze them there or by using Cisco Secure Cloud analytics.

The SEC is installed on a Secure Device Connector deployed in your network, on its own CDO Connector virtual machine deployed in your network, or on an AWS Virtual Private Cloud (VPC).

Secure Event Connector ID

You may need the ID of the SEC when working with Cisco Technical Assistance Center (TAC) or other CDO Support. That ID is found on the Secure Connectors page in CDO. To find the SEC ID:

1. From the CDO menu on the left, choose **Tools & Services > Secure Connectors**.
2. Click the SEC you wish to identify.
3. The SEC ID is the ID listed above the Tenant ID in the Details pane.

Related Information:

- [Secure Logging Analytics for FDM-Managed Devices](#)
- [Install a Secure Event Connector on an SDC Virtual Machine, on page 24](#)
- [Install an SEC Using Your VM Image](#)
- [Install an SEC Using Your VM Image](#)
- [Install a Secure Event Connector on an AWS VPC Using a Terraform Module, on page 42](#)
- [Remove the Secure Event Connector](#)
- [Deprovisioning Cisco Security Analytics and Logging \(SaaS\)](#)

Installing Secure Event Connectors

Secure Event Connectors (SECs) can be installed on a tenant with or without an SDC.

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own CDO Connector virtual machine that you maintain in your network.

See these topics that describe the various installation cases:

- [Install an SEC Using Your VM Image, on page 34](#)
- [Installing an SEC Using a CDO Image, on page 27](#)
- [Install a Secure Event Connector on an AWS VPC Using a Terraform Module, on page 42](#)

Install a Secure Event Connector on an SDC Virtual Machine

The Secure Event Connector (SEC) receives events from ASA and FDM-managed devices and forwards them to the Cisco cloud. CDO displays the events on the Event Logging page so that administrators can analyze them there or by using Cisco Secure Cloud Analytics.

You can install one SEC on the same virtual machine as a Secure Device Connector, if you have one; or you can install the SEC on it's own CDO Connector virtual machine that you maintain in your network.

This article describes installing an SEC on the same virtual machine as an SDC. If you want to install more SECs see [Installing an SEC Using a CDO Image, on page 27](#) or [Install an SEC Using Your VM Image, on page 34](#).

Before you begin

- Purchase the Cisco Security and Analytics Logging, **Logging and Troubleshooting** license. Or, If you want to try Cisco Security and Analytics Logging out first, log in to CDO, and on the main navigation bar, choose **Analytics > Event Logging** and click **Request Trial**. You may also purchase the **Logging**

Analytics and Detection and **Total Network Analytics and Monitoring** licenses to apply Secure Cloud Analytics to the events.

- Make sure your SDC has been installed. If you need to install an SDC, follow one of these procedures:
 - [Deploy a secure device connector using CDO's VM image](#)
 - [Deploy a secure device connector using your own VM](#)



Note If you installed the on-premises SDC on your own VM, there is [Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created](#) required to allow events to reach it.

- Make sure the SDC is communicating with CDO:
 1. From the CDO menu, choose **Tools & Services > Secure Connectors**.
 2. Make sure that the SDC's last heartbeat was less than 10 minutes prior to the installation of the SEC and that the SDC's status is active.
 - System Requirements - Assign additional CPUs and memory to the virtual machine running the SDC:
 - CPU: Assign an **additional** 4 CPUs to accommodate the SEC to make a total of 6 CPU.
 - Memory: Assign an **additional** 8 GB of memory for the SEC to make a total of 10 GB of memory.
- After you have updated the CPU and memory on the VM to accommodate the SEC, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.

Procedure

- Step 1** Log in to CDO.
- Step 2** From the CDO menu, choose **Tools & Services > Secure Connectors**.
- Step 3** Click the blue plus button and click **Secure Event Connector**.

Step 4 Skip Step 1 of the wizard and go to Step 2. In step 2 of the wizard, click the link to **Copy SEC Bootstrap**

Deploy an On-Premises Secure Event Connector



```
dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT2lKaGNHa3RZMnhwW1c1ME1uMC5tTzh0bTZMZ1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZQYzVsRjRITTLteVVEVzh2Qk5FWW44c3V0Z3NTQUo0TH15N0xzVGsydEx4N05nbS00STB6SmZ6
aWdQTkRiV1RsRW1tcjI5SkFVZ2NBWEhySkdzcktmRESzUnJUM0hZU3JkZ21Hd1dGb3FwWUdZNkJHRU
VacmI0YVFLSjFTdnJ5RjVVFZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXRlQTfsYmE3VkxNOUp4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWEcCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxyY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY2lZy28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
Oi8vc3RhZ2luZy5kZXZyubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpbY
IKT05MWV9FVkvOVE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

Step 2

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM

```
U1NFX0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYy00Y2JkLWEzNWQtOGYzZDJKMiq1ZmU3IqpTU0VfRE
U0Vft1RQPSI5Y2IzNTI4ZWZlMzg0TQ2NjViMDFkZmEyYjUyMGUxNSIKVEVOQU5UX05BTUU9IkNET1
9jaXNjby1hbWFSbGlvIg==
```

[Copy SEC Bootstrap Data](#)

Step 3

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Data.

Cancel

OK

Step 5 Open a terminal window and log into the SDC as the "cdo" user.

Step 6 Once logged in, switch to the "sdc" user. When prompted for a password, enter the password for the "cdo" user. Here is an example of those commands:

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

Step 7 At the prompt, run the **sec.sh setup** script:

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

Step 8 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

Please copy the bootstrap data from Setup Secure Event Connector page of CDO:

```
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
```

```
RtyFUiyIOHKNkjbKhvhgyRStwterTyufGUIhoJpojP9UOoiUY8VHHGFXREWRtygfhVjkhOuiehIuyftyXtfcghvjbkB=
```

After the SEC is onboarded, the sec.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "sec-health-check."

```
=====
Running SEC health check for tenant [REDACTED]
=====
SEC cloud URL [REDACTED] is: Reachable
=====
SEC Connector status: Active
=====
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
=====
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate
=====
```

If you receive a message that the registration failed or that the SEC onboarding failed, go to [Troubleshooting Secure Event connector Onboarding Failures](#).

Step 9 Determine if the VM on which the SDC and SEC are running needs additional configuration:

- If you installed your SDC on your own virtual machine, continue with [Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created, on page 39](#).
- If you installed your SDC using a CDO image, continue to "What to do Next."

What to do next

Return to [Implementing Secure Logging Analytics \(SaaS\) for FDM-Managed Devices, on page 14](#).

Related Information:

- [Troubleshoot a Secure Device Connector](#)
- [Troubleshooting Secure Event Connector](#)
- [Troubleshooting SEC Onboarding Failures](#)
- [Troubleshooting Secure Event Connector Registration Failure](#)

Installing an SEC Using a CDO Image

The Secure Event Connector (SEC) forwards events from ASA and FTD to the Cisco cloud so that you can view them in the Event Logging page and investigate them with Secure Cloud Analytics, depending on your licensing.

You can install more than one Secure Event Connector (SEC) on your tenant and direct events from your ASAs and FDM-managed devices to any of the SECs you install. Having multiple SECs allows you to have SECs installed in different locations and distribute the work of sending events to the Cisco cloud.

Installing an SEC is a two part process:

1. [Install a CDO Connector, to Support a Secure Event Connector, Using a CDO VM Image, on page 28](#)
You need one CDO Connector for every SEC you install. The CDO Connector is different than a Secure Device Connector (SDC).
2. [Install the Secure Event Connector on your CDO Connector Virtual Machine, on page 40.](#)



Note If you want to create a CDO Connector by creating your own VM, see [Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created](#).

What to do next:

Continue with [Install a CDO Connector, to Support a Secure Event Connector, Using a CDO VM Image, on page 28](#)

Install a CDO Connector, to Support a Secure Event Connector, Using a CDO VM Image

Before you begin

- Purchase the Cisco Security and Analytics Logging, **Logging and Troubleshooting** license, you may also purchase the **Logging Analytics and Detection** and **Total Network Analytics and Monitoring** licenses to apply Secure Cloud Analytics to the events.
If you would rather, you can request a trial version of Security Analytics and Logging by logging in to CDO, and on the main navigation bar, choose **Analytics > Event Logging** and click **Request Trial**.
- CDO requires strict certificate checking and does not support Web/Content Proxy inspection between the CDO Connector and the Internet. If using a proxy server, disable inspection for traffic between the CDO Connector and CDO.
- **The CDO Connector installed in this process must have full outbound access to the Internet on TCP port 443.**
- **Review [Connect to Cisco Defense Orchestrator using Secure Device Connector](#) to ensure proper network access for the CDO Connector.**
- CDO supports installing its CDO Connector VM OVF image using the vSphere web client or the ESXi web client.
- CDO does not support installing the CDO Connector VM OVF image using the VM vSphere desktop client.
- ESXi 5.1 hypervisor.
- System requirements for a VM intended to host only a CDO Connector and an SEC:
 - VMware ESXi host needs 4 vCPU.
 - VMware ESXi host needs a minimum of 8 GB of memory.
 - VMware ESXi requires 64GB disk space to support the virtual machine depending on your provisioning choice.
- Gather this information before you begin the installation:

- Static IP address you want to use for your CDO Connector VM.
- Passwords for the **root** and **cdo** users that you create during the installation process.
- The IP address of the DNS server your organization uses.
- The gateway IP address of the network the SDC address is on.
- The FQDN or IP address of your time server.
- The CDO Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.

Procedure

- Step 1** Log on to the CDO tenant you are creating the CDO Connector for.
- Step 2** From the CDO menu, choose **Tools & Services > Secure Connectors**.
- Step 3** Click the blue plus button and click **Secure Event Connector**.



- Step 4** In Step 1, click **Download the CDO Connector VM image**. This is a special image that you install the SEC on. Always download the CDO Connector VM to ensure that you are using the latest image.



- Step 5** Extract all the files from the .zip file. They will look similar to these:
- CDO-SDC-VM-ddd50fa.ovf
 - CDO-SDC-VM-ddd50fa.mf
 - CDO-SDC-VM-ddd50fa-disk1.vmdk
- Step 6** Log on to your VMware server as an administrator using the vSphere Web Client.
- Note** Do not use the VM vSphere desktop client.
- Step 7** Deploy the on-premises CDO Connector virtual machine from the OVF template by following the prompts. (You will need the .ovf, .mf, and .vdk files to deploy the template.)
- Step 8** When the setup is complete, power on the VM.
- Step 9** Open the console for your new CDO Connector VM.

- Step 10** Login as the **cdo** user. The default password is `adm123`.
- Step 11** At the prompt type `sudo sdc-onboard setup`
- ```
[cdo@localhost ~]$ sudo sdc-onboard setup
```
- Step 12** When prompted, enter the default password for the **cdo** user: `adm123`.
- Step 13** Follow the prompts to create a new password for the **root** user.
- Step 14** Follow the prompts to create a new password for the **cdo** user.
- Step 15** Follow the prompts to enter your Cisco Defense Orchestrator domain information.
- Step 16** Enter the static IP address you want to use for the CDO Connector VM.
- Step 17** Enter the gateway IP address for the network on which the CDO Connector VM is installed.
- Step 18** Enter the NTP server address or FQDN for the CDO Connector.
- Step 19** When prompted, enter the information for the Docker bridge or leave it blank if it is not applicable and press <Enter>.
- Step 20** Confirm your entries.
- Step 21** When prompted "Would you like to setup the SDC now?" enter **n**.
- Step 22** Create an SSH connection to the CDO Connector by logging in as the **cdo** user.
- Step 23** At the prompt type `sudo sdc-onboard bootstrap`
- ```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```
- Step 24** When prompted, enter the **cdo** user's password.
- Step 25** When prompted, return to CDO and copy the CDO bootstrap data, then paste it into your SSH session. To copy the CDO bootstrap data:
- Log into CDO.
 - From the CDO menu, choose **Tools & Services > Secure Connectors**.
 - Select the Secure Event Connector which you started to onboard. The status should show, "Onboarding."
 - In the Actions pane, click **Deploy an On-Premises Secure Event Connector**.

- e. Copy the CDO Bootstrap Data in step 1 of the dialog

Deploy an On-Premises Secure Event Connector


 SEC will be deployed on a new VM

Step 1

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```
Q0RPX1RPS0V0PSJ1eUp0YkdjaU9pS1NVekkxTm1Jc0luUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSWlPaU
13SW13aWMyTnZjR1VpT2xzazWRISjFjM1FpTENKeVpXRmtJaXdpZDNKcGRHVWlMQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUmhaVFV0T1dNd05DMH10VGRpTlR0aE1qZzFPR1VpWFN3aVlXMX1Jam9pYzJGdGJDSX
Njbkp2YkdWek1qcGJJbEpQVEVWZ1UxVlFSVkpUUVVSTlNVNG1YU3dpYVh0ek1qb2lhWFJrSW13aVky
eDFjM1JsY2tsa01qb2lNU01zSW1sa01qb2labVF3T0dReVpHVXRNM1ZpT1MwMFpEYzRMV0kwWldNdF
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWFtVmpkRlI1Y0dVaU9pSjFjM1Z5SW13aWFuUnBJam9pTURB
VacmI0YVFLSjFTdnJ5RjVFZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzVl9qQW1PNXM3Tm02Sn1rMXRlQTFSYmE3VksxN0Up4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NFN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWDpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY2l2Y28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUE9VUkw9Imh0dHBz
0i8vc3RhZ2luZy5kZXludG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2l2Y28tYW1hbGxpby
IKT05MWV9FVkv0VE10Rz0idHJ1ZSIK
```

 Copy CDO Bootstrap Data

Cancel

OK

box.

Step 26 When prompted, **Would you like to update these settings?** enter **n**.

Step 27 Return to the Deploy an On-Premises Secure Event Connector dialog in CDO and click **OK**. On the Secure Connectors page, you see your Secure Event Connector is in the yellow Onboarding state.

What to do next

Continue to [Install the Secure Event Connector on the CDO Connector VM](#), on page 31.

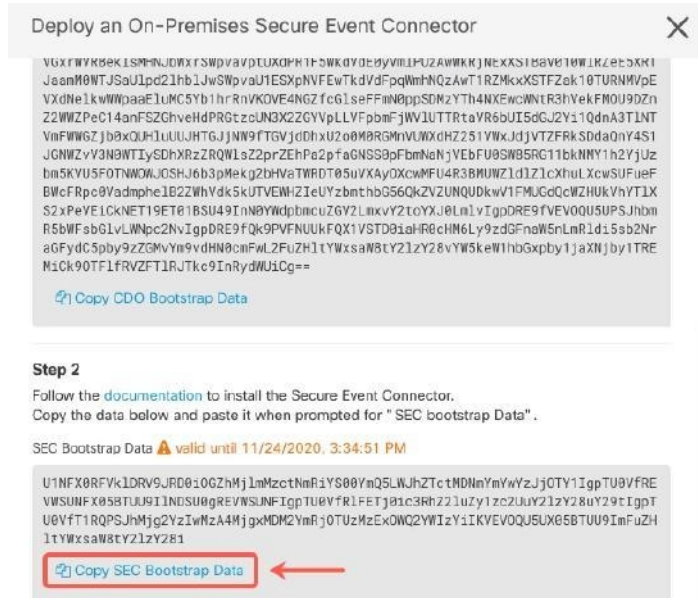
Install the Secure Event Connector on the CDO Connector VM

Before you begin

You should have installed CDO Connector VM as described in [Install a CDO Connector, to Support a Secure Event Connector, Using a CDO VM Image](#), on page 28.

Procedure

- Step 1** Log in to CDO.
- Step 2** From the CDO menu, choose **Tools & Services > Secure Connectors**.
- Step 3** Select the CDO Connector that you onboarded above. In the Secure Connectors table, it will be called a Secure Event Connector and it should still be in the "Onboarding" status.
- Step 4** Click **Deploy an On-Premises Secure Event Connector** in the Actions pane on the right.
- Step 5** In **step 2** of the wizard, click the link to **Copy SEC bootstrap data**.



- Step 6** Create an SSH connection to the CDO Connector and log in as the **cdo** user.
- Step 7** Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "cdo" user. Here is an example of those commands:

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

- Step 8** At the prompt, run the sec.sh setup script:

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

- Step 9** At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

Please copy the bootstrap data from Setup Secure Event Connector page of CDO:

KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE

RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkB=

After the SEC is onboarded, the sec.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "sec-health-check."


```

=====
Running SEC health check for tenant [redacted]
=====
SEC cloud URL [redacted] is: Reachable
=====
SEC Connector status: Active
=====
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
=====
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====

```

If you receive a message that the registration failed or that the SEC onboarding failed, go to [Troubleshooting SEC Onboarding Failures](#).

If you receive the success message return to CDO and click **Done on the Deploy an ON-Premise Secure Event Connector** dialog box.

Step 10 Continue to "What to do next."

What to do next

Return to [Implementing Secure Logging Analytics \(SaaS\) for FDM-Managed Devices](#), on page 14.

Related Information:


- [Troubleshoot a Secure Device Connector](#)
- [Secure Event Connector Troubleshooting](#)
- [Troubleshooting SEC Onboarding Failures](#)

Deploy Secure Event Connector on Ubuntu Virtual Machine

Before you begin

You should have installed Secure Device Connector on your Ubuntu VM as described in [Deploy Secure Device Connector and Secure Event Connector on Ubuntu Virtual Machine](#).

Procedure

-
- Step 1** Log on to CDO.
- Step 2** Choose **Tools & Services > Secure Connectors**.
- Step 3** On the **Services** page, select the **Secure Connectors** tab, click the , and select **Secure Event Connector**.
- Step 4** Copy the SEC bootstrap data in step 2 on the window to a notepad.
- Step 5** Execute the following commands:
- ```
[sdc@vm] :~$sudo su sdc
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```
- When prompted, enter the SEC bootstrap data that you have copied..

```

sdc@vm:~/toolkit$./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC

```

It may take a few minutes for the Secure Event Connector to become "Active" in CDO.

## Install an SEC Using Your VM Image

The Secure Event Connector (SEC) forwards events from ASA and FTD to the Cisco cloud so that you can view them in the Event Logging page and investigate them with Secure Cloud Analytics, depending on your licensing.

You can install more than one Secure Event Connector (SEC) on your tenant and direct events from your ASAs and FDM-managed devices to any of the SECs you install. Having multiple SECs allows you to have SECs installed in different regions and distribute the work of sending events to the Cisco cloud.

Installing multiple SECs using your own VM image is a three part process. You must perform each of these steps:

1. [Install a CDO Connector to Support an SEC Using Your VM Image, on page 34](#)
2. [Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created, on page 39](#)
3. [Install the Secure Event Connector on your CDO Connector Virtual Machine](#)



**Note** Using a CDO VM image for the CDO Connector is the easiest, most accurate, and preferred method of installing a CDO connector. If you want to use that method, see [Installing an SEC Using a CDO Image, on page 27](#).

### What to do next:

Continue to [Install a CDO Connector to Support an SEC Using Your VM Image, on page 34](#)

## Install a CDO Connector to Support an SEC Using Your VM Image

The CDO Connector VM is a virtual machine on which you install an SEC. The purpose of the CDO Connector is solely to support an SEC for Cisco Security Analytics and Logging (SaaS) customers.

This is the first of three steps you need to complete in order install and configure your Secure Event Connector (SEC). After this procedure, you need to complete the following procedures:

- [Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created, on page 39](#)
- [Install the Secure Event Connector on your CDO Connector Virtual Machine](#)

### Before you begin

- Purchase the Cisco Security and Analytics Logging, **Logging and Troubleshooting** license, you may also purchase the **Logging Analytics and Detection** and **Total Network Analytics and Monitoring** licenses to apply Secure Cloud Analytics to the events.

If you would rather, you can request a trial version of Security Analytics and Logging by logging in to CDO, and on the main navigation bar, choose **Analytics > Event Logging** and click **Request Trial**.

- CDO requires strict certificate checking and does not support a Web/Content Proxy between the CDO Connector and the Internet.
- **The CDO Connector must have full outbound access to the Internet on TCP port 443.**
- **Review [Connect to Cisco Defense Orchestrator using Secure Device Connector](#) to ensure proper network access for the CDO Connector.**
- VMware ESXi host installed with vCenter web client or ESXi web client.




---

**Note** We do not support installation using the vSphere desktop client.

---

- ESXi 5.1 hypervisor.
- Cent OS 7 guest operating system.
- System requirements for a VM to host only a CDO Connector and an SEC:
  - CPU: Assign 4 CPUs to accommodate the SEC.
  - Memory: Assign 8 GB of memory for the SEC.
  - Disk Space: 64 GB
- Users performing this procedure should be comfortable working in a Linux environment and using the **vi** visual editor for editing files.
- If you are installing your CDO Connector on a CentOS virtual machine, we recommend you install Yum security patches on a regular basis. Depending on your Yum configuration, to acquire Yum updates, you may need to open outbound access on port 80 as well as 443. You will also need to configure yum-cron or crontab to schedule the updates. Work with your security-operations team to determine if any security policies need to change to allow you to get the Yum updates.
- Gather this information before you begin the installation:
  - Static IP address you want to use for your CDO Connector.
  - Passwords for the **root** and **cdo** users that you create during the installation process.
  - The IP address of the DNS server your organization uses.
  - The gateway IP address of the network the CDO Connector address is on.
  - The FQDN or IP address of your time server.
- The CDO Connector virtual machine is configured to install security patches on a regular basis and in order to do this, opening port 80 outbound is required.
- **Before you get started:** Do not copy and paste the commands in this procedure into your terminal window, type them instead. Some commands include an "n-dash" and in the cut and paste process, these commands can be applied as an "m-dash" and that may cause the command to fail.

## Procedure

- Step 1** From the Secure Device Connectors page, click the blue plus button  and click Secure Event Connector.
- Step 2** Using the link provided, copy the SEC Bootstrap Data in step 2 of the "Deploy an On-Premises Secure Event Connector" window.
- Step 3** Install a CentOS 7 virtual machine ([http://isoredirect.centos.org/centos/7/isos/x86\\_64/CentOS-7-x86\\_64-Minimal-1804.iso](http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso)) with at least the memory, CPU, and disk space mentioned in this procedure's prerequisites.
- Step 4** Once installed, configure basic networking such as specifying the IP address for the CDO Connector, the subnet mask, and gateway.
- Step 5** Configure a DNS (Domain Name Server) server.
- Step 6** Configure a NTP (Network Time Protocol) server.
- Step 7** Install an SSH server on CentOS for easy interaction with CDO Connector's CLI.
- Step 8** Run a Yum update and then install the packages: **open-vm-tools**, **nettools**, and **bind-utils**
- ```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```
- Step 9** Install the **AWS CLI** package (<https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html>)
- Note** Do not use the `--user` flag.
- Step 10** Install the **Docker CE** packages (<https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce>)
- Note** Use the "Install using the repository" method.
- Step 11** Start the Docker service and enable it to start on boot:
- ```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to /usr/lib/systemd/system/docker.service.
```
- Step 12** Create two users: **cdo** and **sdc**. The cdo user will be the one you log-into to run administrative functions (so you don't need to use the root user directly), and the sdc user will be the user to run the CDO Connector docker container.
- ```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```
- Step 13** Configure the sdc user to use crontab:
- ```
[root@sdc-vm ~]# touch /etc/cron.allow
[root@sdc-vm ~]# echo "sdc" >> /etc/cron.allow
```
- Step 14** Set a password for the cdo user.
- ```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```
- Step 15** Add the cdo user to the "wheel" group to give it administrative (sudo) privileges.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

- Step 16** When Docker is installed, there is a user group created. Depending on the version of CentOS/Docker, this may be called either "docker" or "dockerroot". Check the /etc/group file to see which group was created, and then add the sdc user to this group.

```
[root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

- Step 17** If the /etc/docker/daemon.json file does not exist, create it, and populate with the contents below. Once created, restart the docker daemon.

Note Make sure that the group name entered in the "group" key matches the [Step 16](#).

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
{
  "live-restore": true,
  "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

- Step 18** If you are currently using a vSphere console session, switch over to SSH and log in as the **cdo** user. Once logged in, change to the **sdc** user. When prompted for a password, enter the password for the **cdo** user.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

- Step 19** Change directories to /usr/local/cdo.

- Step 20** Create a new file called **bootstrapdata** and paste the bootstrap data from Step 1 of the deployment wizard into this file. **Save** the file. You can use **vi** or **nano** to create the file.

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

[illegible]

OK

The bootstrap data comes encoded in base64. Decode it and export it to a file called **extractedbootstrapdata**

Run the cat command to view the decoded data. The command and decoded data should look similar to this:

Run the following command to export the sections of the decoded bootstrap data to environment variables.

Download the bootstrap bundle from CDO.

```
[sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL" -o
$CDO_TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/CDO_<tenant_name>
```

Step 24

Extract the CDO Connector tarball, and run the bootstrap_sec_only.sh file to install the CDO Connector package.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

What to do next

Continue to [Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created](#), on page 39.

Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created

If you installed your CDO Connector on your own CentOS 7 virtual machine, you need to perform **one** of the following additional configuration procedures to allow events to reach the SEC.

- [Disable the firewalld service on the CentOS 7 VM](#). This matches the configuration of the Cisco-provided SDC VM.
- [Allow the firewalld service to run and add firewall rules to allow event traffic to reach the SEC](#), on page 40. This is a more granular approach to allowing inbound event traffic.

Before you begin:

This is the second of three steps you need to complete in order install and configure your SEC. If you have not already, complete [Install a CDO Connector to Support an SEC Using Your VM Image](#), on page 34 before making these configuration changes.

After you complete one of the additional configuration changes described here, complete [Install the Secure Event Connector on your CDO Connector Virtual Machine](#)

Disable the firewalld service on the CentOS 7 VM

1. Log into the CLI of the SDC VM as the "cdo" user.
2. Stop the firewalld service, and then ensure that it will remain disabled upon subsequent reboots of the VM. If you are prompted, enter the password for the **cdo** user:

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Restart the Docker service to re-insert Docker-specific entries into the local firewall:

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. Continue to [Install the Secure Event Connector on your CDO Connector Virtual Machine](#).

Allow the firewalld service to run and add firewall rules to allow event traffic to reach the SEC

1. Log into the CLI of the SDC VM as the "cdo" user.
2. Add local firewall rules to allow incoming traffic to the SEC from the TCP, UDP, or NSEL ports you configured. See [Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics \(SaaS\)](#) for the ports used by your SEC. If prompted, enter the password for the **cdo** user. Here is an example of the commands. You may need to specify different port values.

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. Restart the firewalld service to make the new local firewall rules both active and persistent:

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. Continue to [Install the Secure Event Connector on your CDO Connector Virtual Machine](#).

Install the Secure Event Connector on your CDO Connector Virtual Machine

Before you begin

This is the third of three steps you need to complete in order install and configure your Secure Event Connector (SEC). If you have not already, complete these two task before continuing with this procedure:

- [Install a CDO Connector to Support an SEC Using Your VM Image, on page 34](#)
- [Additional Configuration for SDCs and CDO Connectors Installed on a VM You Created, on page 39](#)

Procedure

-
- | | |
|---------------|---|
| Step 1 | Log in to CDO. |
| Step 2 | From the CDO menu, choose Tools & Services > Secure Connectors . |
| Step 3 | Select the CDO Connector that you installed using the procedure in the prerequisites above. In the Secure Connectors table, it will be called a Secure Event Connector. |
| Step 4 | Click Deploy an On-Premises Secure Event Connector in the Actions pane on the right. |

Step 5 In step 2 of the wizard, click the link to **Copy SEC Bootstrap**

Deploy an On-Premises Secure Event Connector

```
dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0ppq
YkdsbGJuUmZhV1FpT21KaGNHa3RZMnhwW1c1ME1uMC5tTzh0bTZMZ1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZQYzVsRjRITt1teVVEVzh2Qk5FWW44c3V0Z3NTQUo0TH15N0xzVGSydEx4N05nbS00STB6SmZ6
aWdQTKRiV1RsrW1tcjI5SkFVZ2NBWEhySkdzcktmREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzVl9qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VkxNOUp4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXduVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWDpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY2lZy28tYW1hbGxpbyIKQ0RXP0JPT1RTVFJBUf9VUkw9Imh0dHBz
O18vc3RhZ21uZy5kZXlYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpby
IKT05MWV9FVkvOVE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

Step 2

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM

```
U1NFX0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYy00Y2JkLWEzNWQ0OGYzZDJkMjQ1ZmU3IqpTU0VfRE
U0VfT1RQPSI5Y2IzNTI4ZWZlMzg0OTQ2NjViMDFkZmEyYjUyMGUxNSIKVEVOQU5UX05BTUU9IkNET1
9jaXNjby1hbWFsbG1vIg==
```

[Copy SEC Bootstrap Data](#)

Step 3

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Data.

Cancel

OK

Step 6 Connect to the Secure Connector using SSH and log in as the **cdo** user.

Step 7 Once logged in, switch to the **sdc** user. When prompted for a password, enter the password for the "cdo" user. Here is an example of those commands:

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

Step 8 At the prompt, run the sec.sh setup script:

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

Step 9 At the end of the prompt, paste the bootstrap data you copied in step 4 and press **Enter**.

Please copy the bootstrap data from Setup Secure Event Connector page of CDO:

```
KJHYFuYTFuIGhiJK1KnJHvHfgxTewrtwE
RtyFUIyIOHKNkjbKhvhgyRStwterTyufGUihoJpojP9U0oiUY8VHHGFXREWRTyghfVjhkOuihIuyftyXtfcghvjbkhB=
```

After the SEC is onboarded, the sec.sh runs a script to check on the health of the SEC. If all the health checks are "green," the health check sends a sample event to the Event Log. The sample event shows up in the Event Log as a policy named "sec-health-check."

```
=====
Running SEC health check for tenant [REDACTED]
=====
SEC cloud URL [REDACTED] is: Reachable
=====
SEC Connector status: Active
=====
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
=====
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

If you receive a message that the registration failed or that the SEC onboarding failed, go to [Troubleshooting Secure Event Connector Onboarding Failures](#).

If you receive the success message, click **Done** in the **Deploy an ON-Premise Secure Event Connector** dialog box. You have finished installing an SEC on a your VM image.

Step 10

Continue to "What to do next."

What to do next

Return to this procedure to continue your implementation of SAL SaaS: [Implementing Secure Logging Analytics \(SaaS\) for FDM-Managed Devices, on page 14](#).

Related Information:

- [Troubleshoot a Secure Device Connector](#)
- [Troubleshooting Secure Event Connector](#)
- [Troubleshooting SEC Onboarding Failures](#)
- [Troubleshooting SEC Registration Failure](#)

Install a Secure Event Connector on an AWS VPC Using a Terraform Module

Before you begin

- To perform this task, you must enable SAL on your CDO tenant. This section presumes that you have a SAL license. If you do not have one, purchase the Cisco Security and Analytics Logging, Logging and Troubleshooting license.
- Ensure you have a new SEC installed. To create a new SEC, see [Install a Secure Event Connector on an SDC Virtual Machine, on page 24](#).
- When installing the SEC, make sure you take a note of the CDO bootstrap data and SEC bootstrap data.

Procedure

- Step 1** Go to [Secure Event Connector Terraform Module](#) on the Terraform Registry and follow the instructions to add the SEC Terraform module to your Terraform code.
- Step 2** Apply the Terraform code.
- Step 3** Ensure that you print the `instance_id` and `sec_fqdn` outputs, because you will need them later in the procedure.

Note To troubleshoot your SEC, you must connect to your SEC instance using the AWS Systems Manager Session Manager (SSM). See the [AWS Systems Manager Session Manager](#) documentation to know more about connecting to an instance using SSM.

Ports to connect to the SDC instance using SSH are not exposed for security reasons.

- Step 4** To enable sending of logs from your ASA to the SEC, obtain the certificate chain of the SEC you created and remove the leaf certificate by running the following command with the output from [Step 3](#):

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 <
/dev/null | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if (/BEGIN CERTIFICATE/) {a++};
out="/tmp/cert_chain.pem"; if (a > 1) print >>out}'
```

- Step 5** Copy the contents of `/tmp/cert_chain.pem` to your clipboard.
- Step 6** Take a note of the IP address of the SEC using the following command:

```
nslookup <FQDN>
```

- Step 7** Log in to CDO and start adding a new trustpoint object. See [Adding a Trusted CA Certificate Object](#) for more information. Ensure you uncheck the **Enable CA flag in basic constraints extension** checkbox in **Other Options** before clicking **Add**.
- Step 8** Click **Add**, copy the CLI commands generated by CDO in the **Install Certificate** page, and click **Cancel**.
- Step 9** Below `enrollment terminal`, add `no ca-check` in a text clipboard.
- Step 10** SSH into your ASA device or use the ASA CLI option in CDO and execute the following commands:

```
DataCenterFW-1> en
Password: *****
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

What to do next

You can check if your SEC is receiving packets using AWS SSM:

You should now see logs similar to this:

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

Deprovisioning Cisco Security Analytics and Logging (SaaS)

If you allow your Cisco Security Analytics and Logging (SaaS) paid license to lapse, you have a grace period of 90 days. If you renew your paid license during this grace period, there is no interruption in your service.

Otherwise, if you allow the 90-day grace period to elapse, the system purges all of your customer data. You can no longer view ASA or FTD events from the Event Logging page, nor have dynamic entity modeling behavioral analytics applied to your ASA or FTD events and network flow data.

Remove the Secure Event Connector

Warning: This procedure deletes the Secure Event Connector from the Secure Device Connector. Doing so will prevent you from using Secure Logging Analytics (SaaS). It is not reversible. If you have any questions or concerns, [contact CDO support](#) before taking this action.

Removing the Secure Event Connector from your Secure Device Connector is a two-step process:

1. [Remove an SEC from CDO.](#)
2. [Remove SEC files from the SDC.](#)

What to do next: Continue to [Remove an SEC from CDO](#)

Remove an SEC from CDO

Before you begin

See [Remove the Secure Event Connector, on page 44.](#)

Procedure

-
- | | |
|---------------|--|
| Step 1 | Log in to CDO. |
| Step 2 | From the CDO menu, choose Tools & Services > Secure Connectors . |
| Step 3 | Select the row with the device type, Secure Event Connector . |
| | Warning: Be careful. Do NOT select your Secure Device Connector. |
| Step 4 | In the Actions pane, click Remove . |
| Step 5 | Click OK to confirm your intent to delete the Secure Event Connector. |
-

What to do next

Continue to [Remove SEC files from the SDC, on page 45.](#)

Remove SEC files from the SDC

This is the second part of a two part procedure to remove the Secure Event Connector from your SDC. See [Remove the Secure Event Connector, on page 44](#) before you begin.

Procedure

-
- Step 1** Open your virtual machine hypervisor and start a console session for your SDC.
- Step 2** Switch to the SDC user.
- ```
[cdo@tenant toolkit]$sudo su sdc
```
- Step 3** At the prompt type one of these commands:
- If you are managing only your own tenant:
- ```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
```
- If you manage more than one tenant, add CDO_ to the beginning of the tenant name. For example:
- ```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
```
- Step 4** Confirm your intention to remove the SEC files.
- 

## Provision a Cisco Secure Cloud Analytics Portal

**Required License:** **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

If you purchase a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, after you deploy and configure the Secure Event Connector (SEC), you must associate a Secure Cloud Analytics portal with your CDO portal to view Secure Cloud Analytics alerts. When you purchase the license, if you have an existing Secure Cloud Analytics portal, you can provide the Secure Cloud Analytics portal name and immediately link it to your CDO portal.

Otherwise, you can request a new Secure Cloud Analytics portal from the CDO UI. The first time you access Secure Cloud Analytics alerts, the system takes you to a page to request the Secure Cloud Analytics portal. The user that requests this portal is granted administrator permission in the portal.

### Procedure

- 
- Step 1** From the CDO menu, choose **Analytics > Secure Cloud Analytics** to open the Secure Cloud Analytics UI in a new window.
- Step 2** Click **Start Free Trial** to provision a Secure Cloud Analytics portal and associate it with your CDO portal.
- Note** After you request the portal, the provisioning may take up to several hours.
- 

Ensure that your portal is provisioned before moving on to the next step.

1. From the CDO menu, choose **Analytics > Secure Cloud Analytics** to open the Secure Cloud Analytics UI in a new window.
2. You have the following options:
  - If you requested a Secure Cloud Analytics portal, and the system states it is still provisioning the portal, wait and try to access the alerts later.
  - If the Secure Cloud Analytics portal is provisioned, enter your **Username** and **Password**, then click **Sign in**.



**Note** The administrator user can invite other users to create accounts within the Secure Cloud Analytics portal. See [Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 48](#) for more information.

### What to do next

- If you purchased a **Logging Analytics and Detection** license, your configuration is complete. If you want to view the status of your CDO integration or sensor health from the Secure Cloud Analytics portal UI, see [Review Sensor Health and CDO Integration Status in Secure Cloud Analytics, on page 46](#) for more information. If you want to work with alerts in the Secure Cloud Analytics portal, see [Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 48](#) and [Working with Alerts Based on Firewall Events](#) for more information.
- If you purchased a **Total Network Analytics and Monitoring** license, deploy one or more Secure Cloud Analytics sensors to your internal network to pass network flow data to the cloud. If you want to monitor cloud-based network flow data, configure your cloud-based deployment to pass flow data to Secure Cloud Analytics. See [Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting, on page 47](#) for more information.

## Review Sensor Health and CDO Integration Status in Secure Cloud Analytics

### Sensor Status

#### Required License: Logging Analytics and Detection or Total Network Analytics and Monitoring

In the Secure Cloud Analytics web UI, you can view your CDO integration status and your configured sensors from the Sensor List page. The CDO integration is the read-only *connection-events* sensor. Stelathwatch Cloud provides an overall health of your sensors in the main menu:

- green cloud icon (🟢) - connectivity established with all sensors, and CDO if configured
- yellow cloud icon (🟡) - connectivity established with some sensors, or CDO if configured, and one or more sensors is not configured properly
- red cloud icon (🔴) - connectivity lost with all configured sensors, and CDO if configured

Per sensor or CDO integration, a green icon signifies connectivity established, and a red icon signifies connectivity lost.

## Procedure

- Step 1** 1. In the Secure Cloud Analytics portal UI, select **Settings** (⚙️) > **Sensors**.
- Step 2** Select **Sensor List**.

# Cisco Secure Cloud Analytics Sensor Deployment for Total Network Analytics and Reporting

## Secure Cloud Analytics Sensor Overview and Deployment

### Required License: Total Network Analytics and Monitoring

If you obtain a **Total Network Analytics and Monitoring** license, after you provision a Secure Cloud Analytics portal, you can:

- Deploy and configure a Secure Cloud Analytics sensor within your on-premises network to pass network flow data to the cloud for analysis.
- Configure your cloud-based deployment to pass network flow log data to Secure Cloud Analytics for analysis.

Firewalls at your network perimeter gather information about traffic between your internal network and external networks, while Secure Cloud Analytics sensors gather information about traffic within your internal network.



**Note** FDM-managed Secure Firewall Threat Defense devices may be configured to pass NetFlow data. When you deploy a sensor, do not configure it to pass NetFlow data from any of your FDM-managed Secure Firewall Threat Defense devices which you also configured to pass event information to CDO.

See the [Secure Cloud Analytics Sensor Installation Guide](#) for sensor deployment instructions and recommendations.

See the [Secure Cloud Analytics Public Cloud Monitoring Guides](#) for cloud-based deployment configuration instructions and recommendations.



**Note** You can also review instructions in the Secure Cloud Analytics portal UI to configure sensors and your cloud-based deployment.

See the [Secure Cloud Analytics Free Trial Guide](#) for more information about Secure Cloud Analytics.

## Next Steps

- Continue with [Viewing Cisco Secure Cloud Analytics Alerts from CDO, on page 48](#).

# Viewing Cisco Secure Cloud Analytics Alerts from CDO

**Required License:** **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

While you can review your firewall events on the Events logging page, you cannot review Cisco Secure Cloud Analytics alerts from the CDO portal UI. You can cross-launch from CDO to the Secure Cloud Analytics portal using the Security Analytics menu option, and view alerts generated from firewall event data (and from network flow data if you enabled **Total Network Analytics and Monitoring**). The Security Analytics menu option displays a badge with the number of Secure Cloud Analytics alerts in an open workflow status, if 1 or more are open.

If you use a Security Analytics and Logging license to generate Secure Cloud Analytics alerts, and you provisioned a new Secure Cloud Analytics portal, log into CDO, then cross-launch to Secure Cloud Analytics using Cisco Security Cloud Sign On. You can also directly access your Secure Cloud Analytics portal through its URL.

See [Cisco Security Cloud Sign On](#) for more information.

## Inviting Users to Join Your Secure Cloud Analytics Portal

The initial user to request the Secure Cloud Analytics portal provision has administrator privileges in the Secure Cloud Analytics portal. That user can invite other users by email to join the portal. If these users do not have Cisco Security Cloud Sign On credentials, they can create them using the link in the invite email. Users can then use Cisco Security Cloud Sign On credentials to log in during the cross-launch from CDO to Secure Cloud Analytics.

To invite other users to your Secure Cloud Analytics portal by email:

### Procedure

- 
- Step 1** Log into your Secure Cloud Analytics portal as an administrator.
  - Step 2** Select **Settings > Account Management > User Management**.
  - Step 3** Enter an **Email** address.
  - Step 4** Click **Invite**.
- 

## Cross-Launching from CDO to Secure Cloud Analytics

To view security alerts from CDO:

### Procedure

- 
- Step 1** Log into the CDO portal.
  - Step 2** From the CDO menu, choose **Analytics > Secure Cloud Analytics**.
  - Step 3** In the Secure Cloud Analytics interface, select **Monitor > Alerts**.
-



# Cisco Secure Cloud Analytics and Dynamic Entity Modeling

## Required License: **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Secure Cloud Analytics is a software as a service (SaaS) solution that monitors your on-premises and cloud-based network deployments. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

## Dynamic Entity Modeling

Dynamic entity modeling tracks the state of your network by performing a behavioral analysis on firewall events and network flow data. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they take on your network. Secure Cloud Analytics, integrated with a **Logging Analytics and Detection** license, can draw from firewall events and other traffic information in order to determine the types of traffic the entity usually transmits. If you purchase a **Total Network Analytics and Monitoring** license, Secure Cloud Analytics can also include NetFlow and other traffic information in modeling entity traffic. Secure Cloud Analytics updates these models over time, as the entities continue to send traffic, and potentially send different traffic, to keep an up-to-date model of each entity. From this information, Secure Cloud Analytics identifies:

- Roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- Observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, or a remote access session established with another entity. If you integrate with CDO, these facts can be obtained from firewall events. If you also purchase a **Total Network Analytics and Monitoring** license, the system can also obtain facts from NetFlow, and generate observations from both firewall events and NetFlow. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

## Alerts and Analysis

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system. Note that one alert may represent multiple observations. If a firewall logs multiple connection events related to the same connection and entities, this may result in only one alert.

For example, a New Internal Device observation on its own does not constitute possible malicious behavior. However, over time, if the entity transmits traffic consistent with a Domain Controller, then the system assigns a Domain Controller role to the entity. If the entity subsequently establishes a connection to an external server that it has not established a connection with previously, using unusual ports, and transfers large amounts of data, the system would log a New Large Connection (External) observation and an Exceptional Domain Controller observation. If that external server is identified as on a Talos watchlist, then the combination of all

this information would lead Secure Cloud Analytics to generate an alert for this entity's behavior, prompting you to take further action to research, and remediate malicious behavior.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available. You can also see other observations and alerts that entities were involved with, and determine if this behavior is tied to other potentially malicious behavior.

Note that when you view and close alerts in Secure Cloud Analytics, you cannot allow or block traffic from the Secure Cloud Analytics UI. You must update your firewall access control rules to allow or block traffic, if you deployed your devices in active mode, or your firewall access control rules if your firewalls are deployed in passive mode.

## Working with Alerts Based on Firewall Events

**Required License:** Logging Analytics and Detection or Total Network Analytics and Monitoring

### Alerts Workflow

An alert's workflow is based around its status. When the system generates an alert, the default status is Open, and no user is assigned. When you view the Alerts summary, all open alerts are displayed by default, as these are of immediate concern.

Note: If you have a **Total Network Analytics and Monitoring** license, your alerts can be based on observations generated from NetFlow, observations generated from firewall events, or observations from both data sources.

As you review the Alerts summary, you can assign, tag, and update status on alerts as an initial triage. You can use the filters and search functionality to locate specific alerts, or display alerts of different statuses, or associated with different tags or assignees. You can set an alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove Snoozed status from an alert, to display it as an open alert again. As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

From the Alerts summary, you can view an alert detail page. This page allows you to review additional context about the supporting observations that resulted in this alert, and additional context about the entities involved in this alert. This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior.

As you research within the Secure Cloud Analytics web portal UI, in CDO, and on your network, you can leave comments with the alert that describe your findings. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to Closed, and have it no longer appear by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

The following presents general guidelines and suggestions for how to investigate a given alert. Because Secure Cloud Analytics provides additional context when it logs an alert, you can use this context to help guide your investigation.

These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

In general, you can take the following steps when you review an alert:

1. [Triage open alerts, on page 51](#)

2. [Snooze alerts for later analysis, on page 51](#)
3. [Update the alert for further investigation, on page 52](#)
4. [Review the alert and start your investigation, on page 52](#)
5. [Examine the entity and users, on page 54](#)
6. [Remediate issues using Secure Cloud Analytics, on page 54](#)
7. [Update and close the alert, on page 55](#)

## Triage open alerts

Triage the open alerts, especially if more than one have yet to be investigated:

- See [Viewing Cisco Secure Cloud Analytics Alerts from CDO](#) for more information on cross-launching from CDO to Secure Cloud Analytics, and viewing alerts.

Ask the following questions:

- Have you configured this alert type as high priority?
- Did you set a high sensitivity for the affected subnet?
- Is this unusual behavior from a new entity on your network?
- What is the entity's normal role, and how does the behavior in this alert fit that role?
- Is this an exceptional deviation from normal behavior for this entity?
- If a user is involved, is this expected behavior from the user, or exceptional?
- Is protected or sensitive data at risk of being compromised?
- How severe is the impact to your network if this behavior is allowed to continue?
- If there is communication with external entities, have these entities established connections with other entities on your network in the past?

If this is a *high* priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

## Snooze alerts for later analysis

Snooze alerts when they are of lesser priority, as compared to other alerts. For example, if your organization is repurposing an email server as an FTP server, and the system generates an Emergent Profile alert (indicating that an entity's current traffic matches a behavior profile that it did not previously match), you can snooze this alert as it is intended behavior, and revisit it at a later date. A snoozed alert does not show up with the open alerts; you must specifically filter to review these snoozed alerts.

Snooze an alert:

### Procedure

---

- Step 1** Click **Close Alert**.
- Step 2** In the Snooze this alert pane, select a snooze period from the drop-down.
- Step 3** Click **Save**.
- 

### What to do next

When you are ready to review these alerts, you can unsnooze them. This sets the status to Open, and displays the alert alongside the other Open alerts.

Unsnuzzle a snoozed alert:

- From a snoozed alert, click **Unsnuzzle Alert**.

## Update the alert for further investigation

Open the alert detail:

### Procedure

---

- Step 1** Select **Monitor > Alerts**.
- Step 2** Click an alert type name.
- 

### What to do next

Based on your initial triage and prioritization, assign the alert and tag it:

1. Select a user from the **Assignee** drop-down to assign the alert, so a user can start investigating.
2. Select one or more **Tags** from the drop-down to add tags to the alert, to better categorize your alert's for future identification, as well as to try and establish long-term patterns in your alerts.
3. Enter a **Comment on this alert**, then click **Comment** to leave comments as necessary to track your initial findings, and assist the person assigned to the alert. The alert tracks both system comments and user comments.

## Review the alert and start your investigation

If you are reviewing an assigned alert, review the alert detail to understand why Secure Cloud Analytics generated an alert. Review the supporting observations to understand what these observations mean for the source entity.

Note that if the alert was generated based on firewall events, the system does not note that your firewall deployment was the source of this alert.

View all of the supporting observations for this source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend:

### Procedure

- 
- Step 1** From the alert detail, click the arrow icon (➡) next to an observation type to view all logged observations of that type.
- Step 2** Click the arrow icon (➡) next to **All Observations for Network** to view all logged observations for this alert's source entity.
- 

Download the supporting observations in a comma-separated value file, if you want to perform additional analysis on these observations:

- From the alert detail, in the Supporting Observations pane, click **CSV**.

From the observations, determine if the source entity behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.

View additional context surrounding the source entity from a source entity IP address or hostname, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting:

- Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
- Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
- Select **Device** from the IP address or hostname drop-down to view information about the device.
- Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that the source entity in Secure Cloud Analytics is always internal to your network. Contrast this with the Initiator IP in a firewall event, which indicates the entity that initiated a connection, and may be internal or external to your network.

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.

Review the context for an external entity IP address or hostname with which the source entity established a connection:

- Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
- Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.

- Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
- Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
- Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
- Select **Talos Intelligence** from the IP address or hostname drop-down to view information about this information on Talos's website.
- Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
- Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that connected entities in Secure Cloud Analytics are always external to your network. Contrast this with the Responder IP in a firewall event, which indicates the entity that responded to a connection request, and may be internal or external to your network.

Leave comments as to your findings.

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

## Examine the entity and users

After you review the alert in the Secure Cloud Analytics portal UI, you can perform an additional examination on a source entity directly, any users that may have been involved with this alert, and other related entities.

- Determine where the source entity is on your network, physically or in the cloud, and access it directly. Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.
- Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.
- Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.

Leave comments as to your findings:

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

## Remediate issues using Secure Cloud Analytics

If malicious behavior caused the alert, remediate the malicious behavior. For example:

- If a malicious entity or user attempted to log in from outside your network, update your firewall rules and firewall configuration to prevent the entity or user from accessing your network.
- If an entity attempted to access an unauthorized or malicious domain, examine the affected entity to determine if malware is the cause. If there are malicious DNS redirects, determine if other entities on your network are affected, or part of a botnet. If this is intended by a user, determine if there is a legitimate reason for this, such as testing firewall settings. Update your firewall rules and firewall configuration to prevent further access to the domain.
- If an entity is exhibiting behavior that is different from the historical entity model behavior, determine if the behavior change is intended. If it is unintended, examine whether an otherwise authorized user on your network is responsible for the change. Update your firewall rules and firewall configuration to address unintended behavior if it involves connections with entities that are external to your network.
- If you identify a vulnerability or exploit, update or patch the affected entity to remove the vulnerability, or update your firewall configuration to prevent unauthorized access. Determine if other entities on your network may similarly be affected, and apply the same update or patch to those entities. If the vulnerability or exploit currently does not have a fix, contact the appropriate vendor to let them know.
- If you identify malware, quarantine the entity and remove the malware. Review the firewall file and malware events to determine if other entities on your network are at risk, and quarantine and update the entities to prevent this malware from spreading. Update your security intelligence with information about this malware, or the entities that caused this malware. Update your firewall access control and file and malware rules to prevent this malware from infecting your network in the future. Alert vendors as necessary.
- If malicious behavior resulted in data exfiltration, determine the nature of the data sent to an unauthorized source. Follow your organization's protocols for unauthorized data exfiltration. Update your firewall configuration to prevent future data exfiltration attempts by this source.

## Update and close the alert

Add additional tags based on your findings:

### Procedure

- 
- |               |                                                                              |
|---------------|------------------------------------------------------------------------------|
| <b>Step 1</b> | In the Secure Cloud Analytics portal UI, select <b>Monitor &gt; Alerts</b> . |
| <b>Step 2</b> | Select one or more <b>Tags</b> from the drop-down.                           |
- 

Add final comments describing the results of your investigation, and any remediation steps taken:

- From an alert's detail, enter a **Comment on this alert**, then click **Comment**.

Close the alert, and mark it as helpful or not helpful:

1. From an alert's detail, click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. Note that this does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. Click **Save**.

**What to do next****Reopen a closed alert**

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can then make changes as necessary to the alert, then close it again when your additional investigation is complete.

Reopen a closed alert:

- From a closed alert's detail, click **Reopen Alert**.

## Modifying Alert Priorities

**Required License:** **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alert types come with default priorities, which affect how sensitive the system is to generating alerts of this type. Alerts default to *low* or *normal* priority, based on Cisco intelligence and other factors. Based on your network environment, you may want to reprioritize alert types, to emphasize certain alerts that you are concerned with. You can configure any alert type to be *low*, *normal*, or *high* priority.

- Select **Monitor > Alerts**.
- Click the settings drop-down icon (⚙️), then select **Alert Types and Priorities**.
- Click the edit icon (✎️) next to an alert type and select *low*, *medium*, or *high* to change the priority.

## Viewing Live Events

The Live events page shows the most recent 500 events that match the [Searching for and Filtering Events in the Event Logging Page](#) you entered. If the Live events page displays the maximum of 500 events, and more events stream in, CDO displays the newest live events, and transfers the oldest live events to the Historical events page, keeping the total number of live events at 500. That transfer takes roughly a minute to perform. If no filtering criteria is added, you will see all the latest Live 500 events generated by rules configured to log events.

The event timestamps are shown in UTC.

Changing the filtering criteria, whether live events are playing or paused, clears the events screen and restarts the collection process.

To see live events in the CDO Events viewer:

**Procedure**

- 
- Step 1** In the navigation pane, choose **Analytics > Event Logging**.
- Step 2** Click the **Live** tab.
-





**What to do next**

See how to play and pause events by reading .

**Related Information:**

- [Play/Pause Live Events, on page 57](#)
- [View Historical Events, on page 58](#)
- [Customize the Events View, on page 58](#)

## Play/Pause Live Events

You can "play"  or "pause"  live events as they stream in. If live events are "playing," CDO displays events that match the filtering criteria specified in the Events viewer in the order they are received. If events are paused, CDO does not update the Live events page until you restart playing live events. When you restart playing events, CDO begins populating events in the Live page from the point at which you restarted playing events. It doesn't back-fill the ones you missed.

To view all the events that CDO received whether you played or paused live event streaming, click the Historical tab.







**Auto-pause Live Events**

After displaying events for about 5 consecutive minutes, CDO warns you that it is about to pause the stream of live events. At that time, you can click the link to continue streaming live events for another 5 minutes or allow the stream to stop. You can restart the live events stream when you are ready.

**Receiving and Reporting Events**

There may be a small lag between the Secure Event Connector (SEC) receiving events and CDO posting events in the Live events viewer. You can view the gap on the Live page. The time stamp of the event is the time it was received by SEC.

**Events**

| Events                                                                                                                            |                                                                                     |                                   |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------|
|                                                |  | Search by event fields and values |
| <div>Historical <span>Live</span></div>                                                                                           |                                                                                     |                                   |
| Date/Time                                                                                                                         |                                                                                     | Event Type                        |
|  Waiting for matching events after 1:38:40 PM. |                                                                                     |                                   |
|                                                | May 31, 2019 1:33:35 PM                                                             | Connection                        |
|                                                | May 31, 2019 1:33:36 PM                                                             | Connection                        |
|                                                | May 31, 2019 1:33:44 PM                                                             | Connection                        |

## View Historical Events

The Live events page shows the most recent 500 events that match the [Searching for and Filtering Events in the Event Logging Page](#) you entered. Events older than the most recent 500 are transferred to the Historical events table. That transfer takes roughly a minute to perform. You can then filter all the events you have stored to find events you're looking for.

To view historical events:

### Procedure

- 
- Step 1** In the navigation pane, choose **Analytics > Event Logging**.
- Step 2** Click the **Historical** tab. By default, when you open the Historical events table, the filter is set to display the events collected within the last hour.
- The event attributes are largely the same as what is reported by Firepower Device Manager (FDM) or the Adaptive Security Device Manager (ASDM).
- For a complete description of Firepower Threat Defense event attributes, see [Cisco FTD Syslog Messages](#).
  - For a complete description of ASA event attributes, see [Cisco ASA Series Syslog Messages](#).
- 

## Customize the Events View

Any changes made to the Event Logging page are automatically saved for when you navigate away from this page and come back at a later time.




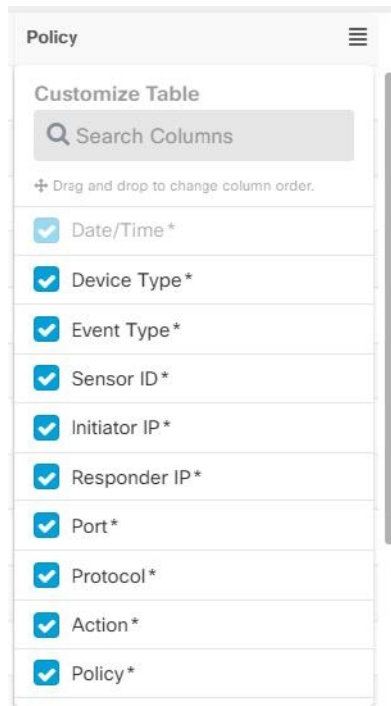
---

**Note** The Live and Historical events view have the same configuration. When you customize the events view, these changes are applied to both the Live and Historical view.

---


### Show or Hide Columns

You can modify the event view for both live and historical events to only include column headers that apply to the view you want. Click the column filter icon  located to the right of the columns and select or deselect the columns you want:

**Figure 1: Show or Hide Columns**

Columns with asterisks are provided within the event table by default, although you can remove them at any time. Use the search bar to manually search for keywords for additional columns you may want to include.

### Reorder the Columns

You can reorder the columns of the Events view. Click the column filter icon  located to the right of the columns to expand the list of selected columns and manually drag/drop the columns into the order you want, where the column at the top of the list in the drop-down menu is the left-most column in the Event View.

### Related Information:

- [Searching for and Filtering Events in the Event Logging Page](#)
- [Event Attributes in Security Analytics and Logging](#)


## Show and Hide Columns on the Event Logging Page

The Event Logging page displays ASA and FTD syslog events and ASA NetFlow Secure Event Logging (NSEL) events sent to the Cisco cloud from configured ASA and FDM-managed devices.

You can show or hide columns on the Event Logging page by using the Show/Hide widget with the table:

### Procedure

- 
- Step 1** From the CDO navigation bar, choose **Analytics > Event Logging**.

- Step 2** Scroll to the far right of the table and click the **Show/Hide Columns** button .
- Step 3** Check the columns you want to see and uncheck the columns you want to hide.
- Step 4** Mouse-over the column names in the Show/Hide Columns drop down menu and grab the grey cross to rearrange the column order.

Other users logging into the tenant will see the same columns you chose to show until columns are shown or hidden again.

This table describes the column headers:

| Column Header | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Date/Time     | The time the device generated the event. Time is displayed in the local time of your computer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Device Type   | FTD (Firepower Threat Defense)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Event Type    | <p>This composite column can have any of the following:</p> <ul style="list-style-type: none"> <li>• <b>FTD Event Types</b> <ul style="list-style-type: none"> <li>• Connection-Displays connection events from access control rules.</li> <li>• File-Displays events reported by file policies in access control rules.</li> <li>• Intrusion-Displays events reported by intrusion policy in access control rules.</li> <li>• Malware-Displays events reported by malware policies in access control rules.</li> </ul> </li> <li>• <b>ASA Event Types</b>-These event types represent groups of syslog or NetFlow events. See <a href="#">ASA Event Types</a> for more information about which syslog ID or which NetFlow ID is included in which group. <ul style="list-style-type: none"> <li>• Parsed Events-Parsed syslog events contain more event attributes than other syslog events and CDO is able to return search results based on those attributes more quickly. Parsed events are not a filtering category; however, parsed event IDs are displayed in the Event Types column in <i>italics</i>. Event IDs that are not displayed in <i>italics</i> are not parsed.</li> </ul> </li> <li>• ASA NetFlow Event IDs: All <a href="#">Netflow (NSEL) events</a> from ASA appear here.</li> </ul> |

| Column Header | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sensor ID     | The Sensor ID is the IP address from which events are sent to the Secure Event Connector. This is typically the Management interface on the Firepower Threat Defense or the ASA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Initiator IP  | This is the IP address of the source of the network traffic. The value of the Initiator address field corresponds to the value of the InitiatorIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Responder IP  | This is the destination IP address of the packet. The value of the Destination address field corresponds to the value in the ResponderIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Port          | The port or ICMP code used by the session <b>responder</b> . The value of the destination port corresponds to the value of the <b>ResponderPort</b> in the event details.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Protocol      | It represents the protocol in the events.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Action        | <p>Specifies the security action defined by the rule. The value you enter must be an exact match to what you want to find; however, the case doesn't matter. Enter different values for connection, file, intrusion, malware, syslog, and NetFlow event types:</p> <ul style="list-style-type: none"> <li>• For connection event types, the filter searches for matches in the AC_RuleAction attribute. Those values could be Allow, Block, Trust.</li> <li>• For file event types, the filter searches for matches in the FileAction attribute. Those values could be Allow, Block, Trust.</li> <li>• For intrusion event types, the filter searches for matches in the InLineResult attribute. Those values could be Allowed, Blocked, Trusted.</li> <li>• For malware event types, the filter searches for matches in the FileAction attribute. Those values could be Cloud Lookup Timeout.</li> <li>• For syslog and NetFlow events types, the filter searches for matches in the Action attribute.</li> </ul> |

| Column Header | Description                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------|
| Policy        | The name of the policy that triggered the event. Names will be different for ASA and FDM-managed devices. |

**Related Information:**

[Searching for and Filtering Events in the Event Logging Page, on page 92](#)

## Customizable Event Filters

If you are a Secure Logging Analytics (SaaS) customer, you can create and save custom filters that you use frequently.

The elements of your filter are saved to a filter tab as you configure them. Whenever you return to the Event Logging page, these searches will be available to you. They will not be available to other CDO users of the tenant. They will not be available to you on a different tenant, if you manage more than one tenant.



**Note** Be aware that when you are working in a filter tab, if you modify any filter criteria, those changes are saved to your custom filter tab automatically.

**Procedure**

- Step 1** From the main menu, choose **Analytics > Event Logging**.
  - Step 2** Clear the Search field of any values.
  - Step 3** Above the event table, click the blue plus button to add a View tab. Filter views are labeled "View 1", "View 2", "View 3" and so on until you give them a name.
- 
- Step 4** Select a view tab.
  - Step 5** Open the filter bar and select the filters attributes you want in your custom filter. See [Searching for and Filtering Events in the Event Logging Page, on page 92](#). Remember that only filter attributes are saved in the custom filter.
  - Step 6** Customize the columns you want to show in the event logging table. See [Show and Hide Columns on the Event Logging Page, on page 59](#) for a discussion of showing and hiding columns.
  - Step 7** Double-click the filter tab with the "View X" label and rename it.
  - Step 8** (Optional) Now that you have created a custom filter, you can fine tune the results displayed on the Event Logging page, without changing the custom filter, by adding search criteria to the Search field. See [Searching for and Filtering Events in the Event Logging Page, on page 92](#).

# Event Attributes in Security Analytics and Logging

## Event Attribute Descriptions

The event attribute descriptions used by CDO are largely the same as what is reported by Firepower Device Manager (FDM) and Adaptive Security Device Manager (ASDM).

- For a complete description of FDM-managed device event attributes, see [Cisco Firepower Threat Defense Syslog Messages](#).

Some ASA syslog events are "parsed" and others have additional attributes which you can use when filtering the contents of the Event Logging table using attribute:value pairs. See these additional topics for other important attributes of syslog events:

- [EventGroup and EventGroupDefinition Attributes for Some Syslog Messages](#)
- [EventName Attributes for Syslog Events](#)
- [Time Attributes in a Syslog Event](#)

## EventGroup and EventGroupDefinition Attributes for Some Syslog Messages

Some syslog events will have the additional attributes "EventGroup" and "EventGroupDefinition". You will be able to filter the events table to find events using these additional attributes by filtering by attribute:value pairs. For example, you could filter for Application Firewall events by entering `apfw:415*` in the search field of the Event Logging table.

### Syslog Message Classes and Associated Message ID Numbers

| EventGroup  | EventGroupDefinition        | Syslog Message ID Numbers (first 3 digits) |
|-------------|-----------------------------|--------------------------------------------|
| aaa/auth    | User Authentication         | 109, 113                                   |
| acl/session | Access Lists/User Session   | 106                                        |
| apfw        | Application Firewall        | 415                                        |
| bridge      | Transparent Firewall        | 110, 220                                   |
| ca          | PKI Certification Authority | 717                                        |
| citrix      | Citrix Client               | 723                                        |
| clst        | Clustering                  | 747                                        |
| cmgr        | Card Management             | 323                                        |
| config      | Command Interface           | 111, 112, 208, 308                         |
| csd         | Secure Desktop              | 724                                        |
| cts         | Cisco TrustSec              | 776                                        |
| dap         | Dynamic Access Policies     | 734                                        |

| EventGroup     | EventGroupDefinition                                     | Syslog Message ID Numbers (first 3 digits)                                                         |
|----------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| eap, eapoudp   | EAP or EAPoUDP for Network Admission Control             | 333, 334                                                                                           |
| eigrp          | EIGRP Routing                                            | 336                                                                                                |
| email          | E-mail Proxy                                             | 719                                                                                                |
| ipaa/envmon    | Environment Monitoring                                   | 735                                                                                                |
| ha             | Failover                                                 | 101, 102, 103, 104, 105, 210, 311, 709                                                             |
| idfw           | Identity-based Firewall                                  | 746                                                                                                |
| ids            | Intrusion Detection System                               | 733                                                                                                |
| ids/ips        | Intrusion Detection System / Intrusion Protection System | 400                                                                                                |
| ikev2          | IKEv2 Toolkit                                            | 750, 751, 752                                                                                      |
| ip             | IP Stack                                                 | 209, 215, 313, 317, 408                                                                            |
| ipaa           | IP Address Assignment                                    | 735                                                                                                |
| ips            | Intrusion Protection System                              | 401, 420                                                                                           |
| ipv6           | IPv6                                                     | 325                                                                                                |
| l4tm           | Block lists, Allow lists, grey lists                     | 338                                                                                                |
| lic            | Licensing                                                | 444                                                                                                |
| mdm-proxy      | MDM Proxy                                                | 802                                                                                                |
| nac            | Network Admission Control                                | 731, 732                                                                                           |
| vpn/nap        | IKE and IPsec / Network Access Point                     | 713                                                                                                |
| np             | Network Processor                                        | 319                                                                                                |
| ospf           | OSPF Routing                                             | 318, 409, 503, 613                                                                                 |
| passwd         | Password Encryption                                      | 742                                                                                                |
| pp             | Phone Proxy                                              | 337                                                                                                |
| rip            | RIP Routing                                              | 107, 312                                                                                           |
| rm             | Resource Manager                                         | 321                                                                                                |
| sch            | Smart Call Home                                          | 120                                                                                                |
| session        | User Session                                             | 108, 201, 202, 204, 302, 303, 304, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710 |
| session/natpat | User Session/NAT and PAT                                 | 305                                                                                                |
| snmp           | SNMP                                                     | 212                                                                                                |



| EventGroup     | EventGroupDefinition         | Syslog Message ID Numbers (first 3 digits)                                               |
|----------------|------------------------------|------------------------------------------------------------------------------------------|
| ssafe          | ScanSafe                     | 775                                                                                      |
| ssl/np ssl     | SSL Stack/NP SSL             | 725                                                                                      |
| svc            | SSL VPN Client               | 722                                                                                      |
| sys            | System                       | 199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741 |
| tre            | Transactional Rule Engine    | 780                                                                                      |
| ucime          | UC-IME                       | 339                                                                                      |
| tag-switching  | Service Tag Switching        | 779                                                                                      |
| td             | Threat Detection             | 733                                                                                      |
| vm             | VLAN Mapping                 | 730                                                                                      |
| vpdn           | PPTP and L2TP Sessions       | 213, 403, 603                                                                            |
| vpn            | IKE and IPsec                | 316, 320, 402, 404, 501, 602, 702, 713, 714, 715                                         |
| vpnc           | VPN Client                   | 611                                                                                      |
| vpnfo          | VPN Failover                 | 720                                                                                      |
| vpnlb          | VPN Load Balancing           | 718                                                                                      |
| vxlan          | VXLAN                        | 778                                                                                      |
| webfo          | WebVPN Failover              | 721                                                                                      |
| webvpn         | WebVPN and AnyConnect Client | 716                                                                                      |
| session/natpat | User Session / NAT and PAT   | 305                                                                                      |

## EventName Attributes for Syslog Events

Some syslog events will have the additional attribute "EventName". You will be able to filter the events table to find events using the EventName attribute by filtering by attribute:value pairs. For example, you could filter events for a "Denied IP packet" by entering **EventName:"Denied IP Packet"** in the search field of the Event Logging table.

### Syslog Event ID and Event Names Tables

- [AAA Syslog Event IDs and Event Names](#)
- [Botnet Syslog Event IDs and Event Names](#)
- [Failover Syslog Event IDs and Event Names](#)
- [Firewall Denied Syslog Event IDs and Event Names](#)
- [Firewall Traffic Syslog Event IDs and Event Names](#)

- [Identity Based Firewall Syslog Event IDs and Event Names](#)
- [IPSec Syslog Event IDs and Event Names](#)
- [NAT Syslog Event ID and Event Names](#)
- [SSL VPN Syslog Event IDs and Event Names](#)

#### AAA Syslog Event IDs and Event Names

| EventID | EventName              |
|---------|------------------------|
| 109001  | AAA Begin              |
| 109002  | AAA Failed             |
| 109003  | AAA Server Failed      |
| 109005  | Authentication Success |
| 109006  | Authentication Failed  |
| 109007  | Authorization Success  |
| 109008  | Authorization Failed   |
| 109010  | AAA Pending            |
| 109011  | AAA Session Started    |
| 109012  | AAA Session Ended      |
| 109013  | AAA                    |
| 109014  | AAA Failed             |
| 109016  | AAA ACL not found      |
| 109017  | AAA Limit Reach        |
| 109018  | AAA ACL Empty          |
| 109019  | AAA ACL error          |
| 109020  | AAA ACL error          |
| 109021  | AAA error              |
| 109022  | AAA HTTP limit reached |
| 109023  | AAA auth required      |
| 109024  | Authorization Failed   |
| 109025  | Authorization Failed   |
| 109026  | AAA error              |

| EventID | EventName                 |
|---------|---------------------------|
| 109027  | AAA Server error          |
| 109028  | AAA Bypassed              |
| 109029  | AAA ACL error             |
| 109030  | AAA ACL error             |
| 109031  | Authentication Failed     |
| 109032  | AAA ACL error             |
| 109033  | Authentication Failed     |
| 109034  | Authentication Failed     |
| 109035  | AAA Limit Reach           |
| 113001  | AAA Session limit reach   |
| 113003  | AAA overridden            |
| 113004  | AAA Successful            |
| 113005  | Authorization Rejected    |
| 113006  | AAA user locked           |
| 113007  | AAA User unlocked         |
| 113008  | AAA successful            |
| 113009  | AAA retrieved             |
| 113010  | AAA Challenge received    |
| 113011  | AAA retrieved             |
| 113012  | Authentication Successful |
| 113013  | AAA error                 |
| 113014  | AAA error                 |
| 113015  | Authentication Rejected   |
| 113016  | AAA Rejected              |
| 113017  | AAA Rejected              |
| 113018  | AAA ACL error             |
| 113019  | AAA Disconnected          |
| 113020  | AAA error                 |

| EventID | EventName                |
|---------|--------------------------|
| 113021  | AAA Logging Fail         |
| 113022  | AAA Failed               |
| 113023  | AAA reactivated          |
| 113024  | AAA Client certification |
| 113025  | AAA Authentication fail  |
| 113026  | AAA error                |
| 113027  | AAA error                |

**Botnet Syslog Event IDs and Event Names**

| EventID | EventName                     |
|---------|-------------------------------|
| 338001  | Botnet Source Block List      |
| 338002  | Botnet Destination Block List |
| 338003  | Botnet Source Block List      |
| 338004  | Botnet Destination Block List |
| 338101  | Botnet Source Allow List      |
| 338102  | Botnet destination Allow List |
| 338202  | Botnet destination Grey       |
| 338203  | Botnet Source Grey            |
| 338204  | Botnet Destination Grey       |
| 338301  | Botnet DNS Intercepted        |
| 338302  | Botnet DNS                    |
| 338303  | Botnet DNS                    |
| 338304  | Botnet Download successful    |
| 338305  | Botnet Download failed        |
| 338306  | Botnet Authentication failed  |
| 338307  | Botnet Decrypt failed         |
| 338308  | Botnet Client                 |
| 338309  | Botnet Client                 |
| 338310  | Botnet dyn filter failed      |

**Failover Syslog Event IDs and Event Names**

| <b>EventID</b> | <b>EventName</b>                   |
|----------------|------------------------------------|
| 101001         | Failover Cable OK                  |
| 101002         | Failover Cable BAD                 |
| 101003         | Failover Cable not connected       |
| 101004         | Failover Cable not connected       |
| 101005         | Failover Cable reading error       |
| 102001         | Failover Power failure             |
| 103001         | No response from failover mate     |
| 103002         | Failover mate interface OK         |
| 103003         | Failover mate interface BAD        |
| 103004         | Failover mate reports failure      |
| 103005         | Failover mate reports self failure |
| 103006         | Failover version incompatible      |
| 103007         | Failover version difference        |
| 104001         | Failover role switch               |
| 104002         | Failover role switch               |
| 104003         | Failover unit failed               |
| 104004         | Failover unit OK                   |
| 106100         | Permit/Denied by ACL               |
| 210001         | Stateful Failover error            |
| 210002         | Stateful Failover error            |
| 210003         | Stateful Failover error            |
| 210005         | Stateful Failover error            |
| 210006         | Stateful Failover error            |
| 210007         | Stateful Failover error            |
| 210008         | Stateful Failover error            |
| 210010         | Stateful Failover error            |
| 210020         | Stateful Failover error            |

| EventID | EventName                             |
|---------|---------------------------------------|
| 210021  | Stateful Failover error               |
| 210022  | Stateful Failover error               |
| 311001  | Stateful Failover update              |
| 311002  | Stateful Failover update              |
| 311003  | Stateful Failover update              |
| 311004  | Stateful Failover update              |
| 418001  | Denied Packet to Management           |
| 709001  | Failover replication error            |
| 709002  | Failover replication error            |
| 709003  | Failover replication start            |
| 709004  | Failover replication complete         |
| 709005  | Failover receive replication start    |
| 709006  | Failover receive replication complete |
| 709007  | Failover replication failure          |
| 710003  | Denied access to Device               |

**Firewall Denied Syslog Event IDs and Event Names**

| EventID | EventName                   |
|---------|-----------------------------|
| 106001  | Denied by Security Policy   |
| 106002  | Outbound Deny               |
| 106006  | Denied by Security Policy   |
| 106007  | Denied Inbound UDP          |
| 106008  | Denied by Security Policy   |
| 106010  | Denied by Security Policy   |
| 106011  | Denied Inbound              |
| 106012  | Denied due to Bad IP option |
| 106013  | Dropped Ping to PAT IP      |
| 106014  | Denied Inbound ICMP         |
| 106015  | Denied by Security Policy   |

| EventID | EventName                               |
|---------|-----------------------------------------|
| 106016  | Denied IP Spoof                         |
| 106017  | Denied due to Land Attack               |
| 106018  | Denied outbound ICMP                    |
| 106020  | Denied IP Packet                        |
| 106021  | Denied TCP                              |
| 106022  | Denied Spoof packet                     |
| 106023  | Denied IP Packet                        |
| 106025  | Dropped Packet failed to Detect context |
| 106026  | Dropped Packet failed to Detect context |
| 106027  | Dropped Packet failed to Detect context |
| 106100  | Permit/Denied by ACL                    |
| 418001  | Denied Packet to Management             |
| 710003  | Denied access to Device                 |

**Firewall Traffic Syslog Event IDs and Event Names**

| EventID | EventName               |
|---------|-------------------------|
| 108001  | Inspect SMTP            |
| 108002  | Inspect SMTP            |
| 108003  | Inspect ESMTP Dropped   |
| 108004  | Inspect ESMTP           |
| 108005  | Inspect ESMTP           |
| 108006  | Inspect ESMTP Violation |
| 108007  | Inspect ESMTP           |
| 110002  | No Router found         |
| 110003  | Failed to Find Next hop |
| 209003  | Fragment Limit Reach    |
| 209004  | Fragment invalid Length |
| 209005  | Fragment IP discard     |
| 302003  | H245 Connection Start   |

| EventID | EventName                |
|---------|--------------------------|
| 302004  | H323 Connection start    |
| 302009  | Restart TCP              |
| 302010  | Connection USAGE         |
| 302012  | H225 CALL SIGNAL CONN    |
| 302013  | Built TCP                |
| 302014  | Teardown TCP             |
| 302015  | Built UDP                |
| 302016  | Teardown UDP             |
| 302017  | Built GRE                |
| 302018  | Teardown GRE             |
| 302019  | H323 Failed              |
| 302020  | Built ICMP               |
| 302021  | Teardown ICMP            |
| 302022  | Built TCP Stub           |
| 302023  | Teardown TCP Stub        |
| 302024  | Built UDP Stub           |
| 302025  | Teardown UDP Stub        |
| 302026  | Built ICMP Stub          |
| 302027  | Teardown ICMP Stub       |
| 302033  | Connection H323          |
| 302034  | H323 Connection Failed   |
| 302035  | Built SCTP               |
| 302036  | Teardown SCTP            |
| 303002  | FTP file download/upload |
| 303003  | Inspect FTP Dropped      |
| 303004  | Inspect FTP Dropped      |
| 303005  | Inspect FTP reset        |
| 313001  | ICMP Denied              |



| EventID | EventName                                |
|---------|------------------------------------------|
| 313004  | ICMP Drop                                |
| 313005  | ICMP Error Msg Drop                      |
| 313008  | ICMP ipv6 Denied                         |
| 324000  | GTP Pkt Drop                             |
| 324001  | GTP Pkt Error                            |
| 324002  | Memory Error                             |
| 324003  | GTP Pkt Drop                             |
| 324004  | GTP Version Not Supported                |
| 324005  | GTP Tunnel Failed                        |
| 324006  | GTP Tunnel Failed                        |
| 324007  | GTP Tunnel Failed                        |
| 337001  | Phone Proxy SRTP Failed                  |
| 337002  | Phone Proxy SRTP Failed                  |
| 337003  | Phone Proxy SRTP Auth Fail               |
| 337004  | Phone Proxy SRTP Auth Fail               |
| 337005  | Phone Proxy SRTP no Media Session        |
| 337006  | Phone Proxy TFTP Unable to Create File   |
| 337007  | Phone Proxy TFTP Unable to Find File     |
| 337008  | Phone Proxy Call Failed                  |
| 337009  | Phone Proxy Unable to Create Phone Entry |
| 400000  | IPS IP options-Bad Option List           |
| 400001  | IPS IP options-Record Packet Route       |
| 400002  | IPS IP options-Timestamp                 |
| 400003  | IPS IP options-Security                  |
| 400004  | IPS IP options-Loose Source Route        |
| 400005  | IPS IP options-SATNET ID                 |
| 400006  | IPS IP options-Strict Source Route       |
| 400007  | IPS IP Fragment Attack                   |

| EventID | EventName                             |
|---------|---------------------------------------|
| 400008  | IPS IP Impossible Packet              |
| 400009  | IPS IP Fragments Overlap              |
| 400010  | IPS ICMP Echo Reply                   |
| 400011  | IPS ICMP Host Unreachable             |
| 400012  | IPS ICMP Source Quench                |
| 400013  | IPS ICMP Redirect                     |
| 400014  | IPS ICMP Echo Request                 |
| 400015  | IPS ICMP Time Exceeded for a Datagram |
| 400017  | IPS ICMP Timestamp Request            |
| 400018  | IPS ICMP Timestamp Reply              |
| 400019  | IPS ICMP Information Request          |
| 400020  | IPS ICMP Information Reply            |
| 400021  | IPS ICMP Address Mask Request         |
| 400022  | IPS ICMP Address Mask Reply           |
| 400023  | IPS Fragmented ICMP Traffic           |
| 400024  | IPS Large ICMP Traffic                |
| 400025  | IPS Ping of Death Attack              |
| 400026  | IPS TCP NULL flags                    |
| 400027  | IPS TCP SYN+FIN flags                 |
| 400028  | IPS TCP FIN only flags                |
| 400029  | IPS FTP Improper Address Specified    |
| 400030  | IPS FTP Improper Port Specified       |
| 400031  | IPS UDP Bomb attack                   |
| 400032  | IPS UDP Snork attack                  |
| 400033  | IPS UDP Chargen DoS attack            |
| 400034  | IPS DNS HINFO Request                 |
| 400035  | IPS DNS Zone Transfer                 |
| 400036  | IPS DNS Zone Transfer from High Port  |

| EventID | EventName                            |
|---------|--------------------------------------|
| 400037  | IPS DNS Request for All Records      |
| 400038  | IPS RPC Port Registration            |
| 400039  | IPS RPC Port Unregistration          |
| 400040  | IPS RPC Dump                         |
| 400041  | IPS Proxied RPC Request              |
| 400042  | IPS YP server Portmap Request        |
| 400043  | IPS YP bind Portmap Request          |
| 400044  | IPS YP password Portmap Request      |
| 400045  | IPS YP update Portmap Request        |
| 400046  | IPS YP transfer Portmap Request      |
| 400047  | IPS Mount Portmap Request            |
| 400048  | IPS Remote execution Portmap Request |
| 400049  | IPS Remote execution Attempt         |
| 400050  | IPS Statd Buffer Overflow            |
| 406001  | Inspect FTP Dropped                  |
| 406002  | Inspect FTP Dropped                  |
| 407001  | Host Limit Reach                     |
| 407002  | Embryonic limit Reached              |
| 407003  | Established limit Reached            |
| 415001  | Inspect Http Header Field Count      |
| 415002  | Inspect Http Header Field Length     |
| 415003  | Inspect Http body Length             |
| 415004  | Inspect Http content-type            |
| 415005  | Inspect Http URL length              |
| 415006  | Inspect Http URL Match               |
| 415007  | Inspect Http Body Match              |
| 415008  | Inspect Http Header match            |
| 415009  | Inspect Http Method match            |

| EventID | EventName                       |
|---------|---------------------------------|
| 415010  | Inspect transfer encode match   |
| 415011  | Inspect Http Protocol Violation |
| 415012  | Inspect Http Content-type       |
| 415013  | Inspect Http Malformed          |
| 415014  | Inspect Http Mime-Type          |
| 415015  | Inspect Http Transfer-encoding  |
| 415016  | Inspect Http Unanswered         |
| 415017  | Inspect Http Argument match     |
| 415018  | Inspect Http Header length      |
| 415019  | Inspect Http status Matched     |
| 415020  | Inspect Http non-ASCII          |
| 416001  | Inspect SNMP dropped            |
| 419001  | Dropped packet                  |
| 419002  | Duplicate TCP SYN               |
| 419003  | Packet modified                 |
| 424001  | Denied Packet                   |
| 424002  | Dropped Packet                  |
| 431001  | Dropped RTP                     |
| 431002  | Dropped RTCP                    |
| 500001  | Inspect ActiveX                 |
| 500002  | Inspect Java                    |
| 500003  | Inspect TCP Header              |
| 500004  | Inspect TCP Header              |
| 500005  | Inspect Connection Terminated   |
| 508001  | Inspect DCERPC Dropped          |
| 508002  | Inspect DCERPC Dropped          |
| 509001  | Prevented No Forward Cmd        |
| 607001  | Inspect SIP                     |

| EventID | EventName                |
|---------|--------------------------|
| 607002  | Inspect SIP              |
| 607003  | Inspect SIP              |
| 608001  | Inspect Skinny           |
| 608002  | Inspect Skinny dropped   |
| 608003  | Inspect Skinny dropped   |
| 608004  | Inspect Skinny dropped   |
| 608005  | Inspect Skinny dropped   |
| 609001  | Built Local-Host         |
| 609002  | Teardown Local Host      |
| 703001  | H225 Unsupported Version |
| 703002  | H225 Connection          |
| 726001  | Inspect Instant Message  |

#### Identity Based Firewall Syslog Event IDs and Event Names

| EventID | EventName               |
|---------|-------------------------|
| 746001  | Import started          |
| 746002  | Import complete         |
| 746003  | Import failed           |
| 746004  | Exceed user group limit |
| 746005  | AD Agent down           |
| 746006  | AD Agent out of sync    |
| 746007  | Netbios response failed |
| 746008  | Netbios started         |
| 746009  | Netbios stopped         |
| 746010  | Import user failed      |
| 746011  | Exceed user limit       |
| 746012  | User IP add             |
| 746013  | User IP delete          |
| 746014  | FQDN Obsolete           |

| EventID | EventName              |
|---------|------------------------|
| 746015  | FQDN resolved          |
| 746016  | DNS lookup failed      |
| 746017  | Import user issued     |
| 746018  | Import user done       |
| 746019  | Update AD Agent failed |

**IPSec Syslog Event IDs and Event Names**

| EventID | EventName                               |
|---------|-----------------------------------------|
| 402114  | Invalid SPI received                    |
| 402115  | Unexpected protocol received            |
| 402116  | Packet doesn't match identity           |
| 402117  | Non-IPSEC packet received               |
| 402118  | Invalid fragment offset                 |
| 402119  | Anti-Replay check failure               |
| 402120  | Authentication failure                  |
| 402121  | Packet dropped                          |
| 426101  | cLACP Port Bundle                       |
| 426102  | cLACP Port Standby                      |
| 426103  | cLACP Port Moved To Bundle From Standby |
| 426104  | cLACP Port Unbundled                    |
| 602103  | Path MTU updated                        |
| 602104  | Path MTU exceeded                       |
| 602303  | New SA created                          |
| 602304  | SA deleted                              |
| 702305  | SA expiration - Sequence rollover       |
| 702307  | SA expiration - Data rollover           |

**NAT Syslog Event ID and Event Names**

| EventID | EventName                        |
|---------|----------------------------------|
| 201002  | Max connection Exceeded for host |
| 201003  | Embryonic limit exceed           |
| 201004  | UDP connection limit exceed      |

| EventID | EventName                                      |
|---------|------------------------------------------------|
| 201005  | FTP connection failed                          |
| 201006  | RCMD connection failed                         |
| 201008  | New connection Disallowed                      |
| 201009  | Connection Limit exceed                        |
| 201010  | Embryonic Connection limit exceeded            |
| 201011  | Connection Limit exceeded                      |
| 201012  | Per-client embryonic connection limit exceeded |
| 201013  | Per-client connection limit exceeded           |
| 202001  | Global NAT exhausted                           |
| 202005  | Embryonic connection error                     |
| 202011  | Connection limit exceeded                      |
| 305005  | No NAT group found                             |
| 305006  | Translation failed                             |
| 305007  | Connection dropped                             |
| 305008  | NAT allocation issue                           |
| 305009  | NAT Created                                    |
| 305010  | NAT teardown                                   |
| 305011  | PAT created                                    |
| 305012  | PAT teardown                                   |
| 305013  | Connection denied                              |

**SSL VPN Syslog Event IDs and Event Names**

| EventID | EventName                     |
|---------|-------------------------------|
| 716001  | WebVPN Session Started        |
| 716002  | WebVPN Session Terminated     |
| 716003  | WebVPN User URL access        |
| 716004  | WebVPN User URL access denied |
| 716005  | WebVPN ACL error              |
| 716006  | WebVPN User Disabled          |
| 716007  | WebVPN Unable to Create       |
| 716008  | WebVPN Debug                  |
| 716009  | WebVPN ACL error              |
| 716010  | WebVPN User access network    |

| EventID | EventName                             |
|---------|---------------------------------------|
| 716011  | WebVPN User access                    |
| 716012  | WebVPN User Directory access          |
| 716013  | WebVPN User file access               |
| 716014  | WebVPN User file access               |
| 716015  | WebVPN User file access               |
| 716016  | WebVPN User file access               |
| 716017  | WebVPN User file access               |
| 716018  | WebVPN User file access               |
| 716019  | WebVPN User file access               |
| 716020  | WebVPN User file access               |
| 716021  | WebVPN user access file denied        |
| 716022  | WebVPN Unable to connect proxy        |
| 716023  | WebVPN session limit reached          |
| 716024  | WebVPN User access error              |
| 716025  | WebVPN User access error              |
| 716026  | WebVPN User access error              |
| 716027  | WebVPN User access error              |
| 716028  | WebVPN User access error              |
| 716029  | WebVPN User access error              |
| 716030  | WebVPN User access error              |
| 716031  | WebVPN User access error              |
| 716032  | WebVPN User access error              |
| 716033  | WebVPN User access error              |
| 716034  | WebVPN User access error              |
| 716035  | WebVPN User access error              |
| 716036  | WebVPN User login successful          |
| 716037  | WebVPN User login failed              |
| 716038  | WebVPN User Authentication Successful |
| 716039  | WebVPN User Authentication Rejected   |
| 716040  | WebVPN User logging denied            |
| 716041  | WebVPN ACL hit count                  |
| 716042  | WebVPN ACL hit                        |



| EventID | EventName                        |
|---------|----------------------------------|
| 716043  | WebVPN Port forwarding           |
| 716044  | WebVPN Bad Parameter             |
| 716045  | WebVPN Invalid Parameter         |
| 716046  | WebVPN connection terminated     |
| 716047  | WebVPN ACL usage                 |
| 716048  | WebVPN memory issue              |
| 716049  | WebVPN Empty SVC ACL             |
| 716050  | WebVPN ACL error                 |
| 716051  | WebVPN ACL error                 |
| 716052  | WebVPN Session Terminated        |
| 716053  | WebVPN SSO Server added          |
| 716054  | WebVPN SSO Server deleted        |
| 716055  | WebVPN Authentication Successful |
| 716056  | WebVPN Authentication Failed     |
| 716057  | WebVPN Session terminated        |
| 716058  | WebVPN Session lost              |
| 716059  | WebVPN Session resumed           |
| 716060  | WebVPN Session Terminated        |
| 722001  | WebVPN SVC Connect request error |
| 722002  | WebVPN SVC Connect request error |
| 722003  | WebVPN SVC Connect request error |
| 722004  | WebVPN SVC Connect request error |
| 722005  | WebVPN SVC Connect update issue  |
| 722006  | WebVPN SVC Invalid address       |
| 722007  | WebVPN SVC Message               |
| 722008  | WebVPN SVC Message               |
| 722009  | WebVPN SVC Message               |
| 722010  | WebVPN SVC Message               |
| 722011  | WebVPN SVC Message               |
| 722012  | WebVPN SVC Message               |
| 722013  | WebVPN SVC Message               |
| 722014  | WebVPN SVC Message               |

| EventID | EventName                         |
|---------|-----------------------------------|
| 722015  | WebVPN SVC invalid frame          |
| 722016  | WebVPN SVC invalid frame          |
| 722017  | WebVPN SVC invalid frame          |
| 722018  | WebVPN SVC invalid frame          |
| 722019  | WebVPN SVC Not Enough Data        |
| 722020  | WebVPN SVC no address             |
| 722021  | WebVPN Memory issue               |
| 722022  | WebVPN SVC connection established |
| 722023  | WebVPN SVC connection terminated  |
| 722024  | WebVPN Compression Enabled        |
| 722025  | WebVPN Compression Disabled       |
| 722026  | WebVPN Compression reset          |
| 722027  | WebVPN Decompression reset        |
| 722028  | WebVPN Connection Closed          |
| 722029  | WebVPN SVC Session terminated     |
| 722030  | WebVPN SVC Session terminated     |
| 722031  | WebVPN SVC Session terminated     |
| 722032  | WebVPN SVC connection Replacement |
| 722033  | WebVPN SVC Connection established |
| 722034  | WebVPN SVC New connection         |
| 722035  | WebVPN Received Large packet      |
| 722036  | WebVPN transmitting Large packet  |
| 722037  | WebVPN SVC connection closed      |
| 722038  | WebVPN SVC session terminated     |
| 722039  | WebVPN SVC invalid ACL            |
| 722040  | WebVPN SVC invalid ACL            |
| 722041  | WebVPN SVC IPv6 not available     |
| 722042  | WebVPN invalid protocol           |
| 722043  | WebVPN DTLS disabled              |
| 722044  | WebVPN unable to request address  |
| 722045  | WebVPN Connection terminated      |
| 722046  | WebVPN Session terminated         |

| EventID | EventName                            |
|---------|--------------------------------------|
| 722047  | WebVPN Tunnel terminated             |
| 722048  | WebVPN Tunnel terminated             |
| 722049  | WebVPN Session terminated            |
| 722050  | WebVPN Session terminated            |
| 722051  | WebVPN address assigned              |
| 722053  | WebVPN Unknown client                |
| 723001  | WebVPN Citrix connection Up          |
| 723002  | WebVPN Citrix connection Down        |
| 723003  | WebVPN Citrix no memory issue        |
| 723004  | WebVPN Citrix bad flow control       |
| 723005  | WebVPN Citrix no channel             |
| 723006  | WebVPN Citrix SOCKS error            |
| 723007  | WebVPN Citrix connection list broken |
| 723008  | WebVPN Citrix invalid SOCKS          |
| 723009  | WebVPN Citrix invalid connection     |
| 723010  | WebVPN Citrix invalid connection     |
| 723011  | WebVPN citrix Bad SOCKS              |
| 723012  | WebVPN Citrix Bad SOCKS              |
| 723013  | WebVPN Citrix invalid connection     |
| 723014  | WebVPN Citrix connected to Server    |
| 724001  | WebVPN Session not allowed           |
| 724002  | WebVPN Session terminated            |
| 724003  | WebVPN CSD                           |
| 724004  | WebVPN CSD                           |
| 725001  | SSL handshake Started                |
| 725002  | SSL Handshake completed              |
| 725003  | SSL Client session resume            |
| 725004  | SSL Client request Authentication    |
| 725005  | SSL Server request authentication    |
| 725006  | SSL Handshake failed                 |
| 725007  | SSL Session terminated               |
| 725008  | SSL Client Cipher                    |

## Time Attributes in a Syslog Event

| EventID | EventName                     |
|---------|-------------------------------|
| 725009  | SSL Server Cipher             |
| 725010  | SSL Cipher                    |
| 725011  | SSL Device choose Cipher      |
| 725012  | SSL Device choose Cipher      |
| 725013  | SSL Server choose cipher      |
| 725014  | SSL LIB error                 |
| 725015  | SSL client certificate failed |

## Time Attributes in a Syslog Event

Understanding the purposes of the different time-stamps in the Event Logging page will help you filter and find the events that interest you.

| Historical |                          | Live                                             |                                                                  |               |                   |                          |                          |                      |                                                  |                            |
|------------|--------------------------|--------------------------------------------------|------------------------------------------------------------------|---------------|-------------------|--------------------------|--------------------------|----------------------|--------------------------------------------------|----------------------------|
|            |                          |                                                  | Initiator                                                        |               | Responder         |                          |                          |                      |                                                  |                            |
| 1          | Date/Time                | Event Type                                       | Sensor ID                                                        | IP            | IP                | Port                     | Protocol                 | Action               | Policy                                           |                            |
|            | Aug 20, 2019 10:44:14 AM | Malware                                          | 192.168.20.53                                                    |               |                   | 80                       | tcp                      | Cloud Lookup Timeout | BlockOfficeDocumentsPDFUpload_BlockMalwareOthers |                            |
| 2          | Application              | HTTP                                             |                                                                  | FileSize      |                   | 68                       |                          | SensorID             | 192.168.20.53                                    |                            |
|            | ClientApplication        | Web browser                                      |                                                                  | FileType      |                   | EICAR                    |                          | SHA_Disposition      | Unavailable                                      |                            |
|            | EventSecond              | 1566312254                                       |                                                                  | 3             | FirstPacketSecond | Aug 20, 2019 10:44:08 AM |                          | SperoDisposition     | Spero detection not performed on file            |                            |
|            | EventType                | MalwareEvent                                     |                                                                  |               |                   |                          |                          |                      | Unknown                                          |                            |
|            | FileAction               | Cloud Lookup Timeout                             |                                                                  |               | InitiatorIP       |                          |                          | 5                    | ThreatName                                       |                            |
|            | FileDirection            | Download                                         |                                                                  |               | InitiatorPort     | 65386                    |                          | timestamp            | Aug 20, 2019 10:44:14 AM                         |                            |
|            | FileName                 | eicar.com                                        |                                                                  |               | 4                 | LastPacketSecond         | Aug 20, 2019 10:44:14 AM |                      |                                                  |                            |
|            | FilePolicy               | BlockOfficeDocumentsPDFUpload_BlockMalwareOthers |                                                                  |               |                   |                          |                          |                      | URI                                              | /eicar.com                 |
|            |                          |                                                  |                                                                  |               | Protocol          | tcp                      |                          |                      | UserName                                         | No Authentication Required |
|            |                          | FileSHA256                                       | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aafb651fd0f |               | ResponderIP       |                          |                          |                      |                                                  |                            |
|            |                          |                                                  |                                                                  | ResponderPort | 80                |                          |                          |                      |                                                  |                            |

| Date/Time                | Device Type                                                                                                                                               | Event Type          | Sensor ID    | Initiator IP  | Responder IP    | Port                          | Protocol | Action | Policy |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------|---------------|-----------------|-------------------------------|----------|--------|--------|
| Jun 12, 2020, 7:27:02 AM | ASA                                                                                                                                                       | 302013              | admin        | 192.168.25.4  | 192.168.0.68    | 443                           | TCP      | Built  |        |
| Action                   | Built                                                                                                                                                     | Event Type          | 302013       | Protocol      | TCP             |                               |          |        |        |
| ConnectionID             | 1169028                                                                                                                                                   | IngressInterface    | management   | ResponderIP   | 192.168.0.68    |                               |          |        |        |
| DeviceType               | ASA                                                                                                                                                       | InitiatorIP         | 192.168.25.4 | ResponderPort | 443             |                               |          |        |        |
| Direction                | inbound                                                                                                                                                   | InitiatorPort       | 36540        | SensorID      | admin           |                               |          |        |        |
| EgressInterface          | identity                                                                                                                                                  | MappedInitiatorIP   | 192.168.25.4 | Severity      | Informational   |                               |          |        |        |
| EventGroup               | session                                                                                                                                                   | MappedInitiatorPort | 36540        | 6             | SyslogTimestamp | 2020-06-12 11:15:26 +0000 UTC |          |        |        |
| EventGroupDefinition     | User Session                                                                                                                                              | MappedResponderIP   | 192.168.0.68 |               | timestamp       | Jun 12, 2020, 7:27:02 AM      |          |        |        |
| EventName                | Built TCP                                                                                                                                                 | MappedResponderPort | 443          |               |                 |                               |          |        |        |
| Message                  | ASA-6-302013: Built inbound TCP connection 1169028 for management:192.168.25.4/36540 (192.168.25.4/36540) to identity:192.168.0.68/443 (192.168.0.68/443) |                     |              |               |                 |                               |          |        |        |

| Date/Time                | Device Type              | Event Type          | Sensor ID                | Initiator IP     | Responder IP             | Port | Protocol | Action | Policy |
|--------------------------|--------------------------|---------------------|--------------------------|------------------|--------------------------|------|----------|--------|--------|
| Jun 12, 2020, 7:27:13 AM | ASA                      | 5                   | 192.168.0.169            | 192.168.25.4     | 192.168.0.169            | 443  | TCP      | Update |        |
| Action                   | Update                   | InitiatorBytes      | 0                        | Protocol         | TCP                      |      |          |        |        |
| ConnectionID             | 482168                   | InitiatorIP         | 192.168.25.4             | ResponderBytes   | 3581                     |      |          |        |        |
| DeviceType               | ASA                      | InitiatorPackets    | 0                        | ResponderIP      | 192.168.0.169            |      |          |        |        |
| EgressInterface          | 65535                    | InitiatorPort       | 38068                    | ResponderPackets | 33                       |      |          |        |        |
| EventType                | 5                        | LastPacketSecond    | Jun 12, 2020, 7:27:07 AM | ResponderPort    | 443                      |      |          |        |        |
| FirewallExtendedEvent    | 2034                     | MappedInitiatorIP   | 192.168.25.4             | SensorID         | 192.168.0.169            |      |          |        |        |
| FirstPacketSecond        | Jun 12, 2020, 7:27:07 AM | MappedInitiatorPort | 38068                    | Severity         | Informational            |      |          |        |        |
| ICMPCode                 | 0                        | MappedResponderIP   | 192.168.0.169            | timestamp        | Jun 12, 2020, 7:27:13 AM |      |          |        |        |
| ICMPType                 | 0                        | MappedResponderPort | 443                      |                  |                          |      |          |        |        |
| IngressInterface         | 9                        | 7                   | NetFlowTimestamp         | 1591961232       |                          |      |          |        |        |

| Number | Label             | Description                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | Date/Time         | The time the Secure Event Connector (SEC) processed the event. This may not be the same as the time the firewall inspected that traffic. Same value as timestamp.                                                                                                                                                                                                                       |
| 2      | EventSecond       | Equals with LastPacketSecond.                                                                                                                                                                                                                                                                                                                                                           |
| 3      | FirstPacketSecond | <p>The time at which the connection opened. The firewall inspects the packet at this time.</p> <p>The value of the FirstPacketSecond is calculated by subtracting the ConnectionDuration from the LastPacketSecond.</p> <p>For connection events logged at the beginning of the connection, the value of FirstPacketSecond, LastPacketSecond, and EventSecond will all be the same.</p> |
| 4      | LastPacketSecond  | The time at which the connection closed. For connection events logged at the end of the connection, LastPacketSecond and EventSecond will be equal.                                                                                                                                                                                                                                     |
| 5      | timestamp         | The time the Secure Event Connector (SEC) processed the event. This may not be the same as the time the firewall inspected that traffic. Same value as Date/Time.                                                                                                                                                                                                                       |
| 6      | Syslog TimeStamp  | Represents the syslog originated time if 'logging timestamp' is used. If the syslog does not have this info, the time the SEC received the event is reflected.                                                                                                                                                                                                                          |
| 7      | NetflowTimeStamp  | The time at which the ASA finished gathering enough flow records/events to fill a NetFlow packet to then send them off to a flow collector.                                                                                                                                                                                                                                             |

## Cisco Secure Cloud Analytics and Dynamic Entity Modeling

Required License: Logging Analytics and Detection or Total Network Analytics and Monitoring

Secure Cloud Analytics is a software as a service (SaaS) solution that monitors your on-premises and cloud-based network deployments. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

### Dynamic Entity Modeling

Dynamic entity modeling tracks the state of your network by performing a behavioral analysis on firewall events and network flow data. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they take on your network. Secure Cloud Analytics, integrated with a **Logging Analytics and Detection** license, can draw from firewall events and other traffic information in order to determine the types of traffic the entity usually transmits. If you purchase a **Total Network Analytics and Monitoring** license, Secure Cloud Analytics can also include NetFlow and other traffic information in modeling entity traffic. Secure Cloud Analytics updates these models over time, as the entities continue to send traffic, and potentially send different traffic, to keep an up-to-date model of each entity. From this information, Secure Cloud Analytics identifies:

- Roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- Observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, or a remote access session established with another entity. If you integrate with CDO, these facts can be obtained from firewall events. If you also purchase a **Total Network Analytics and Monitoring** license, the system can also obtain facts from NetFlow, and generate observations from both firewall events and NetFlow. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

### Alerts and Analysis

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system. Note that one alert may represent multiple observations. If a firewall logs multiple connection events related to the same connection and entities, this may result in only one alert.

For example, a New Internal Device observation on its own does not constitute possible malicious behavior. However, over time, if the entity transmits traffic consistent with a Domain Controller, then the system assigns a Domain Controller role to the entity. If the entity subsequently establishes a connection to an external server that it has not established a connection with previously, using unusual ports, and transfers large amounts of data, the system would log a New Large Connection (External) observation and an Exceptional Domain Controller observation. If that external server is identified as on a Talos watchlist, then the combination of all this information would lead Secure Cloud Analytics to generate an alert for this entity's behavior, prompting you to take further action to research, and remediate malicious behavior.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about

the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available. You can also see other observations and alerts that entities were involved with, and determine if this behavior is tied to other potentially malicious behavior.

Note that when you view and close alerts in Secure Cloud Analytics, you cannot allow or block traffic from the Secure Cloud Analytics UI. You must update your firewall access control rules to allow or block traffic, if you deployed your devices in active mode, or your firewall access control rules if your firewalls are deployed in passive mode.

## Working with Alerts Based on Firewall Events

**Required License:** **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

### Alerts Workflow

An alert's workflow is based around its status. When the system generates an alert, the default status is Open, and no user is assigned. When you view the Alerts summary, all open alerts are displayed by default, as these are of immediate concern.

Note: If you have a **Total Network Analytics and Monitoring** license, your alerts can be based on observations generated from NetFlow, observations generated from firewall events, or observations from both data sources.

As you review the Alerts summary, you can assign, tag, and update status on alerts as an initial triage. You can use the filters and search functionality to locate specific alerts, or display alerts of different statuses, or associated with different tags or assignees. You can set an alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove Snoozed status from an alert, to display it as an open alert again. As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

From the Alerts summary, you can view an alert detail page. This page allows you to review additional context about the supporting observations that resulted in this alert, and additional context about the entities involved in this alert. This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior.

As you research within the Secure Cloud Analytics web portal UI, in CDO, and on your network, you can leave comments with the alert that describe your findings. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to Closed, and have it no longer appear by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

The following presents general guidelines and suggestions for how to investigate a given alert. Because Secure Cloud Analytics provides additional context when it logs an alert, you can use this context to help guide your investigation.

These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

In general, you can take the following steps when you review an alert:

1. [Triage open alerts, on page 51](#)
2. [Snooze alerts for later analysis, on page 51](#)
3. [Update the alert for further investigation, on page 52](#)
4. [Review the alert and start your investigation, on page 52](#)

5. [Examine the entity and users, on page 54](#)
6. [Remediate issues using Secure Cloud Analytics, on page 54](#)
7. [Update and close the alert, on page 55](#)

## Triage open alerts

Triage the open alerts, especially if more than one have yet to be investigated:

- See [Viewing Cisco Secure Cloud Analytics Alerts from CDO](#) for more information on cross-launching from CDO to Secure Cloud Analytics, and viewing alerts.

Ask the following questions:

- Have you configured this alert type as high priority?
- Did you set a high sensitivity for the affected subnet?
- Is this unusual behavior from a new entity on your network?
- What is the entity's normal role, and how does the behavior in this alert fit that role?
- Is this an exceptional deviation from normal behavior for this entity?
- If a user is involved, is this expected behavior from the user, or exceptional?
- Is protected or sensitive data at risk of being compromised?
- How severe is the impact to your network if this behavior is allowed to continue?
- If there is communication with external entities, have these entities established connections with other entities on your network in the past?

If this is a *high* priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

## Snooze alerts for later analysis

Snooze alerts when they are of lesser priority, as compared to other alerts. For example, if your organization is repurposing an email server as an FTP server, and the system generates an Emergent Profile alert (indicating that an entity's current traffic matches a behavior profile that it did not previously match), you can snooze this alert as it is intended behavior, and revisit it at a later date. A snoozed alert does not show up with the open alerts; you must specifically filter to review these snoozed alerts.

Snooze an alert:

### Procedure

- 
- |               |                                                                           |
|---------------|---------------------------------------------------------------------------|
| <b>Step 1</b> | Click <b>Close Alert</b> .                                                |
| <b>Step 2</b> | In the Snooze this alert pane, select a snooze period from the drop-down. |
| <b>Step 3</b> | Click <b>Save</b> .                                                       |
-



### What to do next

When you are ready to review these alerts, you can unsnooze them. This sets the status to Open, and displays the alert alongside the other Open alerts.

Unsnuzzle a snoozed alert:

- From a snoozed alert, click **Unsnuzzle Alert**.

## Update the alert for further investigation

Open the alert detail:

### Procedure

- 
- |               |                                     |
|---------------|-------------------------------------|
| <b>Step 1</b> | Select <b>Monitor &gt; Alerts</b> . |
| <b>Step 2</b> | Click an alert type name.           |
- 

### What to do next

Based on your initial triage and prioritization, assign the alert and tag it:

1. Select a user from the **Assignee** drop-down to assign the alert, so a user can start investigating.
2. Select one or more **Tags** from the drop-down to add tags to the alert, to better categorize your alert's for future identification, as well as to try and establish long-term patterns in your alerts.
3. Enter a **Comment on this alert**, then click **Comment** to leave comments as necessary to track your initial findings, and assist the person assigned to the alert. The alert tracks both system comments and user comments.

## Review the alert and start your investigation

If you are reviewing an assigned alert, review the alert detail to understand why Secure Cloud Analytics generated an alert. Review the supporting observations to understand what these observations mean for the source entity.

Note that if the alert was generated based on firewall events, the system does not note that your firewall deployment was the source of this alert.

View all of the supporting observations for this source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend:

### Procedure

- 
- |               |                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the alert detail, click the arrow icon (➡) next to an observation type to view all logged observations of that type. |
|---------------|---------------------------------------------------------------------------------------------------------------------------|

- Step 2** Click the arrow icon (➡) next to **All Observations for Network** to view all logged observations for this alert's source entity.

---

Download the supporting observations in a comma-separated value file, if you want to perform additional analysis on these observations:

- From the alert detail, in the Supporting Observations pane, click **CSV**.

From the observations, determine if the source entity behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.

View additional context surrounding the source entity from a source entity IP address or hostname, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting:

- Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
- Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
- Select **Device** from the IP address or hostname drop-down to view information about the device.
- Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that the source entity in Secure Cloud Analytics is always internal to your network. Contrast this with the Initiator IP in a firewall event, which indicates the entity that initiated a connection, and may be internal or external to your network.

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.

Review the context for an external entity IP address or hostname with which the source entity established a connection:

- Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
- Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
- Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
- Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
- Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.

- Select **Talos Intelligence** from the IP address or hostname drop-down to view information about this information on Talos's website.
- Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
- Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
- Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.

Note that connected entities in Secure Cloud Analytics are always external to your network. Contrast this with the Responder IP in a firewall event, which indicates the entity that responded to a connection request, and may be internal or external to your network.

Leave comments as to your findings.

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

## Examine the entity and users

After you review the alert in the Secure Cloud Analytics portal UI, you can perform an additional examination on a source entity directly, any users that may have been involved with this alert, and other related entities.

- Determine where the source entity is on your network, physically or in the cloud, and access it directly. Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.
- Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.
- Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.

Leave comments as to your findings:

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

## Update and close the alert

Add additional tags based on your findings:

### Procedure

- 
- |               |                                                                              |
|---------------|------------------------------------------------------------------------------|
| <b>Step 1</b> | In the Secure Cloud Analytics portal UI, select <b>Monitor &gt; Alerts</b> . |
| <b>Step 2</b> | Select one or more <b>Tags</b> from the drop-down.                           |
- 

Add final comments describing the results of your investigation, and any remediation steps taken:

- From an alert's detail, enter a **Comment on this alert**, then click **Comment**.

Close the alert, and mark it as helpful or not helpful:

1. From an alert's detail, click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. Note that this does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. Click **Save**.

### What to do next

#### Reopen a closed alert

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can then make changes as necessary to the alert, then close it again when your additional investigation is complete.

Reopen a closed alert:

- From a closed alert's detail, click **Reopen Alert**.

## Modifying Alert Priorities

**Required License:** **Logging Analytics and Detection** or **Total Network Analytics and Monitoring**

Alert types come with default priorities, which affect how sensitive the system is to generating alerts of this type. Alerts default to *low* or *normal* priority, based on Cisco intelligence and other factors. Based on your network environment, you may want to reprioritize alert types, to emphasize certain alerts that you are concerned with. You can configure any alert type to be *low*, *normal*, or *high* priority.

- Select **Monitor > Alerts**.
- Click the settings drop-down icon (⚙️), then select **Alert Types and Priorities**.
- Click the edit icon (✎️) next to an alert type and select *low*, *medium*, or *high* to change the priority.

## Searching for and Filtering Events in the Event Logging Page

Searching and filtering the historical and live event tables for specific events, works the same way as it does when searching and filtering for other information in CDO. As you add filter criteria, CDO starts to limit what it displays on the Events page. You can also enter search criteria in the search field to find events with specific values. If you combine the filtering and searching mechanisms, search tries to find the value you entered from among the results displayed after filtering the events.

Following are the options to conduct a search for event logs:

- [Search for Events in the Events Logging Page, on page 99](#)
- [Search Historical Events in the Background, on page 99](#)

Filtering works the same way for Live events as it does for Historical events with the exception that live events cannot be filtered by time.



Learn about these filtering methods:

- [Filter Live or Historical Events, on page 93](#)
- [Filter Only NetFlow Events, on page 94](#)
- [Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events, on page 95](#)
- [Combine Filter Elements, on page 95](#)

## Filter Live or Historical Events

This procedure explains how to use event filtering to see a subset of events in the Event Logging page. If you find yourself repeatedly using certain filter criteria, you can create a customized filter and save it. See [Customizable Event Filters](#) for more information.

### Procedure

- Step 1** In the navigation bar, choose **Analytics > Event Logging**
- Step 2** Click either the Historical or Live tab.
- Step 3** Click the filter button . The filtering column can be pinned open by clicking the pin icon .
- Step 4** Click a View tab that has no saved filter elements.



- Step 5** Select the event details you want to filter by:
- **FTD Events**
    - Connection - Displays connection events from access control rules.
    - File - Displays events reported by file policies in access control rules.
    - Intrusion - Displays events reported by intrusion policy in access control rules.
    - Malware - Displays events reported by malware policies in access control rules.
  - **ASA Events** - These event types represent groups of syslog or NetFlow events.  
See [Event Types in CDO](#) for more information about events.
  - **Time Range**-Click the Start or End time fields to select the beginning and end of the time period you want to display. The time stamp is displayed in the local time of your computer.
  - **Action**- Specifies the security action defined by the rule. The value you enter must be an exact match to what you want to find; however, the case doesn't matter. Enter different values for connection, file, intrusion, malware, syslog, and NetFlow event types:
    - For connection event types, the filter searches for matches in the AC\_RuleAction attribute. Those values could be Allow, Block, Trust.
    - For file event types, the filter searches for matches in the FileAction attribute. Those values could be Allow, Block, Trust.

- For intrusion event types, the filter searches for matches in the InLineResult attribute. Those values could be Allowed, Blocked, Trusted.
- For malware event types, the filter searches for matches in the FileAction attribute. Those values could be Cloud Lookup Timeout.
- For syslog and NetFlow events types, the filter searches for matches in the Action attribute.
- **Sensor ID**-The Sensor ID is the the Management IP address from which events are sent to the Secure Event Connector.

For an FDM-managed device, the Sensor ID is typically the IP address of the device's management interface.

- **IP addresses**

- **Initiator** -This is the IP address of the source of the network traffic. The value of the Initiator address field corresponds to the value of the InitiatorIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.
- **Responder**-This is the destination IP address of the packet. The value of the Destination address field corresponds to the value in the ResponderIP field in the event details. You can enter a single address, such as 10.10.10.100, or a network defined in CIDR notation such as 10.10.10.0/24.

- **Ports**

- **Initiator**-The port or ICMP type used by the session initiator. The value of the source port corresponds to the value fo the InitiatorPort in the event details. (Add a range - starting port ending port and space in between or both initiator and responder)
- **Responder**-The port or ICMP code used by the session responder. The value of the destination port corresponds to the value of the ResponderPort in the event details.


**Step 6** (Optional) Save your filter as a custom filter by clicking out of the View tab.

## Filter Only NetFlow Events

This procedure finds only ASA NetFlow events:

### Procedure

**Step 1** From the CDO menu bar, choose **Analytics > Event Logging**.

**Step 2** Click the Filter icon  and pin the filter open.

**Step 3** Check **Netflow** ASA Event filter.


**Step 4** Clear all other ASA Event filters.

Only ASA NetFlow events are displayed in the Event Logging table.

## Filter for ASA or FDM-Managed Device Syslog Events but not ASA NetFlow Events

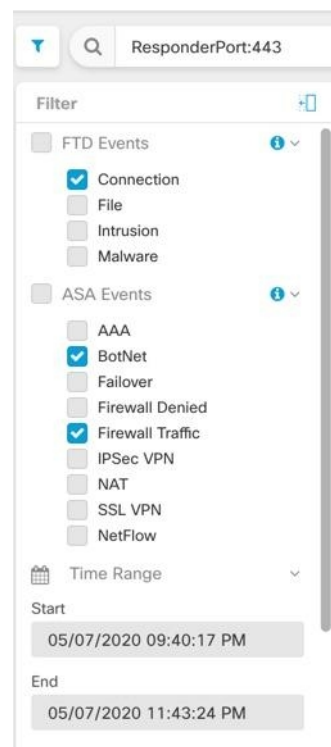
This procedure finds only syslog events:

### Procedure

- Step 1** From the CDO menu bar, choose **Analytics > Event Logging**.
- Step 2** Click the Filter icon  and pin the filter open.
- Step 3** Scroll to the bottom of the filter bar and make sure the **Include NetFlow Events** filter is **unchecked**.
- Step 4** Scroll back up to the ASA Events filter tree, and make sure the **NetFlow** box is **unchecked**.
- Step 5** Pick the rest of your ASA or FTD filter criteria.

## Combine Filter Elements

Filtering events generally follows the standard filtering rules in CDO: The filtering categories are "AND-ed" and the values within the categories are "OR-ed." You can also combine the filter with your own search criteria. In the case of event filters; however, the device event filters are also "OR-ed." For example, if these values were chosen in the filter:



With this filter in use, CDO would display threat defense device connection events **or** ASA BotNet **or** Firewall Traffic events, **and** those events that occurred between the two times in the time range, **and** those events that

also contain the ResponderPort 443. You can filter by historical events within a time range. The live events page always displays the most recent events.

### Search for Specific Attribute: Value Pairs

You can search for live or historical events by entering an event attribute and a value in the search field. The easiest way to do this is to click the attribute in the Event Logging table that you want to search for, and CDO enters it in the Search field. The events you can click on will be blue when you roll over them. Here is an example:

**Event Logging**

Historical Live InitiatorIP: "10.10.11.11" AND EventType: "3"

Clear Time Range After 05/03/2023 07:23:40 PM

+ Views View 1

| Date/Time               | Device Type | Event Type | Sensor ID / Hostname | Initiator IP |
|-------------------------|-------------|------------|----------------------|--------------|
| May 3, 2023, 7:23:40 PM | ASA         | 3          |                      |              |

**Action** [Deny](#)

**ConnectorID** [08c0a888-b619-4f1a-a655-d4bd005dd8c8](#)

**DeviceType** [ASA](#)

**EgressInterface** [4](#)

**EventType** [3](#)

**FirewallExtendedEvent** [1001](#)

**ICMPCode** [0](#)

**ICMPType** [0](#)

**IngressACLID**

**IngressInterface**

**InitiatorIP**

**InitiatorPort**

**LastPacketSecond**

**MappedInitiatorIP**

**MappedInitiatorPort**

**MappedResponderIP**

In this example, the search started by rolling over the InitiatorIP value of 10.10.11.11 and clicking it. Initiator IP and its value were added to the search string. Next, Event Type, 3 was rolled-over and clicked and added to the search string and an AND was added by CDO. So the result of this search will be a list of events that were initiated from 10.10.11.11 AND that are 3 event types.

Notice the magnifying glass next to the value 3 in the example above. If you roll-over the magnifying glass, you could also choose an AND, OR, AND NOT, OR NOT operator to go with the value you want to add to the search.



In the example below, "OR" is chosen. The result of this search will be a list of events that were initiated from 10.10.11.11 OR are a 106023 event type. Note that if the search field is empty and you right click a value from the table, only NOT is available as there is no other value.

**Event Logging**

Historical Live InitiatorIP: "10.10.11.11" AND EventType: "3"

Clear Time Range After 05/03/2023 07:23:40 PM

+ Views View 1

| Date/Time               | Device Type | Event Type | Sensor ID / Hostname | Initiator IP |
|-------------------------|-------------|------------|----------------------|--------------|
| May 3, 2023, 7:23:40 PM | ASA         | 3          |                      |              |

|                       |                            |                     |
|-----------------------|----------------------------|---------------------|
| Action                | Deny                       | IngressACLID        |
| ConnectorID           | 08c0a888-b619-41bd005dd8c8 | IngressInterface    |
| DeviceType            | ASA                        | InitiatorIP         |
| EgressInterface       | 4                          | InitiatorPort       |
| EventType             | 3                          | LastPacketSecond    |
| FirewallExtendedEvent | 1001                       | MappedInitiatorIP   |
| ICMPCode              | 0                          | MappedInitiatorPort |
| ICMPType              | 0                          | MappedResponderIP   |

As long as you rollover a value and it is highlighted blue, you can add that value to the search string.

### AND, OR, NOT, AND NOT, OR NOT Filter Operators

Here are the behaviors of "AND", "OR", "NOT", "AND NOT", and "OR NOT" used in a search string:

#### AND

Use the AND operator in the filter string, to find events that include all attributes. The AND operator cannot begin a search string.

For example, the search string below will search for events that contain the TCP protocol AND that originated from InitiatorIP address 10.10.10.43, AND that were sent from the Initiator port 59614. One would expect that with each additional AND statement, the number of events that meet the criteria would be small and smaller.

Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"

#### OR

Use the OR operator in the filter string, to find events that include any of the attributes. The OR operator cannot begin a search string.

For example, the search string below will display events in the event viewer that include events that include the TCP protocol, OR that originated from InitiatorIP address 10.10.10.43, OR that were sent from the Initiator port 59614. One would expect that with each additional OR statement, the number of events that meet the criteria would be bigger and bigger.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

## NOT

Use this only at the beginning of a search string to exclude events with certain attributes. For example, this search string would exclude any event with the InitiatorIP 192.168.25.3 from the results.

```
NOT InitiatorIP: "192.168.25.3"
```

## AND NOT

Use the AND NOT operator in the filter string to exclude events that contain certain attributes. AND NOT cannot be used at the beginning of a search string.

For example, this filter string will display events with the InitiatorIP 192.168.25.3 but not those whose ResponderIP address is also 10.10.10.1.

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

You can also combine NOT and AND NOT to exclude several attributes. For example this filter string, will exclude events with InitiatorIP 192.168.25.3 and events with ResponderIP 10.10.10.1

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

## OR NOT

Use the OR NOT operator to include search results that exclude certain elements. The OR NOT operator cannot be used at the beginning of a search string.

For example, this search string will find events with the Protocol of TCP, OR that have the InitiatorIP of 10.10.10.43, or those NOT from InitiatorPort 59614.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

You could also think of it this way: Search for (Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614").

## Wildcard Searches

Use an asterisk (\*) to represent a wildcard in the value field of an **attribute:value** search to find results within events. For example, this filter string,

```
URL: *feedback*
```

will find strings in the URL attribute field of events that contain the string **feedback**.

## Related Information:

- [Show and Hide Columns on the Event Logging Page](#)
- [Event Attributes in Security Analytics and Logging](#)

## Search Historical Events in the Background

CDO provides you the ability to define a search criteria and search for event logs based on any defined search criteria. Using the background search capability, you can also perform event log searches in the background, and view the search results once the background search is completed.

Based on the subscription alert and service integrations you have configured, you are notified once the background search has been completed.

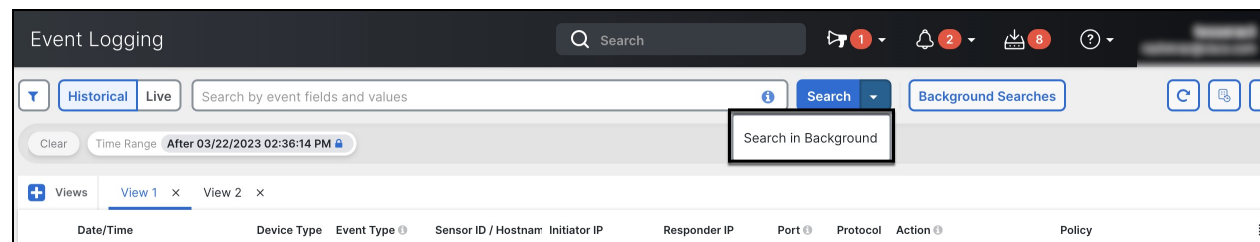
You can view, download, or delete the search results directly from the Background Search page. You can also schedule a background search to occur for a one-time event or schedule a recurring schedule. Navigate to the Notification Settings page to view or modify the subscription options.

## Search for Events in the Events Logging Page

Use the search and background search capabilities to view all logged events in the Event Logging page. Note that background searches can only be performed for historical events.

### Procedure

- Step 1** In the navigation bar, choose **Analytics > Event Logging**.
- Step 2** Click either the **Historical** or **Live** tab.
- Step 3** Navigate to the search bar, type the search expression, and enter the **Search** button to execute the search. You can narrow or expand the search with an Absolute Time Range or Relative Time Range.
- Alternatively, from the **Search** drop-down list, choose **Search in Background** to execute the search in the background while you move away from the search page. You are notified when the search results are ready.



If you click the **Search** button, the results directly appear in the Event Logging view. Upon selecting any specific search result, the search criteria appears in the search bar for an easy reference.

If you choose to execute the search in the background, the search operation is queued, and you are notified once the search is completed. You are allowed to execute multiple search queries in the background.

- Step 4** Click the **Background Searches** button to view the Background Searches page.

Background Searches ✕

[Start a Background Search](#)
[View Notification Settings](#)

| Search Name          | File Size | User              | Status                             | Run Time                                                    | Actions                                                           |
|----------------------|-----------|-------------------|------------------------------------|-------------------------------------------------------------|-------------------------------------------------------------------|
| Search_1679428080471 | 3.74 KB   | admin@example.com | ✔ Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 3:48:03 PM<br>Completed in 2 seconds  | <a href="#">View</a> <a href="#">Download</a> <a href="#">...</a> |
| Search_1679428045727 | 3.74 KB   | admin@example.com | ✔ Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 3:47:27 PM<br>Completed in 2 seconds  | <a href="#">View</a> <a href="#">Download</a> <a href="#">...</a> |
| Search_1679427993327 | 2.25 KB   | admin@example.com | ✔ Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 3:46:35 PM<br>Completed in 2 seconds  | <a href="#">View</a> <a href="#">Download</a> <a href="#">...</a> |
| Search_167942230313  | 662 Bytes | admin@example.com | ✔ Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 1:58:39 PM<br>Completed in 3 seconds  | <a href="#">View</a> <a href="#">Download</a> <a href="#">...</a> |
| Search_1679408015574 | 662 Bytes | admin@example.com | ✔ Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 10:13:44 AM<br>Completed in 3 seconds | <a href="#">View</a> <a href="#">Download</a> <a href="#">...</a> |

Close

The Background Searches page displays a list of search results. You can choose to view, download, or delete the search results. You can also navigate to the Notification Settings page to view or modify the subscription options. Select the **Start a Background Search** button to initiate a search from this page.

### What to do next

You can turn any background search into a scheduled background search if you need a recurring query. See [Schedule a Background Search in the Event Viewer, on page 100](#) for more information.

## Schedule a Background Search in the Event Viewer

Schedule a recurring query in the background in the event viewer page. Searches can only be scheduled for historical events. You can modify or cancel the scheduled search at any time. You can also modify an existing query to be a recurring search.



**Note** You can opt to get alerts on searches that have started, completed, or have failed.

You can schedule a background search only for **historical** events. Use the following steps to create a scheduled background search:

### Procedure

- Step 1** In the navigation bar, choose **Analytics > Event Logging**.
- Step 2** Click the **Historical** toggle to select it. You can only schedule a background search for historical events.
- Step 3** In the search bar, type the search expression you want to search for. Click the **Search** drop-down button and choose **Search in background**.
- Step 4** (Optional) Rename the search.
- Step 5** The **Search Now** checkbox is checked by default. When checked, the search starts upon saving; if unchecked, the background query runs only as a future search.
- Step 6** Check the **Setup recurring schedule** and configure the following settings:

- **Search Logs for the Last** - How far back you want to search through.
- **Frequency** - How frequent you want the scheduled search to occur.

**Step 7** Confirm the scheduled search criteria at the bottom of the window. Select **Schedule and Search Now**. Alternatively, if you did not opt for the search to start immediately, the button reads **Schedule Search**

---

#### What to do next

Results from a scheduled background search are available for review for up to 7 days before CDO automatically deletes them.

## Download a Background Search

Search results and scheduled queries are stored for seven days before CDO automatically removes them. Download a .CSV copy of the background search that was performed for historical events.

#### Procedure

---

- Step 1** In the navigation pane go to **Analytics > Event Logging**.
- Step 2** Click **Background Searches > Actions > Download**.
- Step 3** Locate your search. Scheduled searches are stored under the **Queries** tab.
- Step 4** Click **Download**. The .CSV file automatically downloads to your default storage location on your local drive.
- 

## Data Storage Plans

You need to buy a data storage plan that reflects the number of events the Cisco cloud receives from your on-boarded ASAs and FDM-managed devices on a daily basis. This is called your "daily ingest rate." Data plans are available in whole number amounts of GB/day and in 1, 3 or 5 year terms. The best way to determine your ingest rate is to participate in a free trial of Secure Logging Analytics (SaaS) before you buy it. This will give you a good estimate of your event volume.

Customers automatically receive 90 days of rolling data storage. That means that the most recent 90 days of events are stored in the Cisco cloud and the 91st day is deleted.

Customers can upgrade to additional event retention beyond the default 90-days, or add additional daily volume (GB/day) by a change order to an existing subscription, and will only be billed for the remainder of their subscription term on a prorated basis.

See the [Secure Logging Analytics \(SaaS\) Ordering Guide](#) for all the details about data plans.



**Note** If you have a Security Analytics and Logging license and data plan, then obtain a different Security Analytics and Logging license at a later date, you are not required obtain a different data plan. If your network traffic throughput changes and you obtain a different data plan, that alone does not require you to obtain a different Security Analytics and Logging license.

### What data gets counted against my allotment?

All events sent to the Secure Event Connector accumulate in the Secure Logging Analytics (SaaS) cloud and count against your data allotment.

Filtering what you see in the Events viewer does not decrease the number of events stored in the Secure Logging Analytics (SaaS) cloud, it reduces the number of events you can see in the Events viewer.

Your events are stored in the Secure Logging Analytics (SaaS) cloud for 90 days; after that, they are purged.

### We're using up our storage allotment quickly, what can we do?

Here are two approaches to address that problem:

- [Request more storage](#). You may have underestimated what you need.
- Reduce the number of rules that log events. You can log events from SSL policy rules, security intelligence rules, access control rules, as well as intrusion policies and file and malware policies. Examine what you are logging. Do you need to log events from as many rules and policies as you think?

## Extend Event Storage Duration and Increase Event Storage Capacity

Security Analytics and Logging customers receive 90 days of event storage when they purchase any of these [Licensing](#).

- **Logging and Troubleshooting**
- **Logging Analytics and Detection**
- **Total Network Analytics and Monitoring**

You can choose to upgrade your license to have 1, 2, or 3 years worth of rolling event storage at the time you first purchase your license or at any time during the duration of your license.

At the time you first purchase your Security Analytics and Logging license, you will be asked if you want to upgrade your storage capacity. If you answer, "yes," an additional Product Identifier (PID) will be added to the list of PIDs you are purchasing.

If you decide in the middle of your license term to extend your rolling event storage or increase the amount of event cloud storage, you can:

### Procedure

- 
- Step 1** Log in to your account on [Cisco Commerce](#).
- Step 2** Select your Cisco Defense Orchestrator PID.

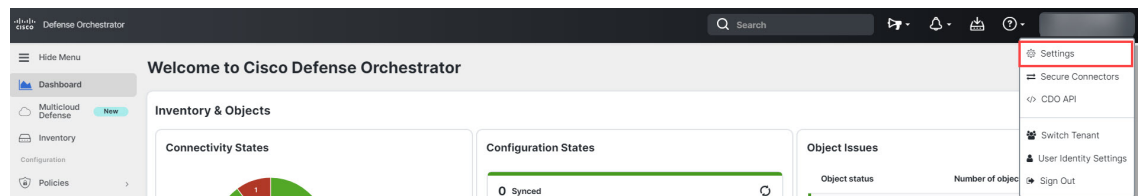
- Step 3** Follow the prompts to upgrade the length or capacity of your storage capacity.
- The increased cost will be pro-rated based for the term remaining on your existing license. See the [Secure Logging Analytics \(SaaS\) Ordering Guide](#) for detailed instructions.

## View Security Analytics and Logging Data Plan Usage

To see your monthly logging limit, the amount of storage you have used, and when the usage period resets to zero, do the following:

### Procedure

- Step 1** Click the tenant and select **Settings**.



- Step 2** Click **Logging Settings**.
- Step 3** You can also click **View Historical Usage** to see up to the last 12 months of storage usage.

## Finding Your Device's TCP, UDP, and NSEL Port Used for Secure Logging Analytics (SaaS)

Secure Logging Analytics (SaaS) allows you to send events from your ASA or FDM-managed devices to certain UDP, TCP, or NSEL ports on the Secure Event Connector (SEC). The SEC then forwards those events to the Cisco cloud.

If these ports aren't already in use, the SEC makes them available to receive events and the Secure Logging Analytics (SaaS) documentation recommends using them when you configure the feature.

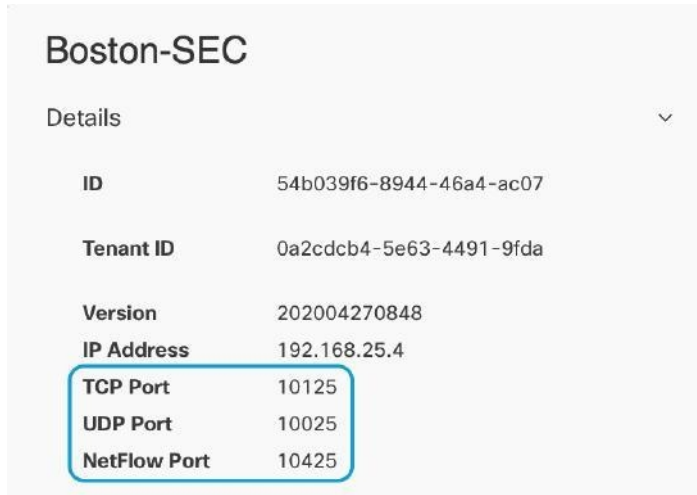
- TCP: 10125
- UDP: 10025
- NSEL: 10425

If those ports are already in use, before you configure Secure Logging Analytics (SaaS), look at your SEC device details to determine what ports it is actually using to receive events.

To find the port numbers the SEC uses:

## Procedure

- Step 1** From the CDO menu, choose **Tools & Services > Secure Connectors**.
- Step 2** In the Secure Connectors page, select the SEC you want to send events to.
- Step 3** In the Details pane, you will see the TCP, UDP, and NetFlow (NSEL) port you should send events to.



| Boston-SEC   |                         |
|--------------|-------------------------|
| Details      |                         |
| ID           | 54b039f6-8944-46a4-ac07 |
| Tenant ID    | 0a2cdcb4-5e63-4491-9fda |
| Version      | 202004270848            |
| IP Address   | 192.168.25.4            |
| TCP Port     | 10125                   |
| UDP Port     | 10025                   |
| NetFlow Port | 10425                   |