Cisco Security Analytics and Logging

About Security Analytics and Logging

Security Analytics and Logging (SAL) is a central log management and advanced threat detection service which delivers scalable Cisco firewall logging and correlated analytics. Central logging helps in providing visibility, helps troubleshoot network access issues including disruptions, and enables device and overall network health monitoring. Analytics provide detection against advanced threats.

The SAL service is available in the following two methods:

- Security Analytics and Logging (SaaS)—A hosted software as a service (SaaS) which stores events and provides data for security analytics using Secure Cloud Analytics (formerly Stealthwatch Cloud). This service connects the Security Analytics and Logging cloud data store to the firewall cloud manager, Cisco Defense Orchestrator (CDO).

  In this documentation, this method is also referred to as SAL (SaaS).

- Security Analytics and Logging (On Premises)—A service that runs on the Secure Network Analytics (formerly Stealthwatch) appliances to store event logs at the customer's own premises. This service connects the Security Analytics and Logging (On Premises) data to the on-premises manager, Secure Firewall Management Center.

  In this documentation, this method is also referred to as SAL (OnPrem).

For more information about Security Analytics and Logging, see https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html.

Comparison of SAL Remote Event Storage and Monitoring Options

SAL integration shows similar options for storing event data externally to a management center and CDO:

	SAL (OnPrem)	**SAL (SaaS)**
Why choose this solution?	You want to increase your on-premises firewall event data storage capacity, retain this data for a longer period, and export your event data to the Secure Network Analytics appliance.	You want to send firewall events for storage and optionally make your firewall event data available for security analytics using Secure Cloud Analytics.
Licensing	Purchase license and set-up the storage system behind your firewall. For more information, see Licensing for SAL (OnPrem), on page 3	Purchase license and a data storage plan and send your data to the Cisco cloud. For more information, see Licensing for SAL (SaaS), on page 8
Supported event types	• Connection • File and Malware • Intrusion • LINA • Security Intelligence	• Connection • File and Malware • Intrusion • Security Intelligence
Supported methods to send events	Supports both, syslog and direct integration.	Supports both, syslog and direct integration.
Event viewing	• View events on the Secure Network Analytics Manager. • Cross-launch from the management center event viewer to view events on the Secure Network Analytics Manager. • View remotely stored connection and security intelligence events in the management center.	View events in CDO or Secure Network Analytics Manager, depending on your license. Cross-launch from the management center event viewer.

About SAL (OnPrem)

You can configure SAL (OnPrem) to store firewall event data for increased storage at a larger retention period. By deploying Secure Network Analytics appliances and integrating them with your firewall deployment, you can export your event data to a Secure Network Analytics appliance.

This provides you with the following capabilities:

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

Licensing for SAL (OnPrem)

You must obtain the Logging and Troubleshooting smart license to use SAL (OnPrem). You can obtain the license based on the amount of data you anticipate while sending the syslog data from your firewall deployment to your Secure Network Analytics appliance on a daily basis.

For information on licensing the Secure Network Analytics appliances, see Secure Network Analytics Smart Software Licensing Guide.

For information on the available SAL (OnPrem) licensing options, see the Cisco Security Analytics and Logging Ordering Guide.

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

Manage SAL (OnPrem) for CDO-Managed Threat Defense Devices

Starting with Secure Firewall Threat Defense(formerly Firepower Threat Defense) version 7.2, you can choose to send fully qualified events that are generated by CDO-managed threat defense devices to the management center. The management center receives and displays data analytics for these events. The management center receiving and displaying the event data is also referred to as an analytics-only management center. .

If your devices are enabled to send connection events to a Secure Network Analytics Manager using SAL (OnPrem), you can view and work with these remotely stored events in the management center event viewer and context explorer, and include them when generating reports. By deploying the Secure Network Analytics appliance and integrating it with the firewall deployment, you can export the event data to the Secure Network Analytics appliance. This allows you to view and manage the events in the management center UI. From the management center interface, you can also cross-launch to Secure Network Analytics Manager to view and manage the events data.

The management center can receive and display event analytics for the following CDO-managed threat defense devices:

- New or existing threat defense devices onboarded to CDO

  For information on onboarding a threat defense device to CDO, see Prerequisites to Onboard a Device to Cloud-delivered Firewall Management Center.

The workflow is as follows:

1. Onboard a threat defense device to CDO.

   Onboard the threat defense devices using the onboarding methods that are described in Prerequisites to Onboard a Device to Cloud-delivered Firewall Management Center. The onboarding process includes assigning policies and choosing the appropriate licenses.

2. Register this threat defense device in the appropriate management center.

   For the management center to display events generated by a CDO-managed threat defense device, you must register the threat defense device in the management center. To register this device in the management center, enable the device to be registered using the **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address*}*reg_key*[*nat_id*] CLI, and then add the device to the management center using the **CDO Managed Device** check box.

   Note The registration key and the NAT ID must be unique from those used while onboarding the device to CDO.

   For more information, see *Add a Device to the Management Center* and *Complete the Threat Defense Initial Configuration Using the CLI* in Firepower Management Center Device Configuration Guide.

3. View events in the management center or cross-launch to a configured Secure Network Analytics Manager.

   To view and work with the events in the management center event viewer. If the Secure Network Analytics appliance is deployed and integrated with the firewall deployment, you can export the event data to the Secure Network Analytics appliance. This allows you to cross-launch from the management center UI to the Secure Network Analytics Manager to view and manage the events data.

   For more information, see *Events and Assets* and *Event Analysis Using External Tools*.

- Existing threat defense devices on the management center.

You can change the management of the threat defense devices from management center to CDO using the change threat defense manager functionality. The change threat defense manager functionality provides you to ability to change the management of threat defense devices from management center to CDO. While changing the manager, you can choose to retain the events data generated by these threat defense devices on the management center. If you choose to retain the events data on the management center, a copy of the threat defense device in an analytics-only mode is retained on the management center.

For more information, see Migrate Secure Firewall Threat Defense to Cloud.

The workflow is as follows:

1. Onboard the management center to CDO

   To onboard the existing threat defense devices from management center to CDO, you must onboard the appropriate management center to CDO.

   For more information, see Onboard an FMC.

2. Complete the change threat defense management process

During the change threat defense management process, while changing the device manager, you can choose to retain events data generated by these threat defense devices on the management center.

For more information, see Migrate Secure Firewall Threat Defense to Cloud.

3. View events in the management center or cross-launch to configured Secure Network Analytics appliance.

   To view and work with the events in the management center event viewer. If the Secure Network Analytics appliance is deployed and integrated with the firewall deployment, you can export the event data to the Secure Network Analytics appliance. This allows you to cross-launch from the management center UI to the Secure Network Analytics Manager to view and manage the events data.

   For more information, see Events and Assets and Event Analysis Using External Tools.

Configure SAL (OnPrem) Integration

You can configure CDO to send events to the Secure Network Analytics appliance using one of the following deployment options:

- Secure Network Analytics Manager Only—Deploy a standalone manager to receive and store events. The threat defense devices send event data to the Network Analytics Manager. All event data is stored on the Network Analytics Manager. From the management center user interface, you can cross-launch the manager to view more information about the stored events.

- Secure Network Analytics Data Store—Deploy a Cisco Secure Network Analytics Flow Collector to receive events, a Cisco Secure Network Analytics Data Store (containing 3 Cisco Secure Network Analytics Data Nodes) to store events, and a manager . The threat defense devices send event data to the flow collector from where the events are sent to the Data Store for storage. From the management center user interface, you can cross-launch the manager to view more information about the stores events.

  Starting with threat defense version 7.2, you can choose to associate different flow collectors to different devices.

Configure a Secure Network Analytics Manager

Configure the Secure Network Analytics Manager deployment to integrate SAL (OnPrem) with CDO-managed threat defensedevices.

Before you begin

Ensure the following:

- You have a provisioned CDO tenant and have the following CDO user roles:
  - Admin
  - Super admin

- Your threat defense devices are working as expected and are generating events.

- If you are currently using syslog to send events to the Secure Network Analytics Manager 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 duplicating events on the remote volume.
- You have the hostname or the IP address of your Secure Network Analytics Manager.

Note You may be logged out of the Secure Network Analytics Manager during the registration process; complete any work in progress before you start with the deployment wizard.

Procedure

Step 1 Log in to CDO.

Step 2 From the CDO menu, navigate **Tools & Services** > **Firewall Management Center**.

Step 3 Select **Firewall Management Center** and click **Configuration**.

Step 4 Navigate to **Integration** > **Security Analytics & Logging**.

Step 5 In the **Secure Network Analytics Manager Only** widget, click **Start**.

Step 6 Enter the hostname or the IP address and port number of the Secure Network Analytics Manager and click **Next**.

Step 7 Deploy the changes to the managed devices.

The event data is not logged to the SAL (OnPrem) until the logging policy changes are deployed to the registered threat defense devices.

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

You can view and work with these remotely stored events in the event viewer and context explorer in the management center, and include them when generating reports. You can also cross-launch from an event in the management center to view related data on your Secure Network Analyticss appliance.

For more information, see the online help for the management center.

Step 8 Click **OK**.

Configure a Secure Network Analytics Data Store

Configure a Secure Network Analytics data store deployment to integrate SAL (OnPrem) with threat defense devices that are CDO-managed.

Before you begin

Ensure the following:

- You have a provisioned CDO tenant and have the following CDO user roles:

  - Admin
  - Super admin

- Your threat defense devices are working as expected and generating events.
- If you are currently using syslog to send events to the Secure Network Analytics appliance 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 information:
  - The hostname or the IP address of your Secure Network Analytics Manager.
  - The IP address of your flow collector.

Note You may be logged out of the Secure Network Analytics Manager during the registration process; complete any work in progress before you start with the deployment wizard.

Procedure

Step 1 Log in to CDO.

Step 2 From the CDO menu, navigate **Tools & Services** > **Firewall Management Center** to open the **Services** page.

Step 3 Choose **Cloud-Delivered FMC** and click **Configuration**.

Step 4 Navigate to **Integration** > **Security Analytics & Logging**.

Step 5 In the **Secure Network Analytics Data Store** widget, click **Start**.

Step 6 Enter the hostname or the IP address and port number of the flow collector.

To add more flow collectors, click **+Add another Flow Collector**.

Step 7 If you have configured more than one flow collector, associate the managed devices with different flow collectors:

Note By default, all the managed devices are assigned to the default flow collector.

a) Click **Assign Devices**.
b) Select the managed devices that you want to assign.
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.**

You can change the default flow collector by hovering over the intended flow collector and clicking **Set default**.

d) Click **Apply Changes**.
e) Click **Next**.

Step 8 Click **Next**.

Step 9 Deploy the changes to the registered managed devices.

The event data is not logged to the SAL (OnPrem) until the logging policy changes are deployed to the registered threat defense devices.

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

You can view and work with these remotely stored events in the event viewer and context explorer in the management center, and include them when generating reports. You can also cross-launch from an event in the management center to view related data on your Secure Network Analytics Manager.

For more information, see the online help for the management center.

About SAL (SaaS)

SAL (SaaS) allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all of your threat defense devices and view them in one place in CDO. The events are stored in the Cisco cloud and are viewable from the Event Logging page in CDO, where you can filter and review them to gain a clear understanding of what security rules are triggering in your network.

With additional licensing, after you capture these events, you can cross-launch from CDO to the Secure Cloud Analytics portal provisioned for you. Secure Cloud Analytics is a software as a service (SaaS) solution that tracks the state of your network by performing a behavioral analysis on events and network flow data. By gathering information about your network traffic from sources including firewall events and network flow data, it creates observations about the traffic and automatically identifies roles for network entities based on their traffic patterns. Using this information combined with other sources of threat intelligence, such as Talos, Secure Cloud Analytics generates alerts, which constitute a warning that there is behavior that may be malicious in nature. Along with the alerts, Secure Cloud Analytics provides network and host visibility, and contextual information it has gathered to provide you with a better basis to research the alert and locate sources of malicious behavior.

Licensing for SAL (SaaS)

The SAL (SaaS) licenses allows you to use a CDO tenant to view firewall logs and a Cisco Secure Cloud Analytics instance for analytics, without holding separate licenses for either of these products.

For details on the available SAL (SaaS) licensing options, see the Cisco Security Analytics and Logging Ordering Guide.

Configure the SAL (SaaS) Integration

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

- Send Events to SAL (SaaS) using Syslog, on page 9
- Send Events to SAL (SaaS) using a Direct Connection, on page 11

Requirements for the SAL (SaaS) Integration

Requirement Type	Requirement
Cisco Secure Firewall Threat Defense	• CDO-managed standalone threat defense devices, version 7.2 and later. • To send events using syslog: threat defense version 6.4 or later • To send events directly: threat defense version 7.2 • Your firewall system must be deployed and successfully generating events.
Regional cloud	• Determine the regionial cloud you want to send events to. • Events cannot be viewed from or moved between different regional clouds. • If you use a direct connection to send events to the cloud for integration with SecureX or Cisco SecureX threat response, you must use the same regional CDO cloud for this integration. • If you send events directly, the regional cloud you specify in CDO must match the region of your CDO tenant.
Data plan	• You must buy a data plan that reflects the number of events the Cisco cloud receives from your threat defense devices daily. This is called your "daily ingest rate." • Use the Logging Volume Estimator Tool to estimate your data storage requirements.
Accounts	When you purchase a license for this integration, you are provided with a CDO tenant account to support the integration.

Send Events to SAL (SaaS) using Syslog

This procedure documents the best practice configuration for sending syslog messages for security events (connection, Security Intelligence, intrusion, file, and malware events) from devices managed by CDO.

Before you begin

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

Procedure

Step 1 Log in to CDO.

Step 2 From the CDO menu, navigate **Tools & Services** > **Firewall Management Center** to open the **Services** page.

Step 3 Choose **Cloud-Delivered FMC** and click **Configuration**.

Step 4 Configure syslog settings for your threat defense device:

a) Navigate **Devices** > **Platform Settings** and edit the platform settings policy associated with your threat defense device.

b) In the left navigation pane, click **Syslog** and configurate the syslog settings as follows:

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

c) Click **Save**.

Step 5 Configure general logging settings for the access control policy (including file and malware logging):

a) Navigate **Policies** > **Access Control** to edit the access control policy associated with your threat defense device.

b) Click the **Logging** tab and configure the general logging settings for the access contol policy (including file and malware logging) as follows:

Click	To do the following
Send using specific syslog alert	Select a syslog alert from the list of existing existing pre-defined alerts or add one by specifying the name, logging host, port, facility, and severity.

Click	To do the following
Use the syslog settings configured in the FTD Platform Settings policy deployed on the device	Unify the syslog configuration by configuring it in Platform Settings and reuse the settings in access control policy. The selected severity is applied to all connection and intrusion events. The default severity is ALERT.
Send Syslog messages for IPS events	To send events as syslog messages. The defaults set above are used unless you override them.
Send Syslog messages for File and Malware events	To send file and malware events as syslog messages. The defaults set above are used unless you override them.

c) Click **Save**.

Step 6 Enable logging for Security Intelligence events for the access control policy:

a) In the same access control policy, click the **Security Intelligence** tab.
b) In each of the following locations, click the **Logging** icon and enable beginning and end of connections and syslog server:

- Besides **DNS Policy**.
- In the **Block List** box, for **Networks** and **URLs**.

c) Click **Save**.

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

a) In the same access control policy, click the **Rules** tab.
b) Click a rule to edit.
c) Click the **Logging** tab in the rule.
d) Enable both beginning and end of connections.
e) If you will log file events, select **Log Files**.
f) Enable **Syslog Server**.
g) Verify that the rule is "**Using default syslog configuration in Access Control Logging**."
h) Click **Save**.
i) Repeat for each rule in the policy.

What to do next

If you are done making changes, deploy your changes to the managed devices.

Send Events to SAL (SaaS) using a Direct Connection

Configure cloud-delivered Firewall Management Center to send events directly to SAL (SaaS).

Before you begin

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

Procedure

Step 1 Log in to CDO.

Step 2 From the CDO menu, navigate **Tools & Services** > **Firewall Management Center** to open the **Services** page.

Step 3 Select **Cloud-Delivered FMC** and in the **Settings** pane located to the right, select **Cisco Cloud Events**.

Step 4 In the **Configure Cisco Cloud Events** widget, do the following:

a. Click the **Send Events to the Cisco Cloud** slider to enable the overall configuration.

b. Check the **Send Intrusion Events to the cloud** check box to send intrusion events to the cloud.

c. Check the **Send File and Malware Events to the cloud** check box to send file and malware events to the cloud.

d. Choose an option to send connection events to the cloud:

- Click the **None** radio button to not send connection events to the cloud.
- Click the **Security Events** radio button to send only security intelligence events to the cloud.
- Click the **All** radio button to send all connection events to the cloud.

e. Click **Save**.

View and Work with Events in CDO

Procedure

Step 1 Log in to CDO.

Step 2 From the CDO menu, choose **Analytics** > **Event Logging**.

Step 3 Use the **Historical** tab to view all historical events data. By default, the viewer displays this tab.

Step 4 To view the live events, click the **Live** tab.

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

View and Work with Events in Cisco Secure Cloud Analytics

Before you begin

To ensure seamless flow of events, before using the Event Viewer, do the following in the Stealthwatch Cloud portal:

- Verify whether Secure Cloud Analytics is integrated with the correct CDO tenant.

  To view the CDO tenant, click **Settings** > **Sensors**.

- Add the subnets that you want monitor to Secure Cloud Analytics.

  To add subnets, click **Settings** > **Subnets**.

Procedure

Step 1 Log in to CDO.

Step 2 From the CDO menu, choose **Analytics** > **Secure Cloud Analytics**.

The Secure Cloud Analytics portal opens in a new browser tab.

Step 3 Click **Investigate** > **Event Viewer**.

For more information, see the Secure Cloud Analytics online help.