



Deployment

- Requirements and Best Practices, on page 1
- Configuration Overview, on page 9
- Manager Configuration, on page 11
- Firepower Configuration, on page 12
- ASA Devices Configuration, on page 20

Requirements and Best Practices

The following lists the requirements and best practices 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 Cisco Security Analytics and Logging (On Premises)	Notes
Firepower Management Center (hardware or virtual)	v7.0+ For Firepower Management Center running earlier versions, see https://cisco.com/go/sal-on-prem-docs .	none	<ul style="list-style-type: none"> • can deploy one Manager per Firepower Management Center, and optionally one Flow Collector and one Data Store (3 Data Nodes)
Firepower managed devices	v7.0+ using the wizard Firepower Threat Defense v6.4 or later using syslog NGIPS v6.4 using syslog	none	

Solution Component	Required Version	Licensing for Cisco Security Analytics and Logging (On Premises)	Notes
ASA devices	v9.12+	none	<ul style="list-style-type: none">supported on Security Analytics and Logging (OnPrem) app v3.0.0+ and Secure Network Analytics v7.4.0+ Multi-node deployment

Secure Network Analytics Appliances

You have the following options for deploying Secure Network Analytics:

- **Single-node** - Deploy only a Manager to ingest and store events, and review and query events
- **Multi-node** - Deploy a Flow Collector to ingest events, Data Store to store events, and Manager to review and query events



Note You cannot deploy a mix of Secure Network Analytics hardware and Secure Network Analytics VE appliances.

Table 1: Single-node

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.3.1+	none	<ul style="list-style-type: none"> • can deploy either an Manager 2210 hardware appliance or Manager Virtual Edition (VE) appliance • can receive events from multiple Firepower Threat Defense devices, all managed by one Firepower Management Center • must install the Security Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events in the Manager Web App
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v2.0+	Logging and Troubleshooting Smart License, based on GB/day	Install this app on the Manager and configure to enable event ingest

Table 2: Multi-node

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.3.2+	none	<ul style="list-style-type: none"> • can deploy either an Manager 2210 hardware appliance or Manager Virtual Edition (VE) appliance • must install theSecurity Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events in the Manager Web App
Flow Collector	Secure Network Analytics v7.3.2+	none	<ul style="list-style-type: none"> • can deploy either a Flow Collector 4210 hardware appliance or Flow Collector VE appliance • can receive events from multiple Firepower Threat Defense devices, all managed by one Firepower Management Center • can receive ASA events from multiple ASA devices (v7.4+)
Data Store (3 Data Nodes)	Secure Network Analytics v7.3.2+	none	<ul style="list-style-type: none"> • can deploy either a Data Store 6200 (3 Data Nodes) hardware or Data Store VE (3 Data Nodes VE) • can store Firewall events received by the Flow Collector

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v2.0+	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 Firepower 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) Single-node 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) Multi-node deployment can ingest up to roughly 50k EPS on average, with short bursts of up to 175k EPS
- a hardware Multi-node deployment 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; see [Troubleshooting](#) for more information.

Single-node VE Recommendations

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

Based on the storage space that you allocate, you can store your data for roughly the following time frames on a Single-node 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
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 4 TB, you may note unanticipated errors due to insufficient resource allocation.

Multi-node Recommendations

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

Table 3: Manager VE

Resource	Recommendation
CPUs	8 Intel Xeon, minimum 2.29 GHz
RAM	64 GB
Hard drive storage	480 GB

Table 4: Flow Collector VE

Resource	Recommendation
CPUs	8 Intel Xeon, minimum 2.29 GHz
RAM	70 GB
Hard drive storage	480 GB

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

Resource	Recommendation
CPUs	12 Intel Xeon, minimum 2.29 GHz 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

Based on the storage space that you allocate, you can store your data for roughly the following time frames on your Multi-node 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	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.



Note We have tested these 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 storage allocation beyond 4 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 Single-node deployment.

From (Client)	To (Server)	Port	Protocol or Purpose
External internet (NTP server)	FMC, FTD devices, and Manager	123/UDP	NTP time synchronization, all to the same NTP server
User workstations	FMC and Manager	443/TCP	Logging into the appliances' web interfaces over HTTPS using a web browser
FTD devices managed by a FMC	Manager	8514/UDP	Syslog export from the FTD devices, ingest to the Manager
FMC	Manager	443/TCP	remote query from FMC to the Manager

The following table lists the communication ports you must open for the Security Analytics and Logging (OnPrem) integration for a Multi-node deployment. In addition, see the [Data Store Hardware Deployment and Configuration Guide](#) or the [Data Store Virtual Edition Deployment and Configuration Guide](#) for the ports you must open for your Secure Network Analytics deployment.

From (Client)	To (Server)	Port	Protocol or Purpose
External internet (NTP server)	FMC, FTD devices, Manager, Flow Collector, and Data Store	123/UDP	NTP time synchronization, all to the same NTP server
user workstations	FMC and Manager	443/TCP	Logging into the appliances' web interfaces over HTTPS using a web browser
FTD devices managed by a FMC	Flow Collector	8514/UDP	Syslog export from the FTD devices, ingest to Flow Collector
ASA devices	Flow Collector	8514/UDP	Syslog export from ASA devices, ingest to Flow Collector
FMC	Manager	443/TCP	Remote query from the FMC 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 Single-node	<p>You have the following options:</p> <ul style="list-style-type: none"> • 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 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 Installation Guide for more information. <p>See Single-node Deployment and Configuration for more information.</p>
Deploy Multi-node	<p>You have the following options:</p> <ul style="list-style-type: none"> • Deploy a hardware Manager, Flow Collector, and 3 Data Nodes to your network. Perform initial configuration for each appliance, and initialize the Data Store. See x2xx Series Hardware (with Data Store) Appliance Installation Guide for more information. • Download the Manager VE ISO, Flow Collector VE ISO, and Data Node ISO. Deploy one Manager VE, one Flow Collector VE, and 3 Data Nodes VE to your hypervisor. Perform initial configuration for each appliance, and initialize the Data Store. See Virtual Edition (with Data Store) Appliance Installation Guide for more information. <p>See Multi-node Deployment and Configuration for more information.</p>
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.	<ul style="list-style-type: none"> • On the Manager, go to App Manager in Central Management and download the app. Configure it to receive events from Firepower devices. • See the Security Analytics and Logging (OnPrem) release notes and app help for more information on using the app. <p>See Manager Configuration for more information.</p>

Component and Task	Steps
Configure the Firepower Management Center to send events to Security Analytics and Logging (OnPrem)	<p>You have the following options:</p> <ul style="list-style-type: none"> • Configure the Firepower Management Center to send events to your Secure Network Analytics appliance. See Configure the Wizard in FMC, on page 13 if your devices are running Firepower 7.0+, or For Managed Devices Running Versions Earlier than 7.0, Use Syslog, on page 15. • Configure Data Plane event logging using the Configure Firepower Management Center to Send Events to Secure Network Analytics using Syslog section. • Reduce logging load on the Firepower Management Center using the Stop Storing Low-Priority Connection Events on the FMC section.
Configure ASA devices to send events to Security Analytics and Logging (OnPrem)	<ul style="list-style-type: none"> • Configure your ASA devices to send events to your Secure Network Analytics appliance. See ASA Devices Configuration, on page 20. • ASA events are supported on Security Analytics and Logging (OnPrem) app v3.0.0+ and Secure Network Analytics v7.4.0+ Multi-node deployment.
Review Next Steps	<p>Review the Next Steps:</p> <ul style="list-style-type: none"> • Review the Firepower online help for more information. See Work in Firepower 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.

Single-node 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 FMC's management IP address and your FTD device's management IP addresses. Note the management IP address for further configuration. See the [Secure Network Analytics Virtual Edition 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.

Procedure

Follow the instructions in the [Secure Network Analytics Virtual Edition Installation Guide](#) to deploy your Manager VE, or the [x2xx Series Hardware Installation Guide](#) and [Secure Network Analytics System Configuration Guide](#) if you are deploying a Manager 2210.

Note We support installing the app on an Manager as a standalone appliance (Single-node), or an Manager that manages a Flow Collector and 3 Data Nodes (Multi-node). You cannot install the app on an Manager if it manages one or more Flow Collectors without managing 3 Data Nodes. See [Troubleshooting](#) for more information.

Multi-node Deployment and Configuration



Important

After you choose to configure your Manager or Flow Collector for use with Security Analytics and Logging (OnPrem), you cannot update the appliance's configuration to change this. You must RFD the appliance if you select the wrong choice. Enable this only if you plan to use Secure Network Analytics for Security Analytics and Logging (OnPrem) to store your Firewall event information.

Before you begin

- Ensure that you have deployed a Manager, Flow Collector, and 3 Data Nodes (v7.3.2+) to your network, that the Flow Collector management IP address is reachable by your Firepower Threat Defense devices' management IP addresses, and that the Manager management IP address is reachable by your Firepower 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

Follow the instructions in [x2xx Series Hardware \(with Data Store\) Appliance Installation Guide](#) to deploy your Secure Network Analytics hardware appliances, or [Virtual Edition \(with Data Store\) Appliance Installation Guide](#) to deploy your Secure Network Analytics virtual appliances.

Note We support installing the app on an Manager as a standalone appliance (Single-node), or an Manager that manages a Flow Collector and 3 Data Nodes (Multi-node). You cannot install the app on an Manager if it manages one or more Flow Collectors without managing 3 Data Nodes. See [Troubleshooting](#) for more information.

Manager Configuration

To configure your Secure Network Analytics deployment for Security Analytics and Logging (OnPrem), install the Security Analytics and Logging (OnPrem) app on the Manager. This configures your Manager to receive events from your Firewall devices.



Note We support installing the app on an Manager as a standalone appliance (Single-node), or an Manager that manages a Flow Collector and 3 Data Nodes (Multi-node). You cannot install the app on an Manager if it manages one or more Flow Collectors without managing 3 Data Nodes. See [Troubleshooting](#) for more information.

Installing 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.

Procedure

- 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** Click the **Global Settings** icon.
- Step 4** Select **Central Management**.
- Step 5** Click the **App Manager** tab.
- Step 6** Click **Browse**.
- Step 7** Follow the on-screen prompts to upload the app file.

What to do next

- Configure the FMC to send events to your Secure Network Analytics appliance. See [Configure the Wizard in FMC, on page 13](#) if your devices are running Firepower 7.0+, or [For Managed Devices Running Versions Earlier than 7.0, Use Syslog, on page 15](#).
- Configure your ASA devices to send events to your Secure Network Analytics appliance. See [ASA Devices Configuration, on page 20](#).



Caution Uninstalling the Security Analytics and Logging (OnPrem) app removes all related information, including Firewall event data, from your Manager. If you have a Single-node deployment, it also removes the standalone Manager restriction. After you uninstall the Security Analytics and Logging (OnPrem) app, you can then manage one or more Flow Collectors with your standalone Manager as part of a traditional Secure Network Analytics deployment to inspect traffic.

Firepower Configuration

When you configure Firepower for Security Analytics and Logging (OnPrem), you have the following options:

- If your Firepower Threat Defense devices are running Firepower 7.0+, use the configuration wizard. See [Configure the Wizard in FMC](#) for more information.
- If your Firepower Threat Defense devices are running Firepower 6.4 to 6.8, manually configure syslog export. See [For Managed Devices Running Versions Earlier than 7.0, Use Syslog, on page 15](#) for more information.

Configure the Wizard in FMC

This procedure sets up the integration for all the FMC users.

Before you begin

- Your system must be working as expected and generating the events you want to send.
- Set up your Secure Network Analytics and Security Analytics and Logging (OnPrem) products to be ready to receive event data.
- You must have one of the following 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.
- Gather the following:
 - 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 FMC; they are used once in order to establish a read-only analyst API account for the FMC on the Manager. A dedicated account is not needed for this; 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.

Procedure

- Step 1** In the FMC, go to **System > Logging > Security Analytics and Logging**.

- Step 2** Click an option to use a standalone Secure Network Analytics appliance (Single-node) or a Flow Collector (Multi-node) for extended storage capacity.
- Step 3** Complete the wizard.
If you see any field with a red box around it, hover over the field to see an error message.
- Step 4** Deploy your changes to managed devices.
-

What to do next

- If you are using the Security Analytics and Logging (OnPrem) app v3.0.0+ and Secure Network Analytics v7.4.0+ Multi-node deployment, enable sending Data Plane events using the [Configure Firepower Management Center to Send Events to Secure Network Analytics using Syslog](#) section.
- If your FMC manages supported devices running versions earlier than 7.0, see [For Managed Devices Running Versions Earlier than 7.0, Use Syslog](#), on page 15.
- 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 FMC are also available remotely. Then see [Stop Storing Low-Priority Connection Events on the FMC](#), on page 19.



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 Firepower Management Center to Send Events to Secure Network Analytics using Syslog

The following describes how to configure the FMC to send event data 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) app v3.0.0+ and Secure Network Analytics v7.4.0+ Multi-node deployment.

Before you begin

- Make sure you enable sending Data Plane event logging to Secure Network Analytics using the [Configure the Wizard in FMC](#) in the FMC.

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.
- Go to **Syslog > Logging Destinations**.
 - Click + **Add Logging Destination**.
 - For **Logging Destination**, select **Syslog Servers**.
 - For **Event Class**, select **Filter on Severity**.
 - Choose any severity.
- Step 3** Configure logging facility.
- Go to **Syslog > Syslog Settings > Facility**.
 - For **Facility**, select **default = LOCAL4(20)**.

For Managed Devices Running Versions Earlier than 7.0, Use Syslog

If your FMC manages devices running version 6.4 or later, you can run the wizard described in this document to enable viewing the events on the FMC and cross-launching from FMC into Secure Network Analytics, then configure your system to use syslog to send events to Security Analytics and Logging (OnPrem) from pre-7.0 FTD devices.

Configuration Overview: Sending Events from FTD Devices On Earlier Versions

To configure your Firepower deployment for Security Analytics and Logging (OnPrem), perform the following:

- Verify that your Firepower object names, such as policy and rule names, do not contain commas, as this may cause issues. Use other special characters instead, such as hyphens.
- Note the Firepower Management Center management IP address and the Firepower Threat Defense devices management IP addresses. See the [Firepower documentation](#) for more information.
- Create a network host object with your Secure Network Analytics ingest appliance management IP address
- Configure your Firepower Threat Defense device to export syslog over UDP to the Secure Network Analytics ingest appliance
- Optionally restrict the exported syslog to only connection, intrusion, file, and malware events to improve performance
- Enable your access control policy to log to syslog
- Configure logging connection, intrusion, file, and malware events to syslog.



Note If you export unsupported event types to the appliance, it drops these events and does not store them. However, the events count towards your overall exported events per second (EPS). Removing these events from the export can reduce your overall exported EPS and improve overall performance.



Note If you want to send different event types to different syslog destinations, contact Cisco Support.

Create a Network Host Object

Before you begin

- Log into the Firepower Management Center web interface as an Admin, Access Admin, or Network Admin.

Procedure

- Step 1** Select **Objects > Object Management**.
- Step 2** Choose **Network** from the list of object types.
- Step 3** Choose **Add Object** from the Add Network drop-down list.
- Step 4** Enter an object **Name**, such as *csal-sw-appliance* or another descriptive name.
- Step 5** Enter a **Description**, such as *Security Analytics and Logging (OnPrem) Secure Network Analytics appliance for event export* or another description.
- Step 6** In the **Network** field, enter your Manager's *eth0* management IP address.
- Step 7** Click **Save**.
-

Configure Firepower Threat Defense Settings to Export syslog to Secure Network Analytics

Procedure

- Step 1** From the Firepower Management Center web interface, select **Devices > Platform Settings** and create or edit a Firepower Threat Defense policy associated with your Firepower Threat Defense device.
- Step 2** In the left navigation pane, click **Syslog**.
- Step 3** Click **Syslog Servers** and click **Add** to add a new syslog server (in this case, the Secure Network Analytics appliance).
- Step 4** Select *csal-sw-appliance* from the **IP Address** drop-down list.
- Step 5** Select the **UDP Protocol**.
- Step 6** Enter **Port 8514**.
- Step 7** Under **Reachable By**, check **Device Management Interface**.
- Step 8** Click **Syslog Settings**.
- Step 9** Check **Enable Timestamp on Syslog Messages**.
- Step 10** Select the **RFC 5424 (yyyy-MM-ddTHH:mm:ssZ) Timestamp Format**. Security Analytics and Logging (OnPrem) requires the RFC 5424 timestamp format.
- Step 11** Click **Logging Setup**.
- Step 12** Check **Log messages in Cisco EMBLEM format (UDP only)**.
-

Optionally Configure Firepower Threat Defense Settings to Export only Connection, Intrusion, File, and Malware Events

If you want to limit the exported syslog to only connection, intrusion, file, and malware events, and regulate the sent events per second to improve performance, you can configure a syslog event list in the Firepower Threat Defense settings.



Note 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; see [Troubleshooting](#) for more information.

Add the following message IDs to your event list:

Table 6:

Message ID	Event Type
430001	Intrusion event
430002	Connection event logged at beginning of connection
430003	Connection event logged at end of connection
430004	File event
430005	Malware event

Procedure

- Step 1** From your Firepower Threat Defense policy, in the left navigation pane, click **Syslog**.
- Step 2** Click **Event Lists**.
- Step 3** Click **Add**.
- Step 4** Enter a descriptive **Name**, such as *SecurityAnalyticsandLogging*. Note that spaces are not allowed.
- Step 5** Click **Message ID**.
- Step 6** Click **Add**.
- Step 7** Enter *430001-430005* in the **Message ID** field.
- Step 8** Click **OK**.
- Step 9** Click **OK**.
- Step 10** **Save** your settings.

Enable syslog Export per Access Control Policy

You configure each access control policy to use the Firepower Threat Defense syslog settings that you configured in the previous procedure.

Procedure

- Step 1** From the access control policy, select **Logging**.
 - Step 2** Check **FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device**.
 - Step 3** Click **Save**.
-

Enable Connection Event Logging to syslog per Access Control Rule

You enable connection event logging to syslog at the access control rule level.

Procedure

- Step 1** From the Firepower Management Center web interface, click **Policies > Access Control** and edit your access control policy.
 - Step 2** Click the **Edit** (✎) icon next to a rule where you want to configure connection event logging.
 - Step 3** Click the **Logging** tab.
 - Step 4** Specify whether you want to **Log at Beginning of Connection** or **Log at End of Connection**. To optimize performance, log either the beginning or the end of any connection, but not both.
 - Step 5** If you will log file events, select **Log Files**.
 - Step 6** Enable **Syslog Server**.

Verify that the rule is "**Using default syslog configuration in Access Control Logging**." Do not enable overrides.
 - Step 7** Click **Save**.
 - Step 8** Repeat steps 1-6 for each access control rule for which you want to enable connection event logging to syslog.
 - Step 9** If you have finished your Firepower configuration, you can now go to **Deploy > Deployment** and deploy the policy to managed devices. The changes are not active until you deploy them. Otherwise, continue Firepower configuration.
-

Enable File and Malware Event Logging to syslog

You enable file and malware event logging to syslog at the access control policy level. In addition, each access control rule must have an associated file policy to generate file and malware events.

Procedure

- Step 1** From the Firepower Management Center web interface, click **Policies > Access Control**, and edit your access control policy.
- Step 2** Click the **Logging** tab.
- Step 3** Check **Send Syslog messages for File and Malware events** to enable file and malware event logging.

Verify that the rule is "Using default syslog configuration in Access Control Logging." Do not enable overrides.

- Step 4** Click **Save**.
- Step 5** For each access control rule associated with the file policy, follow the instructions in [Enable Connection Event Logging to syslog per Access Control Rule](#) to ensure that your Firepower deployment logs file events to syslog.
- Step 6** If you have finished your Firepower configuration, you can now go to **Deploy > Deployment** and deploy the policy to managed devices. The changes are not active until you deploy them. Otherwise, continue Firepower configuration.

Enable Intrusion Event Logging to syslog

You enable intrusion event logging to syslog at the intrusion policy level. In addition, each access control rule must have an associated intrusion policy to generate intrusion events.

Procedure

- Step 1** From the web interface, click **Policies > Access Control > Intrusion** to navigate to your intrusion policy.
- Step 2** Click the **Edit** icon next to the intrusion policy where you want to configure logging.
- Step 3** Click **Advanced Settings > Syslog Alerting > Enabled**.
- Step 4** Click **Back**.
- Step 5** Click **Policy Information** in the left navigation pane.
- Step 6** Click **Commit Changes**.
- Step 7** If you have finished your configuration, you can now go to **Deploy > Deployment** and deploy the policy to managed devices. The changes are not active until you deploy them. Otherwise, continue configuration.

Stop Storing Low-Priority Connection Events on the FMC

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 FMC.

Events that are not stored on your FMC do not count against the maximum flow rate for your FMC 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 FMC, 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 FMC 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 FMC.

Before you begin



Caution

This procedure will immediately permanently delete all connection events currently stored on your FMC.

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 FMC is successfully sending events to Secure Network Analytics.

Procedure

Step 1

There are two ways to stop storing low priority connection events on the FMC:

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) app v3.0.0+ and Secure Network Analytics v7.4.0+ Multi-node 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 EMBLEM logging format and secure logging are 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-TTHH: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
```

EMBLEM logging format is not supported for this integration. Hence, 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.

Note This integration does not support EMBLEM format. Hence, ensure that the **Send syslogs in EMBLEM** check box is not selected.

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).

Note The **Log messages in Cisco EMBLEM format** check box is available if you selected UDP. This integration does not support EMBLEM format. Hence, ensure that this check box is not selected.

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.
- EMBLEM logging format and secure logging are 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. Click **Save**.

Note This integration does not support EMBLEM format. Hence, ensure that the **Send syslogs in EMBLEM** check box is not selected.

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).

Note The **Log messages in Cisco EMBLEM format** check box is available if you selected UDP. This integration does not support EMBLEM format. Hence, ensure that this check box is not selected.

- 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.
