Cisco Security Analytics and Logging (On Premises) v3.2.0: Firewall Event Integration Guide

First Published: 2023-01-27

Last Modified: 2023-01-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CHAPTER 1

Introduction

Overview

This guide explains how to configure Cisco Security Analytics and Logging (On Premises) to store your Firewall event data for increased storage at a larger retention period. By deploying Cisco Secure Network Analytics (formerly Stealthwatch) appliances, and integrating them with your Firewall deployment, you can export your event data to a Secure Network Analytics appliance.

You can then:

- Store events on the Secure Firewall Management Center and events on the Secure Network Analytics deployment.
- Specify this remote data source to view these events in the management center.
- Review your event data from the Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console) Web App UI using the Event Viewer.
- Cross-launch from the management center UI to the Event Viewer to view additional context on the information from which you cross-launched.

Note If you want to store Firewall event data in the Cisco cloud, as opposed to on-premises, see the Cisco Security Analytics and Logging (SaaS) documentation for more information.

Concepts and Architecture

In a Security Analytics and Logging (OnPrem) deployment, you can use a Secure Network Analytics appliance to store data from another Cisco product deployment. In the case of the Secure Firewall deployment, you can export your Security Events and data plane events from your Secure Firewall Threat Defense devices managed by the management center to a Manager to store that information.

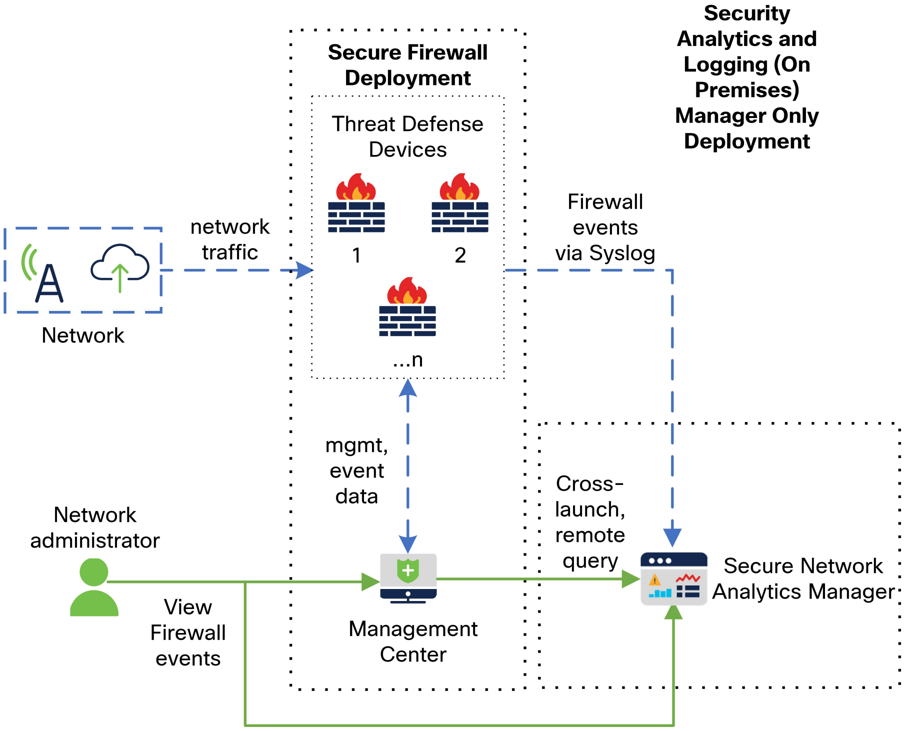
You have two options for Secure Network Analytics deployment:

- Manager only - Deploy a standalone Manager to receive and store events, and from which you can review and query events

- Data Store - Deploy Cisco Secure Network Analytics Flow Collectors (up to 5) to receive events, a Cisco Secure Network Analytics Data Store containing 1, 3, or more (in sets of 3) Cisco Secure Network Analytics Data Nodes to store events, and a Manager from which you can review and query events

Manager Only

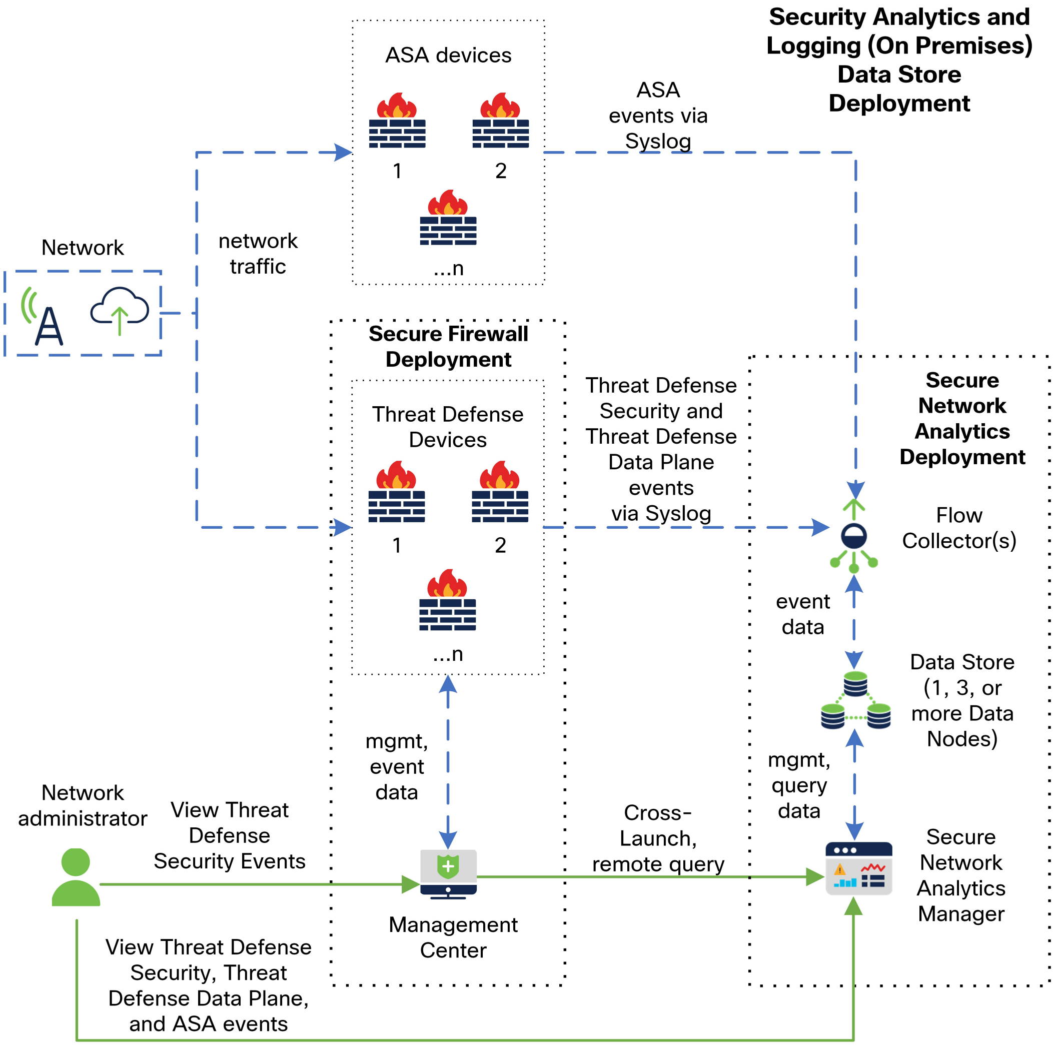
See the following diagram for an example of a Manager only deployment:


Secure Firewall Deployment
Threat Defense Devices
1
2
...n
Security Analytics and Logging (On Premises) Manager Only Deployment
network traffic
Network
Firewall events via Syslog
mgmt, event data
Network administrator
View Firewall events
Management Center
Cross-launch, remote query
Secure Network Analytics Manager

In this deployment, the threat defense devices send Secure Firewall events to the Manager, and the Manager stores these events. From the management center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the management center.

Data Store

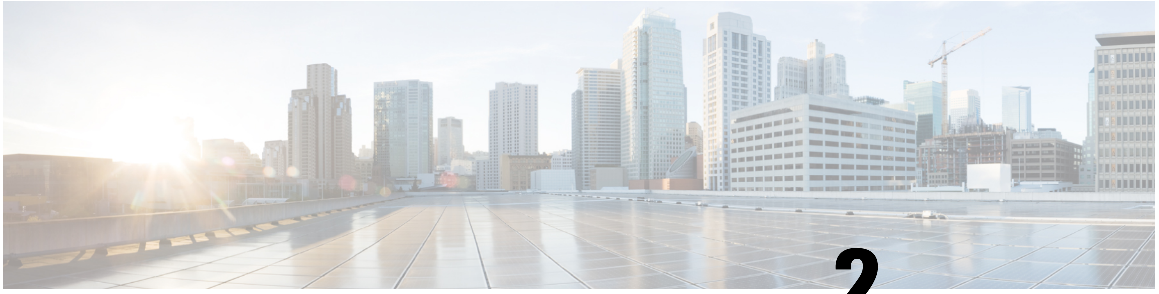
See the following diagram for an example of a Data Store deployment with a Manager, Data Nodes, and Flow Collector(s):


Security Analytics and Logging (On Premises) Data Store Deployment
ASA devices
1
2
...n
ASA events via Syslog
Network
network traffic
Secure Firewall Deployment
Threat Defense Devices
1
2
...n
Threat Defense Security and Threat Defense Data Plane events via Syslog
Secure Network Analytics Deployment
Flow Collector(s)
event data
Data Store (1, 3, or more Data Nodes)
mgmt, event data
mgmt, query data
Network administrator
View Threat Defense Security Events
Cross-Launch, remote query
Management Center
Secure Network Analytics Manager
View Threat Defense Security, Threat Defense Data Plane, and ASA events

In this deployment, the threat defense and Secure Firewall ASA devices send Firewall events to the Flow Collector. The Flow Collector sends the events to the Data Store for storage. From the management center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the management center.

Supported Event Types

- Threat Defense Security events
  - Connection
  - Intrusion
  - File and Malware
- Threat Defense Data Plane events (Data Store deployment only)
- ASA events (Data Store deployment only)



CHAPTER 2

Deployment

Requirements

The following lists the appliance requirements for deploying Security Analytics and Logging (OnPrem) to store your Firewall event data.

Firewall Appliances

You must deploy the following Firewall appliances:

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Secure Firewall Management Center (hardware or virtual)	v7.2+ For the management center running earlier versions, see https://cisco.com/go/sal-on-prem-docs.	none	• You can deploy one Manager per management center, and optionally multiple Flow Collectors and Data Nodes.
Secure Firewall managed devices	v7.0+ using the wizard Threat Defense v6.4 or later using syslog NGIPS v6.4 using syslog	none	• For instructions on how to use syslog for the threat defense v6.4 or later, see Sending Events from Threat Defense Devices On Earlier Versions.
ASA devices	v9.12+	none	

Secure Network Analytics Appliances

You have the following options for deploying Secure Network Analytics:

- Manager only - Deploy only a Manager to ingest and store events, and review and query events
- Data Store - Deploy Flow Collector(s) to ingest events, Data Store to store events, and Manager to review and query events

Table 1: Manager only

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.4.2	none	• The Manager can receive events from multiple threat defense devices, all managed by one management center. • Make sure to install the Security Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events on the Manager.
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v3.2.x	Logging and Troubleshooting Smart License, based on GB/day	• Install this app on the Manager and configure to enable event ingest.

Table 2: Data Store

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.4.2	none	• Make sure to install theSecurity Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events on the Manager. • Secure Network Analytics v7.4.1+ is required for Single Node Data Store and multi-telemetry,
Flow Collector	Secure Network Analytics v7.4.2	none	• You can deploy up to 5 Flow Collectors that are configured for Data Store. • The Flow Collector can receive events from multiple threat defense devices, all managed by one management center. • The Flow Collector can receive ASA events from multiple ASA devices. • Secure Network Analytics v7.4.1+ is required for Single Node Data Store and multi-telemetry.

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Data Store	Secure Network Analytics v7.4.2	none	• You can deploy either 1, 3, or more (in sets of 3) Data Nodes. • Stores Firewall events received by Flow Collector(s). • Secure Network Analytics v7.4.1+ is required for Single Node Data Store and multi-telemetry.
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v3.2.x	Logging and Troubleshooting Smart License, based on GB/day	• Install this app on the Manager and configure to enable event ingest.

In addition to these components, you must make sure that all of the appliances can synchronize time using NTP.

If you want to remotely access the Secure Firewall or Secure Network Analytics appliances' consoles, you can enable access over SSH.

Secure Network Analytics Licensing

You can use Security Analytics and Logging (OnPrem) for 90 days without a license in Evaluation Mode. To continue using Security Analytics and Logging (OnPrem) after the 90 day period, you must obtain a Logging and Troubleshooting Smart License for Smart Licensing, based on the GB per day you anticipate sending in syslog data from your Firewall deployment to your Secure Network Analytics appliance.

Note For license calculation purposes, the amount of data is reported to the nearest whole GB, truncated. For example, If you send 4.9 GB in a day, it is reported as 4 GB.

See the Secure Network Analytics Smart Software Licensing Guide for more information on licensing your Secure Network Analytics appliances.

Secure Network Analytics Resource Allocation

Secure Network Analytics offers the following ingest rates when deployed for Security Analytics and Logging (OnPrem):

- a hardware or virtual edition (VE) Manager only deployment can ingest up to roughly 20k events per second (EPS) on average, with short bursts of up to 35k EPS
- a virtual edition (VE) Data Store deployment, with 3 Data Nodes, can ingest up to roughly 50k EPS on average, with short bursts of up to 175k EPS
- a hardware Data Store deployment, with 3 Data Nodes, can ingest up to roughly 100k EPS on average, with short bursts of up to 350k EPS

Based on the allocated hard drive storage, you can store the data for several weeks or months. These estimates are subject to various factors, including network load, traffic spikes, and information transmitted per event.

Note At higher EPS ingest rates, the Security Analytics and Logging (OnPrem) app may drop data. In addition, if you send all event types, instead of only connection, intrusion, file, and malware events, the app may drop data as your overall EPS rises. Review the log files in this case.

Manager Only Recommendations

Manager VE Resources

For optimum performance, allocate the following resources if you deploy a Manager VE:

Resource	Recommendation
CPUs	12
RAM	64 GB
Hard drive storage	2 TB

Manager 2210 Specifications

For hardware specifications, see the Manager 2210 Specification Sheet.

Estimated Retention

Based on the storage space that you allocate for your Manager VE or if you have a Manager 2210, you can store your data for roughly the following time frames on a Manager only deployment:

Average EPS	Average Daily Events	Estimated Retention Period for 1 TB Storage	Estimated Retention Period for 2 TB Storage	Estimated Retention Period for 4 TB Storage (Hardware)
1,000	86.5 million	250 days	500 days	1000 days
5,000	430 million	50 days	100 days	200 days
10,000	865 million	25 days	50 days	100 days
20,000	1.73 billion	12.5 days	25 days	50 days

When the Manager reaches maximum storage capacity, it deletes the oldest data first to make room for incoming data.

Note We have tested the Manager VE with these resource allocations for this estimated ingest and storage period. You may note unanticipated errors due to insufficient resource allocation if you do not assign enough CPUs or RAM to the virtual appliance. If you increase the storage allocation beyond 2 TB, you may note unanticipated errors due to insufficient resource allocation.

Data Store Recommendations

For optimum performance, allocate the following resources if you deploy a Manager VE, Flow Collector VE, and Data Store VE:

Note If you are using a Single Node Data Store or if you have enabled multi-telemetry in Secure Network Analytics, your resource allocation and storage capacity may be different from the following recommendations. For more information, refer to the Secure Network Analytics Appliance Installation Guide (Hardware or Virtual Edition) and the System Configuration Guide v7.4.1.

Table 3: Manager VE

Resource	Recommendation
CPUs	8
RAM	64 GB
Hard drive storage	480 GB

Table 4: Flow Collector VE

Resource	Recommendation
CPUs	8
RAM	70 GB
Hard drive storage	480 GB

Table 5: Data Nodes VE (as part of a Data Store)

Resource	Recommendation
CPUs	12 per Data Node
RAM	32 GB per Data Node
Hard drive storage	5 TB per Data Node VE, or 15 TB total across 3 Data Nodes

Hardware Specifications

For hardware specifications, refer to the appliance specification sheets.

Estimated Retention (3 Data Nodes)

Based on the storage space that you allocate for your Data Store VE or if you have a hardware deployment, you can store your data for roughly the following time frames on your Data Store deployment:

Average EPS	Average Daily Events	Virtual	Hardware
1,000	86.5 million	1,500 days	3,000 days
5,000	430 million	300 days	600 days
10,000	865 million	150 days	300 days
20,000	1.73 billion	75 days	150 days
25,000	2.16 billion	60 days	120 days
50,000	4.32 billion	30 days	60 days
75,000	6.48 billion	Not supported	40 days
100,000	8.64 billion	Not supported	30 days

When the Data Store reaches maximum storage capacity, it deletes the oldest data first to make room for incoming data. To increase your storage capacity, add more Data Nodes using the Secure Network Analytics System Configuration Guide.

Note We have tested the virtual appliances with these resource allocations for this estimated ingest and storage period. You may note unanticipated errors due to insufficient resource allocation if you do not assign enough CPUs or RAM to the virtual appliance. If you increase the Data Node storage allocation beyond 5 TB, you may note unanticipated errors due to insufficient resource allocation.

Communication Ports

The following table lists the communication ports you must open for the Security Analytics and Logging (OnPrem) integration for a Manager only deployment.

Table 6: Manager only

From (Client)	To (Server)	Port	Protocol or Purpose
Management Center, Threat Defense devices, and Manager	External internet (NTP server)	123/UDP	NTP time synchronization, all to the same NTP server
User workstations	Management Center and Manager	443/TCP	Logging into the appliances' web interfaces over HTTPS using a web browser

From (Client)	To (Server)	Port	Protocol or Purpose
Threat Defense devices managed by a management center	Manager	8514/UDP	Syslog export from the threat defense devices, ingest to the Manager
Management Center	Manager	443/TCP	remote query from management center to the Manager

The following table lists the communication ports you must open for the Security Analytics and Logging (OnPrem) integration for a Data Store deployment. In addition, see the x2xx Series Hardware Appliance Installation Guide or the Virtual Edition Appliance Installation Guide for the ports you must open for your Secure Network Analytics deployment.

Table 7: Data Store

From (Client)	To (Server)	Port	Protocol or Purpose
Management Center, Threat Defense devices, Manager, Flow Collector, and Data Store	External internet (NTP server)	123/UDP	NTP time synchronization, all to the same NTP server
user workstations	Management Center and Manager	443/TCP	Logging into the appliances' web interfaces over HTTPS using a web browser
Threat Defense devices managed by a management center	Flow Collector	8514/UDP	Syslog export from the threat defense devices, ingest to Flow Collector
ASA devices	Flow Collector	8514/UDP	Syslog export from ASA devices, ingest to Flow Collector
Management Center	Manager	443/TCP	Remote query from the management center to the Manager

Configuration Overview

The following describes the high-level steps for configuring your deployment to store event data.

Review these tasks before starting your deployment.

Component and Task	Steps
Deploy Manager only	You have the following options: • Deploy a Manager 2210 to your network, and perform initial configuration, including assigning an eth0 management interface IP address and other information. See the x2xx Series Hardware Appliance Installation Guide and Secure Network Analytics System Configuration Guide for more information. • Download the Manager VE ISO, and deploy the Manager VE to your hypervisor. Perform initial configuration, and assign an eth0 management interface IP address and other information. See the Secure Network Analytics Virtual Edition Appliance Installation Guide for more information.
Deploy Data Store	• Deploy a Manager, Flow Collector(s), and 1, 3 or more (in sets of 3) Data Nodes to your network. Perform initial configuration for each appliance, and initialize the Data Store. See x2xx Series Hardware Appliance Installation Guide or Virtual Edition Appliance Installation Guide, and the Secure Network Analytics System Configuration Guide for more information.
Download and install the Security Analytics and Logging (OnPrem) app on your Manager, and configure your Secure Network Analytics deployment to receive and store Firewall events.	• Download the app file, app-smc-sal-3.2.0-v2.swu from https://software.cisco.com. • On the Manager, go to App Manager in Central Management and install the app. See the Security Analytics and Logging (OnPrem) release notes and app help for more information on the app.
Configure the management center to send events to Security Analytics and Logging (OnPrem)	You have the following options: • Configure the management center to send events to your Secure Network Analytics appliance using the Secure Firewall Management Center Configuration, on page 16 section. • Configure Data Plane event logging using the Configure Secure Firewall Management Center to Send Data Plane Event Logs to Secure Network Analytics using Syslog section. • Reduce logging load on the management center using the Stop Storing Low-Priority Connection Events on the Management Center section.
Configure ASA devices to send events to Security Analytics and Logging (OnPrem)	• Configure your ASA devices to send events to your Secure Network Analytics appliance using the ASA Devices Configuration, on page 22 section.

Component and Task	Steps
Review Next Steps	Review the Next Steps: • Review the Secure Firewall online help for more information. See Work in the Management Center with Connection Events Stored on a Secure Network Analytics Appliance. • Review the Manager Web App online help for more information on how to use Secure Network Analytics.

Secure Network Analytics Deployment and Configuration

To deploy and configure Secure Network Analytics for Security Analytics and Logging (OnPrem):

1. Follow the instructions for your Secure Network Analytics deployment:
   - Manager Only Deployment and Configuration, on page 14
   - Data Store Deployment and Configuration, on page 15
2. Install the Security Analytics and Logging (OnPrem) App, on page 15.

Manager Only Deployment and Configuration

Before you begin

- Ensure that you have deployed a Manager to your network, and that the management IP address is reachable by both your management center's management IP address and your threat defense device's management IP addresses. Note the management IP address for further configuration. See the Secure Network Analytics Virtual Edition Appliance Installation Guide for more information.
- Ensure that you register your Secure Network Analytics product instance. The Manager VE license is automatically added to your account after registration. See the Secure Network Analytics Smart Software Licensing Guide for more information.

Follow the instructions in the Secure Network Analytics Virtual Edition Appliance Installation Guide to deploy your Manager VE, or the x2xx Series Hardware Appliance Installation Guide to deploy your Manager 2210, and Secure Network Analytics System Configuration Guide to configure your Manager.

Data Store Deployment and Configuration

Important Make sure to enable your Flow Collector(s) to ingest and store Firewall Logs during appliance First Time Setup. This setting configures your Flow Collector for use with Security Analytics and Logging (OnPrem). After appliance configuration, you can update your ingest settings using Flow Collector Advanced Settings. Refer to the Security Analytics and Logging (OnPrem) Configuration Using Flow Collector Advanced Settings section for more information.

Before you begin

- Ensure that you have deployed a Manager, Flow Collector(s), and Data Node(s) to your network, that the Flow Collector(s) management IP address is reachable by your threat defense device's management IP addresses, and that the Manager management IP address is reachable by your management center's management IP address. Note the management IP address for further configuration.
- Ensure that you register your Secure Network Analytics product instance. The Manager VE license is automatically added to your account after registration. See the Secure Network Analytics Smart Software Licensing Guide for more information.

Step 1 Follow the instructions in the x2xx Series Hardware Appliance Installation Guide to deploy your Secure Network Analytics hardware appliances, or Virtual Edition Appliance Installation Guide to deploy your Secure Network Analytics virtual appliances.

Step 2 Configure your appliances using the Secure Network Analytics System Configuration Guide. When configuring First Time Setup on your Flow Collector(s), make sure to select the following:

- Select **Yes** when asked to deploy the Flow Collector as part of a Data Store. If you select No, you will have to deploy a new virtual appliance or RFD your appliance.
- Select **Firewall Logs** on the select telemetry types screen. Then enter a UDP Port, 8514 is used by default. Click **Yes** to confirm your settings.

Install the Security Analytics and Logging (OnPrem) App

Install the Security Analytics and Logging (OnPrem) app on your Manager. See the Security Analytics and Logging (OnPrem) Release Notes for more information.

Step 1 Log in to your Cisco Smart Account at https://software.cisco.com, or contact your administrator, to download the Security Analytics and Logging (OnPrem) app.

Step 2 Log in to your Manager.

Step 3 From the main menu, select **Configure** > **GLOBAL Central Management.**

Step 4 Click the **App Manager** tab.

Step 5 Click **Browse**.

Step 6 Follow the on-screen prompts to upload the app file.

What to do next

- Configure the management center to send events to your Secure Network Analytics appliance.
- Configure your ASA devices to send events to your Secure Network Analytics appliance. See ASA Devices Configuration, on page 22.

Secure Firewall Management Center Configuration

When you configure Secure Firewall Management Center for Security Analytics and Logging (OnPrem), you have the following options to send events to Secure Network Analytics:

- Configure the Wizard in Secure Firewall Management Center to send events directly to Secure Network Analytics deployment.
- Configure Secure Firewall Management Center to Send Data Plane Event Logs to Secure Network Analytics using Syslog.

Configure the Wizard in Secure Firewall Management Center

The following describes the wizard for deploying Security Analytics and Logging (OnPrem) for all Secure Firewall Management Center users to send and store firewall events.

- Manager only: Deploy a standalone Manager to send and store events, and from which you can review and query events. For more information on configuring a Manager only deployment, see Configure the Secure Firewall Management Center to Send Event Data to a Manager Only Deployment.
- Data Store: Deploy Flow Collector(s) to receive events, Data Store to store events, and a Manager from which you can review and query events. For more information on configuring a Data Store deployment, see Configure the Secure Firewall Management Center to Send Event Data to a Data Store Deployment.

Prerequisites for Secure Firewall Integration

- Your Secure Firewall system must be working as expected and generating the events that you want to send.
- Set up your Secure Network Analytics and Security Analytics and Logging (OnPrem) products to be ready to receive Firewall event data.
- You must have one of the following Secure Firewall user roles:
  - Admin
  - Analyst
  - Security Analyst

- If you are currently using syslog to send events to Secure Network Analytics from device versions that support sending events directly, disable syslog for those devices (or assign those devices an access control policy that does not include syslog configurations) to avoid duplicate events on the remote volume.
- You have the following details:
    - The hostname or IP address of your Manager.
    - (If you are using a Flow Collector to aggregate multiple Secure Network Analytics appliances for extended storage capacity) The IP address of your Flow Collector. (You cannot use hostname for this setting.)
    - Credentials for an account on your Secure Network Analytics appliance that has administrator privileges.

      These credentials are NOT stored on the management center; they are used once in order to establish a read-only analyst API account for the management center on the Manager. A dedicated account is not needed for this integration; you can use your own admin credentials.

      You may be logged out of the Manager during the registration process; complete any work in progress before starting this wizard.
    - SSL certificate from your Manager, if you prefer not to use the "trust on first use" option.

Configure the Secure Firewall Management Center to Send Event Data to a Manager Only Deployment

Before you begin

Ensure that you meet all the requirements that are mentioned in Configure the Wizard in Secure Firewall Management Center.

Step 1 In Secure Firewall Management Center, go to **Integration** > **Security Analytics & Logging**.

Step 2 In the **Manager only** widget, click **Start**.

Step 3 Enter the host name or IP address and port of your Secure Network Analytics Manager, and click **Next**.

Step 4 Confirm the discovered settings.

a. Verify the IP address and port for logging, and modify if necessary.

b. Verify the cross-launch URL and port, and modify if necessary.

c. If you prefer not to use the "trust on first use" option, upload the SSL certificate from your Manager.

d. Click **Next**.

Step 5 Enter credentials to log in to the Manager to establish secure communication for queries, and click **Complete**.

These credentials are not stored on the management center; they are used once to establish a read-only analyst API account for the management center on the Secure Network Analytics Manager. A dedicated account is not needed for this integration; you can use your own admin credentials.

What to do next

- After you have confirmed that events are successfully being stored on your Secure Network Analytics appliance, allow time to pass until you are certain that all events stored on your management center are also available remotely. Then see Stop Storing Low-Priority Connection Events on the Management Center.

Note If you need to change any of these configurations, run the wizard again. If you disable the configuration or run the wizard again, all settings except the account credentials are retained.

Configure the Secure Firewall Management Center to Send Event Data to a Data Store Deployment

Before you begin

- Ensure that you meet all the requirements that are mentioned in Configure the Wizard in Secure Firewall Management Center.
- The managed device version is 7.0 or later.

Step 1 In the management center, go to **Integration** > **Security Analytics & Logging**.

Step 2 In the **Data Store** widget, click **Start**.

Step 3 Enter the hostname or IP address and port of your Manager.

Step 4 Enter the hostname or IP address and port of the Flow Collector.

To add more Flow Collectors, click **+ Add another flow collector**.

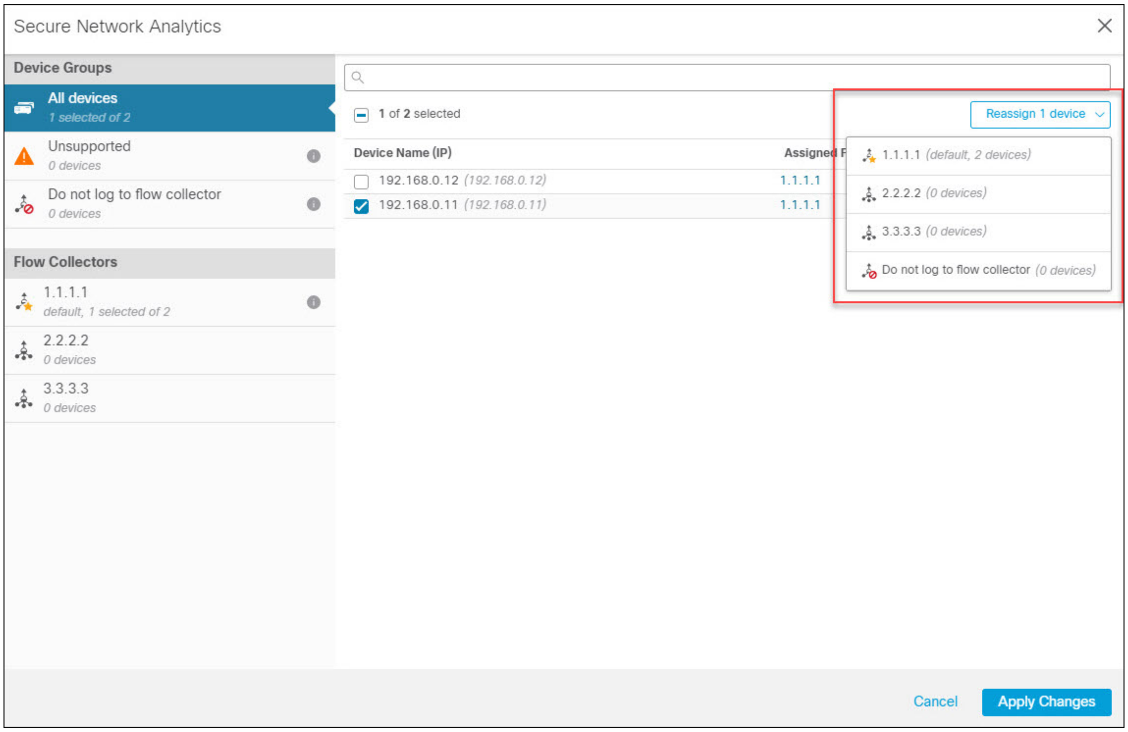
Step 5 (Optional) If you have configured more than one Flow Collector, associate the managed devices with different Flow Collectors.

By default, all your managed devices are assigned to the default Flow Collector.

a. Click **Assign Devices**.

b. Select the managed devices that you want to reassign.

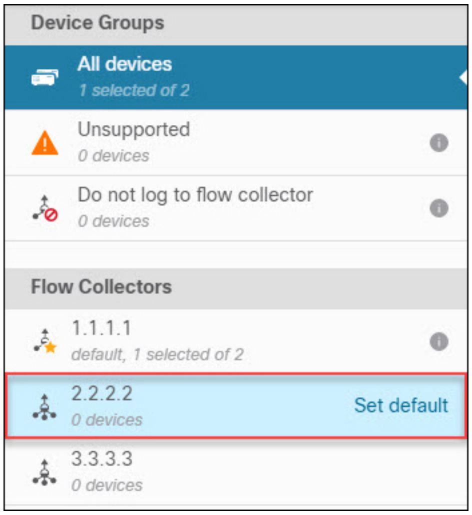
c. From the reassign device drop-down list, choose the Flow Collector.



	Device Name (IP)	Assigned F
□	192.168.0.12 (192.168.0.12)	1.1.1.1
☑	192.168.0.11 (192.168.0.11)	1.1.1.1

If you do not want a managed device to send event data to any of the Flow Collectors, select that device, and choose **Do not log to flow collector** from the reassign device drop-down list.

Note You can change the default Flow Collector by hovering over the intended Flow Collector and clicking **Set default**.



d. Click **Apply Changes**.

Step 6 Click **Next**.

Step 7 Confirm the discovered settings.

a. Verify the cross-launch URL and port, and modify if necessary.

b. If you prefer not to use the "trust on first use" option, upload the SSL certificate from your Manager.

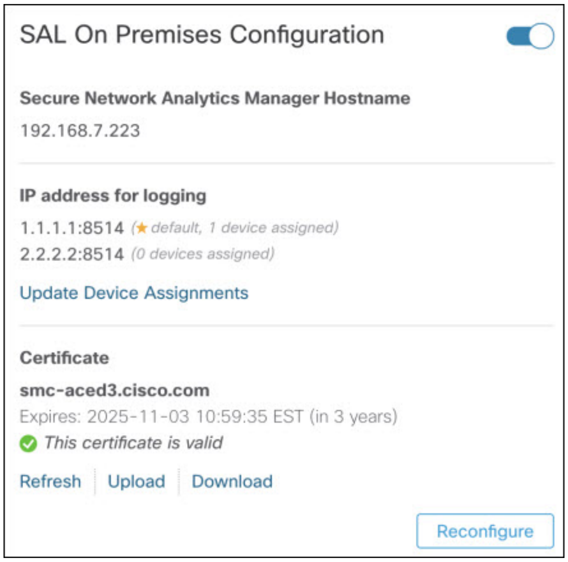
Note For more information on how to obtain and upload SSL certificate, see Cisco Secure Network Analytics: SSL/TLS Certificates for Managed Appliances.

c. Click **Next**.

Step 8 Enter credentials to log in to the Manager to establish secure communication for queries, and click **Complete**.

These credentials are not stored on the management center; they are used once to establish a read-only analyst API account for the management center on the Manager. A dedicated account is not needed for this; you can use your own admin credentials.

After you save the configuration, you can update the device assignment by clicking **Update Device Assignments** on the **Security Analytics & Logging** page.



SAL On Premises Configuration

Secure Network Analytics Manager Hostname
192.168.7.223

IP address for logging
1.1.1.1:8514 (★ default, 1 device assigned)
2.2.2.2:8514 (0 devices assigned)

Certificate
smc-aced3.cisco.com
Expires: 2025-11-03 10:59:35 EST (in 3 years)
✓ This certificate is valid

What to do next

- Enable sending Data Plane event logs using Configure Secure Firewall Management Center to Send Data Plane Event Logs to Secure Network Analytics using Syslog, on page 21.
- After you have confirmed that events are successfully being stored on your Secure Network Analytics appliance, allow time to pass until you are certain that all events stored on your management center are also available remotely. Then see Stop Storing Low-Priority Connection Events on the Management Center.

Note If you need to change any of these configurations, run the wizard again. If you disable the configuration or run the wizard again, all settings except the account credentials are retained.

Configure Secure Firewall Management Center to Send Data Plane Event Logs to Secure Network Analytics using Syslog

The following describes how to configure the management center to send data plane event logs to Secure Network Analytics using syslog, in the UI options in appliance Platform Settings Policy.

Note Data Plane events are supported on the Security Analytics and Logging (OnPrem) Data Store deployment.

Before you begin

Make sure you enable sending Data Plane event logging to Secure Network Analytics using the Configure the Wizard in Secure Firewall Management Center in the management center.

Step 1 Enable logging.

a) Go to **Syslog** > **Logging Setup** > **Basic Logging Settings**.
b) Check the **Enable Logging** check box.

Step 2 Configure logging trap.

a) Go to **Syslog** > **Logging Destinations**.
b) Click **+ Add Logging Destination**.
c) For **Logging Destionation**, select **Syslog Servers**.
d) For **Event Class**, select **Filter on Severity**.
e) Choose any severity.

Step 3 Configure logging facility.

a) Go to **Syslog** > **Syslog Settings** > **Facility**.
b) For **Facility**, select **default = LOCAL4(20)**.

Stop Storing Low-Priority Connection Events on the Management Center

The vast majority of connection events are not associated with identified threats. You can choose not to store this large volume of events on your management center.

Events that are not stored on your management center do not count against the maximum flow rate for your management center appliance, as specified in the data sheet at https://www.cisco.com/c/en/us/products/collateral/security/%20firesight-management-center/datasheet-c78-736775.html.

The following connection events are considered high priority and are always stored on the management center, even if you disable storage of connection events:

- Security events
- Connection events associated with intrusion events
- Connection events associated with file events
- Connection events associated with malware events

Not storing low priority connection events on your management center allows you to allocate more storage space to other event types, increasing your time window for investigating threats. This setting does not affect statistics collection.

This setting applies to events from all devices managed by this management center.

Before you begin

Caution This procedure will immediately permanently delete all connection events currently stored on your management center.

Before performing this procedure, ensure that all low priority connection events that you want to keep already exist on your Secure Network Analytics appliance. Generally, we recommend enabling this option some time after you have confirmed that your management center is successfully sending events to Secure Network Analytics.

Step 1 There are two ways to stop storing low priority connection events on the management center:

Both methods have the same effect.

- After you complete the wizard to send events to Security Analytics and Logging (OnPrem), go to **System > Logging > Security Analytics and Logging**, enable the option to **Store Fewer Events on FMC**.
- Go to **System** > **Configuration** > **Database**, look for the **Connection Database** section, and set **Maximum Connection Events** to zero (`0`).

  Setting this value to anything other than 0 counts all low priority connection events toward the maximum flow rate. This setting does not affect connection summaries.

Step 2 Save your changes.

What to do next

Increase the storage limits for all other event types on the **System** > **Configuration** > **Database** page.

ASA Devices Configuration

The ASA system logs provide you with information for monitoring and troubleshooting the ASA devices. For list of ASA event types, see Cisco ASA Series Syslog Messages.

Note ASA event storage is supported on the Security Analytics and Logging (OnPrem) Data Store deployment.

To have ASA send the syslog events to Security Analytics and Logging (OnPrem), you must configure logging on the ASA device:

- Enable logging

- Configure output destination to Secure Network Analytics Flow Collector

Note Secure logging is not supported for Security Analytics and Logging (OnPrem).

CLI Commands to Send Syslog Events from ASA Devices

Use the following configuration commands to send syslog messages for security events from ASA devices to Security Analytics and Logging (OnPrem).

Before you begin

- Review the requirements and prerequisites section.
- Confirm that your ASA devices can reach your Flow Collector.
- Obtain the Flow Collector IP address and port number from Central Management on your Manager.

Step 1 Enable logging:

logging enable

Example:

```
ciscoasa(config)# logging enable
```

Step 2 Specify which syslog messages should be sent to syslog server (Flow Collector):

logging trap {*severity_level* | *message_list*}

Example:

You can specify the severity level number (1 through 7) or name of the syslog messages to send to Flow Collector:

```
ciscoasa(config)# logging trap errors
```

Example:

Alternatively, you can specify a custom message list that identifies the syslog messages to send to Flow Collector:

```
ciscoasa(config)# logging list specific_event_list message 106100
ciscoasa(config)# logging list specific_event_list message 302013-302018
ciscoasa(config)# logging trap specific_event_list
```

Step 3 Configure the ASA to send messages to Flow Collector:

logging host *interface_name syslog_ip* [**protocol**/*port*]

Example:

```
ciscoasa(config)# logging host management 209.165.201.3 17/8514
```

Note

a. For the syslog ip and port, specify the Flow Collector IP and the corresponding syslog port number (for instructions, refer to the Before you begin section).

b. Specify *17* to denote UDP protocol.

Step 4 (Optional) Configure timestamp format in Syslog messages:

logging timestamp *{rfc5424}*

Example:

```
ciscoasa(config)# logging timestamp
ciscoasa(config)# logging timestamp rfc5424
```

The timestamp format specified in RFC5424 is yyyy-MM-THH:mm:ssZ, where the letter Z indicates the UTC time zone.

Note RFC5424 is supported only from ASA 9.10(1).

Step 5 (Optional) Configure ASA to display syslog messages with device ID:

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

Example:

```
ciscoasa(config)# logging device-id context-name
```

The syslog server uses the device ID to identify the syslog generator. You can specify only one type of device ID for syslog messages.

ASDM Configuration to Send Syslog Events from ASA Devices

Use the following procedure to configure ASDM to send ASA syslog messages for security events to Security Analytics and Logging (OnPrem).

Before you begin

- Review the requirements and prerequisites section.
- Confirm that your ASA devices can reach your Flow Collector.
- Obtain the Flow Collector IP address and port number from Central Management on your Manager.

Step 1 Log in to ASDM.

Step 2 Enable logging.

a) Click **Configuration** > **Device Management** > **Logging** > **Logging Setup**.
b) Check the **Enable logging** check box to turn on logging.
c) (Optional) Check the **Send syslogs in EMBLEM** check box to enable EMBLEM logging format.

Step 3 Configure the logging filter settings for the syslog server (Flow Collector).

a) Choose **Configuration** > **Device Management** > **Logging** > **Logging Filters**.

b) From the table, select **Syslog Servers**, and then click **Edit**.

c) In the **Edit Logging Filters** dialog box, select one of the following logging filter settings:

To filter the syslog messages based on the severity levels, click **Filter on severity**, and then choose the severity level.

Note ASA generates system log messages with severity levels up to the specified level.

OR

To filter the syslog messages based on the message IDs, click **Use event list**. You can choose an event list that is created with the required syslog message IDs, or click **New** to create a list with the syslog messages IDs or range of IDs.

d) Save your settings.

Step 4 Configure the external syslog server with your Flow Collector address and port.

a) Choose **Configuration** > **Device Management** > **Logging** > **Syslog Server**.

b) Click **Add** to add a new syslog server.

c) In the **Add Syslog Server** dialog box, specify the following:

- **Interface**—The interface that will be used to communicate to the syslog server.
- **IP Address**—The Flow Collector IP obtained from Central Management on your Manager.
- **Protocol**—Select UDP.
- **Port**—The corresponding Flow Collector syslog port (8514 by default).
- (Optional) Check the **Log messages in Cisco EMBLEM format** check box to enable EMBLEM logging format.

Step 5 Click **Save** to apply changes to the configuration.

CSM Configuration to Send Syslog Events from ASA Devices

Use the following procedure to configure Cisco Security Manager (CSM) to send ASA syslog messages for security events to Security Analytics and Logging (OnPrem).

Before you begin

- Review the requirements and prerequisites section.
- Confirm that your ASA devices can reach your Flow Collector.
- Obtain the Flow Collector IP address and port number from Central Management on your Manager.
- Secure logging is not supported for this integration.

Step 1 Log in to **Configuration Manager** window of Cisco Security Manager.

Step 2 Enable syslog logging.

a) To access the Syslog Logging Setup page, do one of the following:

- (Device view) Choose **Platform** > **Logging** > **Syslog** > **Logging Setup** from the Policy selector.
- (Policy view) Choose **Router Platform** > **Logging** > **Syslog** > **Logging Setup** from the Policy Type selector. Select an existing policy or create a new one.

b) In the Syslog Logging Setup page, check the **Enable Logging** check box to turn on syslog logging.

c) (Optional) Check the **Send syslogs in EMBLEM** check box to enable EMBLEM logging format.

d) Click **Save**.

Step 3 Configure the logging filter settings for the syslog server (Flow Collector).

a) Choose **Platform** > **Logging** > **Syslog** > **Logging Filters** from the Policy selector.

b) From the table, select **Syslog Servers** under the **Logging Destination** column, and then click **Edit**. If the Syslog Servers object is not found, click **Add Row**.

c) In the **Add/Edit Logging Filters** dialog box, select one of the following logging filter settings:

- To filter the syslog messages based on the severity levels, click **Filter on severity**, and then choose the severity level.

  Note ASA generates system log messages with severity levels up to the specified level.

- To filter the syslog messages based on the message IDs, click **Use event list** and from the drop-down list, select the event list of your choice.

  Note The drop-down list will be blank if you have not defined any event list. You must define at least one event list (**Platform** > **Logging** > **Syslog** > **Event Lists**).

d) Save your settings.

Step 4 (Optional) Configure logging parameters:

a) (Device view) Choose **Platform** > **Logging** > **Syslog** > **Server Setup**.

b) To configure timestamp format in syslog messages, check the **Enable Timestamp on Each Syslog Message** check box, and then check the **Enable Timestamp Format(rfc5424)** check box.

Note RFC5424 is supported only from ASA 9.10(1).

c) (Optional) Configure ASA to display syslog messages with device ID:

- **Interface**—Click this radio button and select an interface of the ASA device.
- **User Defined ID**—Click this radio button and enter a desired name to be added to all syslog messages of the ASA device.
- **Host Name**—Click this radio button to display syslog messages with the device hostname.

Note The syslog server uses the device ID to identify the syslog generator. You can specify only one type of device ID for syslog messages.

d) Click **Save**.

Step 5 Configure the external logging server to which the syslog messages are to be sent.

a) To access the Syslog Servers page, do one of the following:

- (Device view) Select **Platform** > **Logging** > **Syslog Servers** from the Policy selector.

- (Policy view) Select **Router Platform** > **Logging** > **Syslog Servers** from the Policy Type selector. Select an existing policy or create a new one.

b) Click **Add** to add a new syslog server.

c) In the **Add/Edit Syslog Server** dialog box, specify the following:

- **Interface**—The interface that is used to communicate to the syslog server
- **IP Address**—The Flow Collector IP obtained from Central Management on your Manager.
- **Protocol**—Select UDP.
- **Port**—The corresponding Flow Collector syslog port (8514 by default).
- (Optional) Check the **Log messages in Cisco EMBLEM format** check box to enable EMBLEM logging format.

d) Click **OK** to save your configuration and close the dialog box. The syslog server you defined is displayed in the table.

Step 6 Submit and deploy the configuration changes.

CHAPTER 3

Next Steps

Next Steps

After you configure your Firewall devices to send event data to your Secure Network Analytics appliance as part of Security Analytics and Logging (OnPrem), you can take the following steps:

- Review the management center online help.
- Review the Manager Web App online help to learn more about Secure Network Analytics.

Work in the Management Center with Connection Events Stored on a Secure Network Analytics Appliance

If your devices are sending connection events to a Secure Network Analytics appliance using Security Analytics and Logging (OnPrem), you can view and work with these remotely stored events in the management center's event viewer and context explorer, and include them when generating reports. You can also cross-launch from an event in the management center to view related data on your Secure Network Analytics appliance.

By default, the system automatically selects the appropriate data source based on the time range you specify. If you want to override the data source, use this procedure.

Important When you change the data source, your selection persists across all of the relevant analytics features that rely on the event data source, including reports, until you change it, even after you sign out. Your selection does not apply to other management center users.

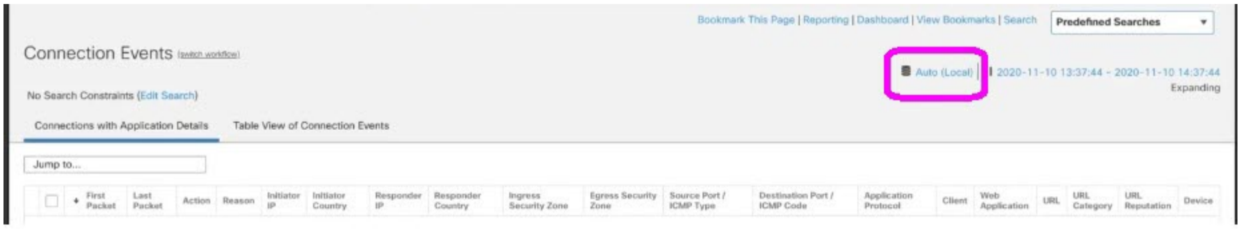
The selected data source is used for low-priority connection events only. All other event types (intrusion, file, and malware events; connection events associated with those events; and Security Intelligence events) are displayed regardless of data source.

Before you begin

You have used the wizard to send connection events to Security Analytics and Logging (OnPrem).

Step 1 In the management center web interface, navigate to a page that displays connection event data, such as **Analysis** > **Connections** > **Events**.

Step 2 Click the data source displayed here and select an option:



Caution If you select **Local**, the system displays only the data available on the management center, even if local data is not available for the entire time range selected. You will not be notified that this situation is occurring.

Step 3 (Optional) To view related data directly in your Secure Network Analytics appliance, right-click (in the unified event viewer, click) a value such as an IP address or domain and choose a cross-launch option.

Investigate Events Using Cross-launch

When viewing events in themanagement center, you can right-click certain event data (for example, an IP address) and view related data in Manager.

Step 1 Navigate to one of the following pages in the management center that shows events:

- A dashboard (**Overview** > **Dashboards**), or
- An event viewer page (any menu option under the Analysis menu that includes a table of events).

Step 2 Right-click the event field of interest and choose the Security Analytics and Logging (OnPrem) cross-launch resource. The Manager opens in a separate browser window. You may be prompted for a username and password if you are not already logged in. It may take some time for the query to be processsed, depending on the amount of data to be queried, speed of and demand on the Manager, and so on.

Step 3 Sign into the Manager.

APPENDIX A

Troubleshooting

Troubleshooting

Security Analytics and Logging (OnPrem) General Troubleshooting Information

On the Manager, the following log files contain troubleshooting information related to Security Analytics and Logging (OnPrem):

- `/lancope/var/logs/containers/sal.log` - general app logging information (Manager only deployment only)
- `/lancope/var/logs/sal_preinstall.log` - information specific to the app installation process

On the Flow Collector, the following log files contain troubleshooting information related to Security Analytics and Logging (OnPrem) Data Store deployment:

- `/lancope/var/sw/today/logs/sw.log` - information specific to telemetry logging
- `/lancope/var/logs/containers/svc-db-ingest.log` - information specific to event ingestion and the database

Security Analytics and Logging (OnPrem) Configuration Using Flow Collector Advanced Settings (Data Store Only)

If you configured your Flow Collector(s) to not store Firewall Logs during First Time Setup, you can update your ingest settings using the Flow Collector Advanced Settings page. To access Advanced Settings:

1. Log in to your Flow Collector (formerly known as Appliance Administration (Admin) interface).
2. Click **Support** > **Advanced Settings**.
3. In the **enable_sal** field, enter 1 to enable ingest of Firewall event logs.
4. If you want to change the port for Firewall logs, enter the new value in the **sal_syslog_port** field (default port is 8514).
5. Click **Apply** and then click **OK**.

Security Analytics and Logging (OnPrem) App Install Failure on Manager Only Deployment

We support installing the app on an Manager as a standalone appliance (Manager only), or an Manager that manages Flow Collector(s) and Data Node(s) (Data Store). You cannot install the app on a Manager if it manages one or more Flow Collectors and does not manage a Data Store. If you attempt to install the app in this situation, then the installation fails. To verify that this is the cause, review the log file at `/lancope/var/logs/sal_preinstall.log`. If you see the following message or similar, then the installation detected a managed Flow Collector:

```
Checking flow collectors...
1 Flow Collector(s) detected
Flow Collector(s) are present in inventory -- aborting installation.
```

To install the app, remove all managed Flow Collectors from the Central Manager Appliance Inventory, then try again.

Security Analytics and Logging (OnPrem) App Dropping Events

The app may drop events in the following situations:

- You export all event types in syslog, instead of only connection, file, malware, and intrusion events.
- Your average events per second (EPS) ingest rate or burst EPS ingest rate exceeds the recommended specifications in the Secure Network Analytics Resource Allocation section.

For Manager only deployment, review the information in the Manager `/lancope/var/logs/containers/sal.log` log file to determine whether the app is dropping events. Search the file for entries containing "`events_dropped:`".

For Data Store deployment, review the information in the Flow Collector `lancope/var/sw/today/logs/sw.log` log file to determine whether the app is dropping events. Search the file for entries containing "`sal_event`".

Contact Cisco Support if this behavior persists.

Security Analytics and Logging (OnPrem) App Crash

If the Security Analytics and Logging (OnPrem) app crashes (due to an excessive ingest rate, for example), restart the Manager. This also restarts the app.