Integrating Cisco ASA and Cisco Security Analytics and Logging (SaaS) using CLI and ASDM

Cisco ASA and Cisco Security Analytics and Logging (SaaS) Integration Guide 2

Overview 2

ASA Event Flow in SAL (SaaS) 3

Requirements and Prerequisites for SAL (SaaS) Integration 3

How to Set Up Event Data Storage in SAL (SaaS) Using Syslog 5

How to Obtain SEC IP and Port Numbers from CDO 6

Send Syslog Events from ASA Devices 7

Send NetFlow Secure Event Logging (NSEL) Data from ASA Devices 10

View and Work with Events 13

Frequently Asked Questions 14

Revised: May 19, 2023

Cisco ASA and Cisco Security Analytics and Logging (SaaS) Integration Guide

This guide describes how to configure ASA with SAL (SaaS), how the events and syslog messages are handled in SAL (SaaS), and how to view the events from CDO.

Overview

You can configure your ASA devices to send syslog and NetFlow Secure Event Logging (NSEL) events to an external eventing service, store the logs in the Cisco cloud, and view them in the Event Logging page of Cisco Defense Orchestrator (CDO). In the Event Logging page, you can filter the events, download them, and review them for troubleshooting security issues. This guide provides the procedure to integrate Adaptive Security Device Manager (ASDM) managed ASA devices with Cisco Security Analytics and Logging (SaaS) solution.

Note For information on integrating CDO managed ASA with SAL (SaaS), see Cisco Security Analytics and Logging for ASA Devices.

Syslog and NSEL Events

The syslogs are system log or event messages sent to a syslog server by ASA devices that are used for monitoring and troubleshooting device issues. The syslog messages have classes and IDs to denote the type of events and their severity.For detailed information on ASA syslog messages, see ASA Syslog Guide.

NSEL is a stateful flow tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events have equivalent syslog messages. Those syslog messages are classified under CDO event filter as Firewall denied and Firewall traffic. The Cisco ASA supports NetFlow version 9 services. For more information, see Cisco ASA NetFlow Implementation Guide.

Note You must enable NSEL to send data to SAL (SaaS) to avail the SWC services.

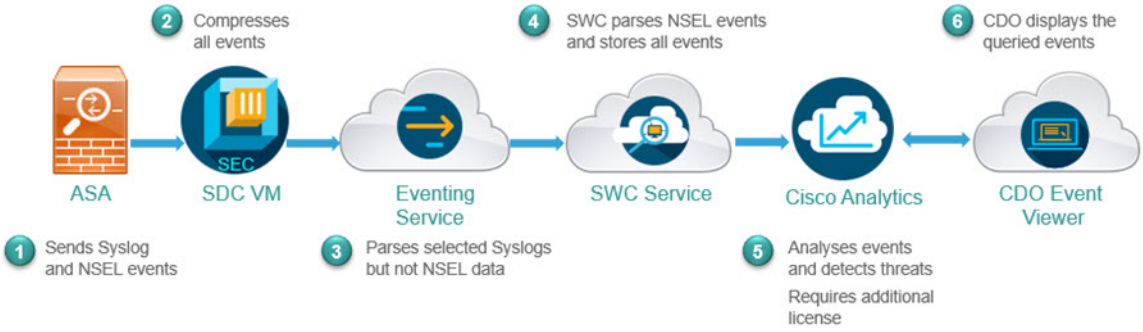
Components of ASA and SAL (SaaS) Integration

- Cisco Adaptive Security Device Manager (ASDM)—A graphical interface tool that manages your ASA device.
- On-Premises Secure Device Connector (SDC)—The SDC handles communication between CDO and your ASA. The on-premises SDC is a virtual appliance installed on a hypervisor in your network. You can create your on-premises SDC by using an image provided by Cisco or you can create your own VM and install the SDC on it.
- Secure Event Connector (SEC)—An application installed on an on-premises Secure Device Connector (SDC) that receives events from ASA devices and forwards them to the Cisco cloud.
- Stealthwatch Cloud (SWC)—Cloud-based analytical solution that provides a deeper analysis of events gathered from your network. It allows you to identify trends and examine anomalous behavior in your network traffic.

- Cisco Defense Orchestrator (CDO)—CDO is a cloud-based multi-device manager that co-exists with local ASA device manager, namely, ASDM, and SSH connections. With a CDO account, you can view the ASA event logs stored in the Cisco cloud. With additional licensing, you can cross-launch from CDO to a Stealthwatch Cloud portal provisioned for you.

ASA Event Flow in SAL (SaaS)

Following is the flow of ASA events in SAL after a successful integration:



1. ASA sends events (syslog and NSEL events) to the SEC component of the SDC VM that is configured in CDO.
2. The SEC accepts both TCP and UDP syslogs from ASA and compresses the events. From here on, the events are securely transferred to the Cisco cloud. The SEC sends the compressed events to the cloud-based Eventing Service.

   Note Events are compressed to ensure secured transfer of data. Your data subscription and historical monthly consumption are r assessed on this compressed data. They are assessed on the uncompressed data that you use.

3. The Eventing service parses the syslog events; it does not parse the NSEL data. It forwards both the syslog events and the NSEL data to the Stealthwatch Cloud (SWC) solution.
4. The SWC parses NSEL and stores the results along with syslog events.
5. The Cisco Analytics service, analyzes the events and detects threats based on observations. Note that to avail this service, you must have the Logging Analytics and Detection or Total Network Analytics and Detection license.
6. The CDO event viewer displays the events stored in the Cisco cloud based on your filter criteria.

Requirements and Prerequisites for SAL (SaaS) Integration

Requirement or Prerequisite Type	Requirement
ASA	Cisco Adaptive Security Device Manager (ASDM) Release 7.0 or later. ASA running software release 9.0 or later. Your appliance must be deployed and successfully generating events.

Requirement or Prerequisite Type	Requirement
Regional cloud	Determine which regional cloud you will send events to. Events cannot be viewed from or moved between different regional clouds.
Data plan	Determine the amount of cloud storage your system will require: See Calculate Storage Requirements and Purchase a Data Plan, on page 5.
Licensing	• Cisco Security Analytics and Logging licenses: Any For licensing options and descriptions, see SAL (SaaS) Licenses, on page 4. • CDO licenses: No additional CDO licensing is required. • Stealthwatch Cloud licenses: No additional licensing is required. • ASA licenses: No additional licensing required. For information on Cisco Smart Software Licensing for ASA, see Cisco Smart Software Licensing.
Accounts	When you purchase a license for this integration, you will be provided with a CDO tenant account to support this functionality.
Additional prerequisites	See the Before You Begin or Prerequisites section of each procedure.

SAL (SaaS) Licenses

License	Details
Free trial	To get a 30 day free trial license, visit https://info.securexanalytics.com/sal-trial.html.
Logging and Troubleshooting	Store events in the Cisco cloud, and view and filter stored events using the CDO web interface.
(Optional) Logging Analytics and Detection	The system can apply Stealthwatch Cloud dynamic entity modeling to your ASA events, and use behavioral modeling analytics to generate Stealthwatch Cloud observations and alerts. You can cross-launch from CDO to a Stealthwatch Cloud portal provisioned for you, using Cisco Single Sign-On. When you purchase a license for SAL, you will be provided access to a CDO tenant for log viewing and a SWC instance for threat detections. Users of SAL do not need a separate CDO or SWC license to access these two portals for the outcomes that SAL provides.
(Optional) Total Network Analytics and Detection	The system applies dynamic entity modeling to both your ASA events and your network traffic, and generates observations and alerts. You can cross-launch from CDO to a Stealthwatch Cloud portal provisioned for you, using Cisco Single Sign-On. When you purchase a license for SAL, you will be provided access to a CDO tenant for log viewing and a SWC instance for threat detections. Users of SAL do not need a separate CDO or SWC license to access these two portals for the outcomes that SAL provides.

For details about SAL (SaaS) licensing options, see the *Cisco Security Analytics and Logging Ordering Guide* at https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html.

SAL (SaaS) licenses provide the right to use a Cisco Defense Orchestrator tenant to view firewall logs and a Stealthwatch Cloud (SWC) instance for analytics, without holding separate licenses for either of these products.

To purchase SAL (SaaS) licenses, contact your authorized Cisco sales representative, or see the ordering guide (link above) and look for PIDs starting with **SAL-SUB**.

Additional information about this product is here: https://apps.cisco.com/Commerce/guest.

Calculate Storage Requirements and Purchase a Data Plan

You need to buy a data plan that reflects the number of events the Cisco cloud receives from your ASAs on a daily basis. This is called your "daily ingest rate."

To estimate your data storage requirements:

- (Recommended) Participate in a free trial of Cisco Security Analytics and Logging (SaaS) before you buy it. See SAL (SaaS) Licenses, on page 4.
- Use the Logging Volume Estimator Tool at https://ngfwpe.cisco.com/ftd-logging-estimator.

Data plans are available in various daily volumes, and in various yearly terms. See the *Cisco Security Analytics and Logging Ordering Guide* at https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html for information about data plans.

Note If you have a SAL (SaaS) license and data plan, then obtain a different license at a later date, that alone does not require you to obtain a different data plan. If your network traffic throughput changes and you obtain a different data plan, that alone does not require you to obtain a different SAL (SaaS) license.

How to Set Up Event Data Storage in SAL (SaaS) Using Syslog

	Do This	More Information
Step	Review requirements and prerequisites	See Requirements and Prerequisites for SAL (SaaS) Integration, on page 3.
Step	Obtain required licenses, accounts, and a data storage plan	Contact your authorized Cisco sales representative.
Step	Set up CDO access using multi-factor authentication	See instructions in the CDO online help for Signing in to CDO.

	Do This	More Information
Step	Set up an on-premises Secure Device Connector (SDC) on a VMWare virtual machine	This component is required solely to enable installation of the SEC, which is the component to which your ASA devices will send events. Use one of the following, as described in the CDO online help: • (Preferred) Use the CDO-provided VM image. • Create an SDC without using the CDO-provided image. **Important!** Don't skip the procedure prerequisites. However, ignore any information about onboarding, which does *not* apply to this integration.
Step	Install the Secure Event Connector (SEC) on the SDC virtual machine you just created.	This is the component to which your ASA devices will send events. See the CDO online help for instructions to Install the Secure Event Connector. **Important!** Don't skip the procedure prerequisites. However, ignore any information about onboarding, which does *not* apply to this integration.
Step	Configure ASDM to have your ASA send syslog and NSEL events to the SEC.	Send Syslog Events from ASA Devices, on page 7 and Send NetFlow Secure Event Logging (NSEL) Data from ASA Devices, on page 10
Step	Verify that your events are being sent successfully	See View and Work with Events, on page 13.
Step	(Optional) Configure general settings in CDO	For example, you can make your data unavailable to Cisco support staff. In the CDO online help, see General Settings.
Step	(Optional) Create CDO user accounts for colleagues to view and work with your events.	In the CDO online help, see Create a New CDO User.

How to Obtain SEC IP and Port Numbers from CDO

While configuring your ASA device to connect with the Cisco cloud, you would require the SEC IP and its port number. To obtain the SEC details from CDO, do the following:

Procedure

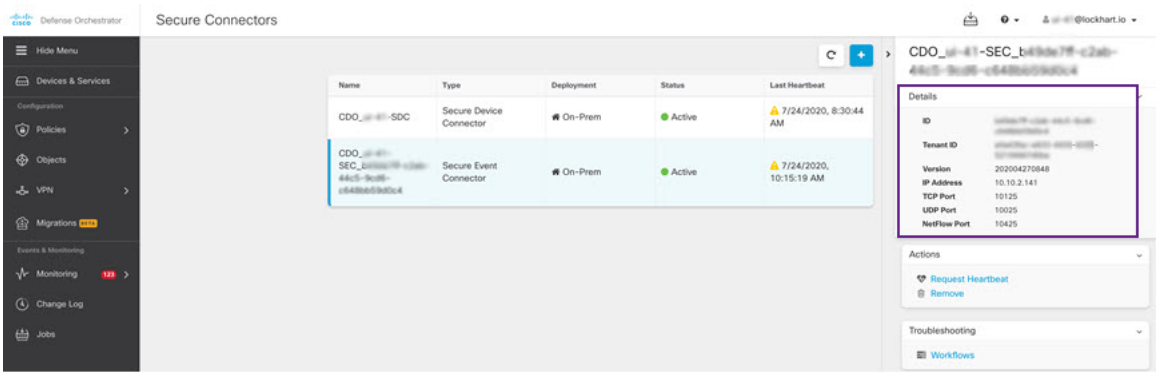
Step 1 Sign in to CDO.

Step 2 From the user menu at the top right side of the CDO browser window, select **Secure Connectors**.

Step 3 In the Secure Connectors list, click the desired SEC.

Step 4 In the Details section, look for the configured IP address, TCP, UDP, and NetFlow port numbers.

Figure 1: Obtaining SEC IP and Port Numbers



Send Syslog Events from ASA Devices

The ASA system logs provide you with information for monitoring and troubleshooting the ASA. For list of ASA event types, see here.

To have ASA send the syslog events to the SAL (SaaS) cloud, you must configure logging on the ASA device:

- Enable logging
- Configure output destination to SEC

Note EMBLEM logging format and secure logging are not supported for this integration.

Use the following links for information on logging configuration in ASA CLI and ASDM.

- CLI Commands to Send Syslog Events from ASA Devices, on page 7
- ASDM Configuration to Send Syslog Events from ASA Devices, on page 9

CLI Commands to Send Syslog Events from ASA Devices

This procedure documents the configuration commands for sending syslog messages for security events from ASA devices to SAL.

Before you begin

- Review the requirements and prerequisites section.
- Set up event data storage in SAL (SaaS).
- Confirm that your ASA devices can reach SECs.
- If you have installed SDC on a custom linux VM, ensure that SEC receives the ASA syslogs.

- Obtain the SEC IP address and port number from CDO.

Procedure

Step 1 Enable logging:

logging enable

Example:

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

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

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 SEC:

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

Example:

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

```
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 Secure Event Connector (SEC):

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

Example:

```
ciscoasa(config)#  logging host management 209.165.201.3 6/10125

OR
ciscoasa(config)#  logging host management 209.165.201.3 17/10025
```

Note

a. For the syslog ip and port, specify the SEC IP and the corresponding port number obtained from CDO (for instructions, refer to the Before you begin section).

b. Specify *6* to denote TCP protocol, and *17* to denote UDP protocol.

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

logging timestamp {**legacy** | **rfc5424**}

Example:

```
ciscoasa(config)# logging host tftp 1.1.1.1 tcp/1900 format ?

configure mode commands/options:
```

```
  analytics  Enable Analytics on syslog messages
  emblem     Enable EMBLEM format logging, available only for udp syslog messages
  timestamp  Enable logging timestamp on syslog messages
ciscoasa(config)# logging host tftp 1.1.1.1 tcp/1900 format timestamp ?

configure mode commands/options:
  legacy   Timestamp formatted as per legacy
  rfc5424  Timestamp formatted as per RFC5424
ciscoasa(config)# logging host tftp 1.1.1.1 tcp/1900 format 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
```

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

This procedure documents the ASDM configuration for sending ASA syslog messages for security events to SAL (SaaS).

Before you begin

- Review the requirements and prerequisites section.
- Set up event data storage in SAL (SaaS).
- Confirm that your ASA devices can reach SEC(s).
- If you have installed SDC on a custom linux VM, ensure that SEC receives the ASA syslogs.
- Obtain the SEC IP address and port number from CDO.

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 (SEC).

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 SEC IP 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 SEC IP obtained from CDO (for instructions, refer to the Before you begin section).
- **Protocol**—Select TCP or UDP.
- **Port**—The corresponding SEC port number obtained from CDO (for instructions, refer to the Before you begin section).

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.

Send NetFlow Secure Event Logging (NSEL) Data from ASA Devices

ASAs report detailed connection event data using NetFlow Secure Event Logging (NSEL). For list of supported ASA NSEL event types, see here.

You can apply Stealthwatch Cloud analytics to this connection event data, which includes bidirectional flow statistics. To have ASA send the NSEL events to a flow collector you must configure NSEL on the ASA device:

- Add a NetFlow collector, here, it is the Secure Event Connector (SEC).
- Configure service policy rules.
- The information sent through NSEL events overlap with some of the syslog connection events. Disable redundant syslog messages from being forwarded to SEC.

Use the following links for information on NSEL configuration in ASA CLI and ASDM.

- CLI Commands to Send NSEL Data from ASA Devices, on page 11

• ASDM Configuration to Send NSEL Data from ASA Devices, on page 12

CLI Commands to Send NSEL Data from ASA Devices

This procedure documents the configuration commands for sending NSEL events from ASA devices to SAL (SaaS).

Before you begin

- Review the requirements and prerequisites section.
- Set up event data storage in SAL (SaaS).
- Confirm that your ASA devices can reach SEC(s).
- If you have installed SDC on a custom linux VM, ensure that SEC receives the ASA events.
- Obtain the SEC IP address and port number from CDO.

Procedure

Step 1 Add the NetFlow collector to which the NetFlow packets are to be sent. Here, the Secure Event Connector (SEC) is the NetFlow collector.

flow-export destination *interface_name ipv4_address | host name udp-port*

Example:

```
ciscoasa(config)# flow-export destination management 209.165.201.3 10425
```

Note For the ipv4 address and udp-port, specify the SEC IP address and UDP port number obtained from CDO (for instructions, refer to the Before you begin section).

Step 2 Configure policies to send NetFlow events to NetFlow collector (SEC):

a) Define the class map that identifies traffic for which NSEL events need to be exported.

class-map *flow_export_class*

Example:

```
ciscoasa(config)# class-map global_class
```

b) Match any traffic.

match any

Example:

```
ciscoasa(config-cmap)# match any
```

c) Define the policy map to apply flow-export actions to the defined classes.

policy-map *flow_export_policy*

Example:

```
ciscoasa(config-cmap)# policy-map global_policy
```

d) Define the class to apply flow-export actions.

class *flow_export_class*

Example:

```
ciscoasa(config-pmap)# class global_class
```

e) Configure a flow-export action.

flow-export event-type *event-type* **destination** *flow_export_host1* [*flow_export_host2*]

Example:

```
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.201.3
```

For detailed information on the NetFlow commands, refer the Cisco ASA NetFlow Implementation Guide.

Step 3 Disable redundant syslog messages.

logging flow-export-syslogs disable

Example:

```
ciscoasa(config)# logging flow-export-syslogs disable
```

ASDM Configuration to Send NSEL Data from ASA Devices

This procedure documents the ASDM configuration for sending ASA's NetFlow Secure Event Logging (NSEL) events to SAL (SaaS) solution.

Before you begin

- Review the requirements and prerequisites section.
- Set up event data storage in SAL (SaaS).
- Confirm that your ASA devices can reach SEC(s).
- If you have installed SDC on a custom linux VM, ensure that SEC receives the ASA events.
- Obtain the SEC IP address and port number from CDO.

Procedure

Step 1 Log in to ASDM.

Step 2 Add the NetFlow collector to which the NetFlow packets are to be sent. Here, the Secure Event Connector (SEC) is the NetFlow collector.

a) Choose **Configuration** > **Device Management** > **Logging** > **NetFlow**.
b) In the **Collectors** section, click **Add** to add a collector.
c) In the **Add NetFlow Collector** dialog box, specify the following:

- **Interface**— Specify the interface that will be used to communicate to the NetFlow collector.
- **IP Address or Hostname**—The SEC IP address obtained from CDO (for instructions, refer to the Before you begin section)
- **UDP Port**—The SEC port number obtained from CDO (for instructions, refer to the Before you begin section)

d) Click **Ok**.

Step 3 Configure service policy:

a) Choose **Configuration** > **Firewall** > **Service Policy Rules**.
b) Click **Add**.
c) In **Add Service Policy Rule Wizard - Service Policy**, click the **Global - applies to all interfaces** radio button to apply the rule to the global policy, and then click **Next**.
d) In **Add Service Policy Rule Wizard - Traffic Classification Criteria**, check the **Any traffic** check box, and then click **Next**.
e) In **Add Service Policy Rule Wizard - Rule Actions**, click the **NetFlow** tab, and then click **Add**.
f) In the **Add Flow Event** dialog box, the collector added in Step 2 is listed in the Collectors table. Check the check box under **Send** column against the collector (SEC), and then click **Ok**.
g) Click **Finish**.

Step 4 Disable the redundant syslog messages from being forwarded to SEC.

a) Choose **Configuration** > **Device Management** > **Logging** > **NetFlow**.
b) Check the **Disable redundant syslog messages** check box.
c) Click **Apply**.

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

View and Work with Events

To view and search your events in the cloud:

Procedure

Step 1 Use your browser to go to the regional CDO cloud to which you sent your events:

- North America:

  http://www.defenseorchestrator.com

- Europe:

  http://www.defenseorchestrator.eu

Step 2 Sign in to CDO.

Step 3 From the navigation bar, select **Monitoring > Event Logging**.

Step 4 Use the **Historical** tab to view historical events data. By default, the viewer displays this tab.

Step 5 To view the live events, click the **Live** tab.

Note In the Event Logging page,

- The deep parsed ASA syslog events are displayed in italics.
- To view the NetFlow events, in the **Filters** pane, under **ASA Events**, check the **NetFlow** check box. The NetFlow events can be identified by their event type values—1, 2, 3, and 5.
- The **Include NetFlow Events** check box at the bottom of the **Filters** pane is checked by default. When you filter the events to view Firewall Denied and Firewall Traffic, the NetFlow events are also displayed along with the syslog events.

For more information about what you can do on this page, see the CDO online help for instructions on viewing events.

What to do next

If you have a **Logging Analytics and Detection** or **Total Network Analytics and Detection** license, see instructions in the CDO online help to cross-launch into the Stealthwatch Cloud portal.

Frequently Asked Questions

Do I need to onboard my ASA devices to CDO?

No. Do NOT onboard your devices to CDO.

Do I need CDO and Stealthwatch Cloud licenses also with SAL (SaaS)?

No. SAL (SaaS) provides right to use Cisco Defense Orchestrator (CDO) for event viewing, and Stealthwatch Cloud (SWC) for behavioral detections, without need to hold licenses to these two products separately. However, to use diagnostic and analytical features of SWC, you need to procure appropritae licenses.

If I upgrade my ASA, do I need to upgrade my data plan also?

No. Data plans are based on the number of events the Cisco cloud receives from your ASAs on a daily basis. You can change your data plan irrespective of the device version. See Calculate Storage Requirements and Purchase a Data Plan, on page 5.

I am not seeing events in CDO Event viewer. What should I do?

1. Perform basic health-check of service running in SEC and its connectivity with Cisco cloud. You need to be in SDC VM as *sdc user* to run health check. For detailed information, see Cisco Defense Orchestrator Guide.
2. Ensure ASA is configured with the correct SEC IP address and TCP/UDP port.

If problem persists, contact Cisco Defense Orchestrator Support.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.