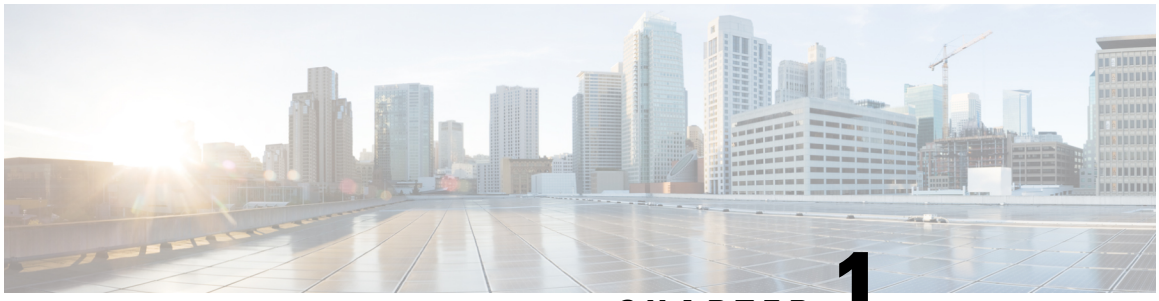
Cisco Security Analytics and Logging (On Premises) for Secure Network Analytics 7.5.3: Firewall Event Integration Guide

First Published: 2025-08-25

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

CONTENTS



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 Firewall 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 Firewall 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

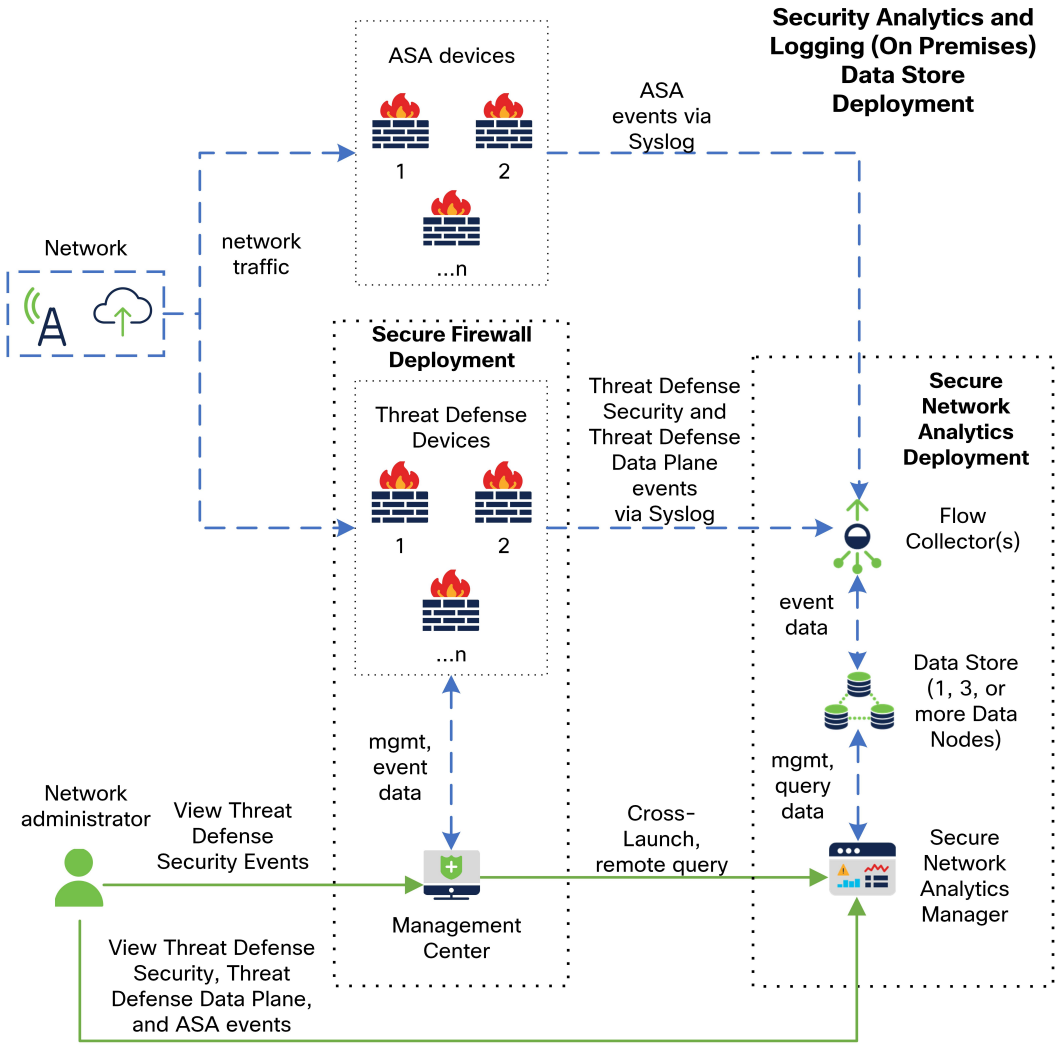
In a Security Analytics and Logging (OnPrem) deployment, you can use a Secure Network Analytics appliance to store data from another Cisco product deployment. In the case of the Secure Firewall deployment, you can export your Security Events and data plane events from your Secure Firewall Threat Defense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

You can deploy Secure Network Analytics as follows:

- 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

Data Store

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

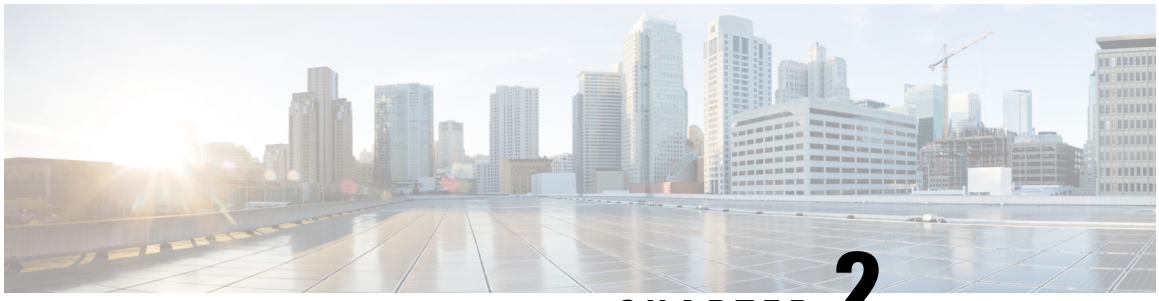


In this deployment, the Firewall Threat Defense and Secure Firewall ASA devices send Firewall events to the Flow Collector. The Flow Collector sends the events to the Data Store for storage. From the Firewall Management Center UI, users can cross-launch to the Manager to view more information about the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

Supported Event Types

- Firewall Threat Defense Security events

    - Connection
    - Intrusion
    - File and Malware
- Threat Defense Data Plane events
- ASA events



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:

Table 1: 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 Firewall Management Center running earlier versions, see https://cisco.com/go/sal-on-prem-docs.	none	• You can deploy one Manager per Firewall Management Center, and optionally multiple Flow Collectors and Data Nodes.

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Secure Firewall managed devices	v7.0+ using the wizard Firewall Threat Defense v6.5 or later using syslog NGIPS v6.5 using syslog	none	• For instructions on how to use syslog for the Firewall Threat Defense v6.5, see Sending Events from Threat Defense Devices On Earlier Versions.
ASA devices	v9.12+	none	

Secure Network Analytics Appliances

You can deploy Secure Network Analytics as follows:

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

Table 2: Data Store

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.5.3	none	• Secure Network Analytics v7.5.3 is required for Single Node Data Store and multi-telemetry,

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Flow Collector	Secure Network Analytics v7.5.3	none	• You can deploy up to 5 Flow Collectors that are configured for Data Store. • The Flow Collector can receive events from multiple Firewall Threat Defense devices, all managed by one Firewall Management Center. • The Flow Collector can receive ASA events from multiple ASA devices. • Secure Network Analytics v7.5.3 is required for Single Node Data Store and multi-telemetry.
Data Store	Secure Network Analytics v7.5.3	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 v7.5.3 is required for Single Node Data Store and multi-telemetry.

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 no longer need to purchase a separate license for Security Analytics and Logging (OnPrem) telemetry starting with v7.5.3. Security Analytics and Logging (OnPrem) traffic is now included along with NetFlow, Zeek, and NVM when calculating Flow Rate (FPS) licensing requirements.

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 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 150k EPS on average with Security Analytics and Logging (OnPrem) and `sal_to_flow_cache` ON

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

Firewall Event Logs for Network Detections

We have added network detections based on Cisco Security Analytics and Logging (On Premises) data. If you enable this configuration, you will have more insight into your traffic patterns, risks, and the scope of an attack.

You can enable or disable the ingest of Firewall event logs using the `sal_to_flow_cache` toggle in the advanced setttings in the Flow Collector Admin UI. This is used to enable or disable network detections when you already have Firewall logs ingest enabled.

For more information about editing advanced settings on the Flow Collector, refer to the *Advanced Settings* Help topic.

Note The `sal_to_flow_cache` option is optional and only needed if you want Security Analytics and Logging (On Premises) data to be part of the flow cache for enhanced detections.

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 v7.5.3.

Table 3: Manager VE

Resource	Recommendation
CPUs	12
RAM	70 GB
Hard drive storage	480 GB

Table 4: Flow Collector VE

Resource	Recommendation
CPUs	8
RAM	64 GB
Hard drive storage	500 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:

Table 6: Estimated Retention

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

Average EPS	Average Daily Events	Virtual	Hardware
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 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
Firewall Management Center, Firewall 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	Firewall Management Center and Manager	443/TCP	Logging into the appliances' web interfaces over HTTPS using a web browser
Firewall Threat Defense devices managed by a Firewall Management Center	Flow Collector	8514/UDP	Syslog export from the Firewall Threat Defense devices, ingest to Flow Collector

From (Client)	To (Server)	Port	Protocol or Purpose
ASA devices	Flow Collector	8514/UDP	Syslog export from ASA devices, ingest to Flow Collector
Firewall Management Center	Manager	443/TCP	Remote query from the Firewall 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 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.
Configure the Firewall Management Center to send events to Security Analytics and Logging (OnPrem)	You have the following options: • Configure the Firewall Management Center to send events to your Secure Network Analytics appliance using the Secure Firewall Management Center Configuration, on page 13 section. • Configure Data Plane event logging using the Configure Data Plane Event Logs section. • Reduce logging load on the Firewall Management Center using the Stop Storing Low-Priority Connection Events on the Secure Firewall 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 18 section.
Review Next Steps	Review the Next Steps: • Review the Secure Firewall online help for more information. See Work in Secure Firewall Management Center with Connection Events Stored on a Secure Network Analytics appliance.. • Review the Manager online help for more information on how to use Secure Network Analytics. Go to **Investigate** > **Security Analytics and Logging (OnPrem)**.

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:
   - Data Store Deployment and Configuration, on page 12

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 Firewall Threat Defense device's management IP addresses, and that the Manager management IP address is reachable by your Firewall 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.

Procedure

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.

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 Firewall Management Center to send events directly to Secure Network Analytics deployment.
- Configure Data Plane event logging.

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.

- 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 Firewall Management Center; they are used once in order to establish a read-only analyst API account for the Firewall 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 Data Store Deployment

Before you begin

- Ensure that you meet all the requirements that are mentioned in Prerequisites for Secure Firewall Integration.
- The managed device version is 7.0 or later.

Procedure

Step 1 In the Firewall 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**.

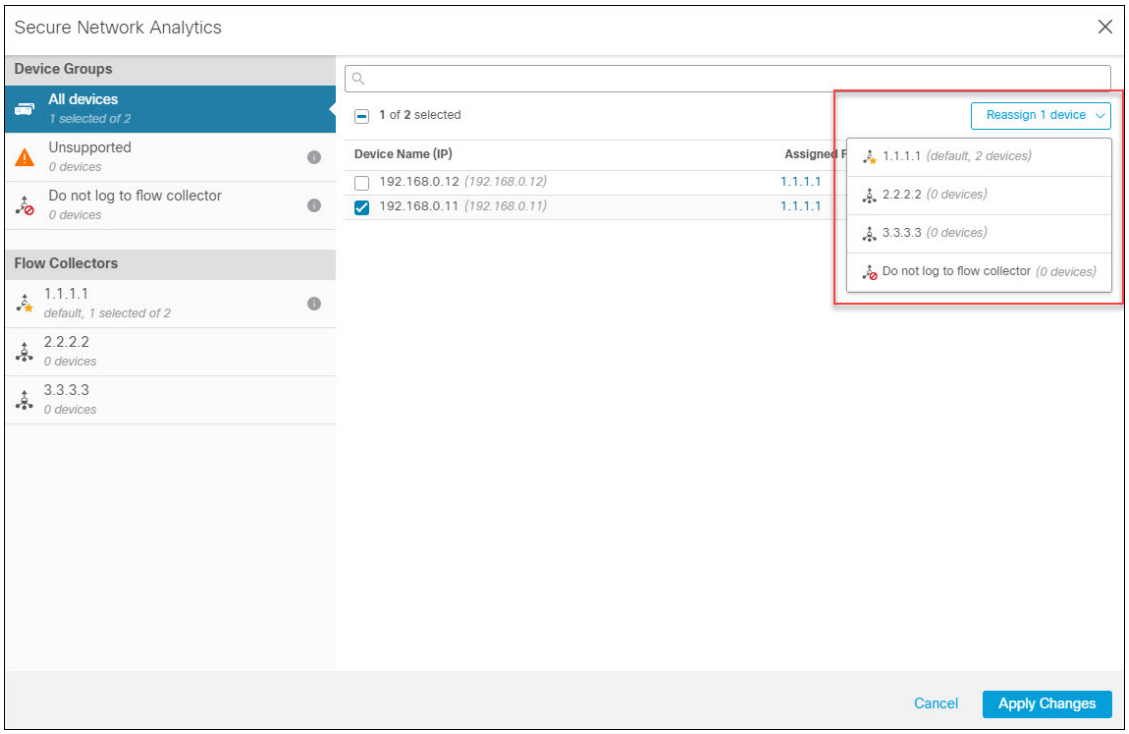
Step 5 (Optional) If you have configured more than one Flow Collector, associate the managed devices with different Flow Collectors.

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

a. Click **Assign Devices**.

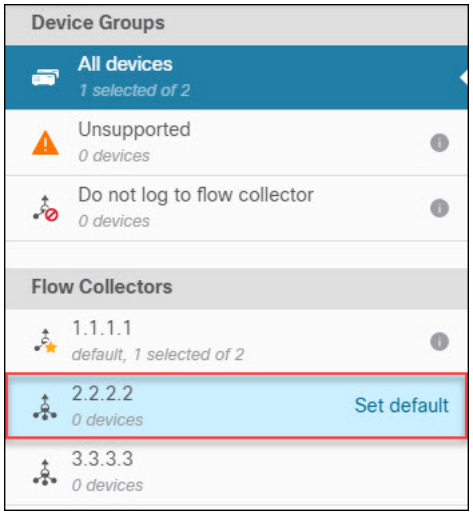
b. Select the managed devices that you want to reassign.

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



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.

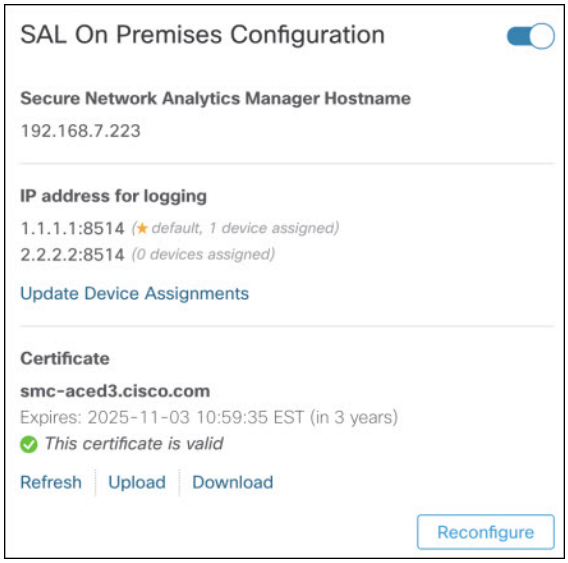
Note
For more information on how to obtain and upload SSL certificate, see Cisco Secure Network Analytics: SSL/TLS Certificates for Managed Appliances.

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 Firewall Management Center; they are used once to establish a read-only analyst API account for the Firewall 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.



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 17.
- 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 Firewall Management Center are also available remotely. Then see Stop Storing Low-Priority Conneciton Events on the Firewall 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 Firewall 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 Wizard in the Firewall Management Center.

Procedure

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 Firewall 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 Firewall Management Center.

Events that are not stored on your Firewall Management Center do not count against the maximum flow rate for your Firewall 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 Firewall 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 Firewall 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 Firewall Management Center.

Before you begin

Caution This procedure will immediately permanently delete all connection events currently stored on your Firewall 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 Firewall Management Center is successfully sending events to Secure Network Analytics.

Procedure

Step 1 There are two ways to stop storing low priority connection events on the Firewall 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.

Procedure

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.

Procedure

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.

Procedure

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.

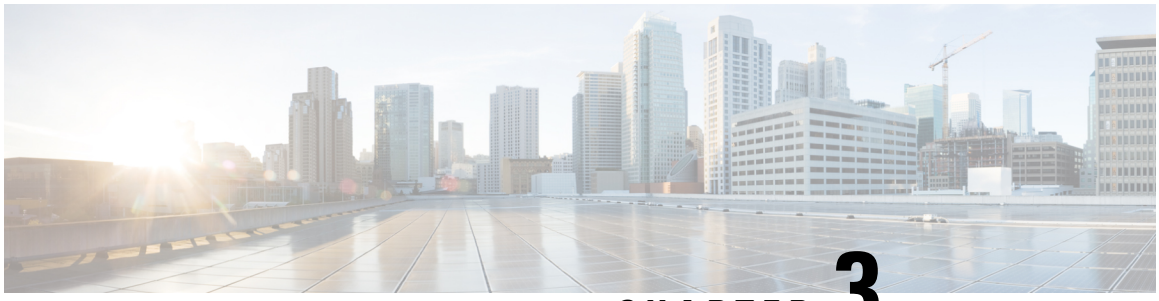
b) Click **Add** to add a new syslog server.

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 Firewall Management Center online help.
- Review the Manager online help to learn more about Secure Network Analytics. Go to **Investigate** > **Security Analytics and Logging (OnPrem)**.

Work in the Firewall 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 Firewall Management Center's event viewer and context explorer, and include them when generating reports. You can also cross-launch from an event in the Firewall 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 Firewall 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.

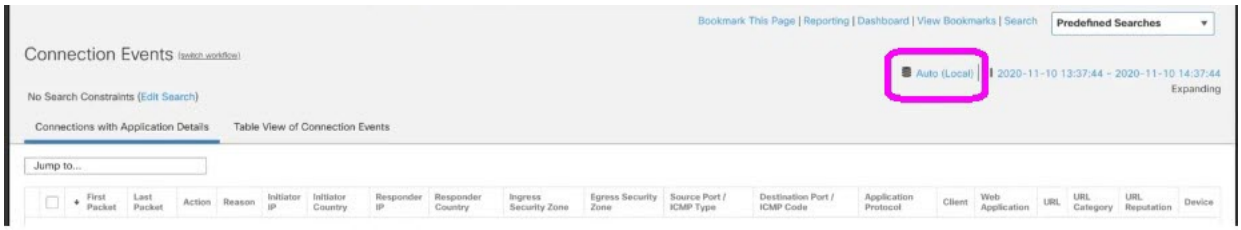
Before you begin

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

Procedure

Step 1 In the Firewall 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 Firewall 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 theFirewall Management Center, you can right-click certain event data (for example, an IP address) and view related data in Manager.

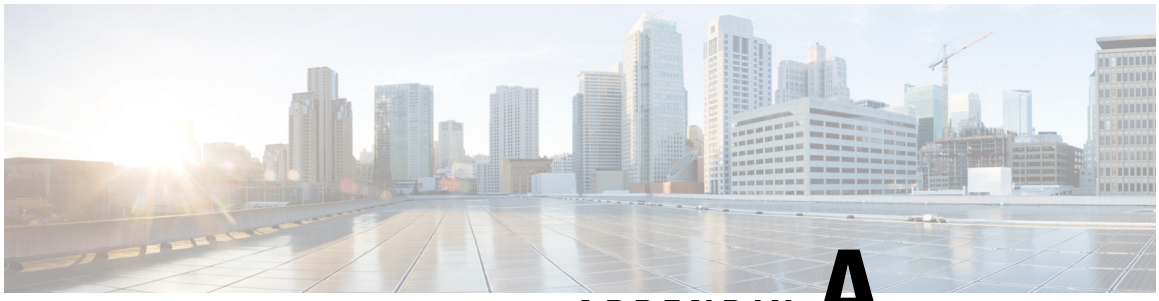
Procedure

Step 1 Navigate to one of the following pages in the Firewall 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 file contains troubleshooting information related to Security Analytics and Logging (OnPrem):

- `/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**.

Troubleshooting