Security Analytics and Logging Licenses

This chapter provides information on Security Analytics and Logging licenses.

Security Analytics and Logging licenses

Security Analytics and Logging subscription overview

You can combine SAL with your Security Cloud Control subscription. When managing your firewalls with Security Cloud Control, you can obtain Security Analytics and Logging entitlement in these ways:

- Device management with unlimited logging: This option provides a per-device license. It includes device management capabilities for your firewall device and unlimited log storage for a rolling period of 90 days.
- Device management only with optional cloud logging: This option involves purchasing a per-device license for management only. You can then add Security Analytics and Logging as a separate cloud logging subscription. This allows you to customize logging data storage and log retention based on your specific operational and compliance needs.

90-day free trial

To accurately estimate your daily ingest rate, log in to Security Cloud Control and navigate to the **Events & Logs** > **Events** > **Event Logging** tab to request a 90-day trial. You can purchase the desired subscription plan to continue the service by reviewing the instructions in the Security Cloud Control Firewall Management Ordering Guide.

Security Analytics and Logging paid subscription tiers

If you choose not to use device management with unlimited logging option, you can purchase logging capacity separately. This standalone Security Analytics and Logging subscription provides greater flexibility, longer default retention, and increased storage entitlements. The default minimum retention period for these subscription tiers is 1 year.

Select these flexible Security Analytics and Logging subscription tiers if:

- You have already purchased your firewall devices as part of a different order.

- You have specific logging estimates and want to buy a tier based on a fixed amount of ingest, storage, and logging retention.
- You want a log retention period that is more than 90 days.

Security Analytics and Logging subscription is categorized into three tiers—Essentials, Advantage, and Premier. This table lists the storage capacities and log retention periods for each tier.

Description	Retention Period	Storage Limit	Subscription Term
Cisco SAL Essentials Subscriptions	1, 2, or 3 years	2 TB	0 to 5 years
Cisco SAL Advantage Subscriptions	1, 2, or 3 years	4 TB	0 to 5 years
Cisco SAL Premier Subscriptions	1, 2, or 3 years	10 TB	0 to 5 years

For more information about the subscription plans, refer to the Security Cloud Control Firewall Management Ordering Guide.

Note For paid subscriptions, Security Analytics and Logging automatically manages your event data to ensure that it aligns with your licensed retention period. Security Analytics and Logging removes event data that is older than your specified retention period on a daily basis, and ensures that you always retain access to all event data within your full retention period.

Estimate your daily ingest rate

Purchase a subscription plan that matches the number of events the Cisco cloud receives from your onboarded firewall devices on a daily basis. This is called your *daily ingest rate*. You can use the Logging Volume Estimator tool to estimate your daily ingest rate and as that rate changes you can update your subscription plan.

Subscribe to a Security Analytics and Logging license

Start a Security Analytics and Logging trial subscription

Purchase a data storage plan that matches the daily event volume your onboarded security devices send to Cisco cloud. This volume is referred to as your daily ingest rate. Before making a purchase, participate in a free trial of Security Analytics and Logging to accurately estimate your daily ingest rate.

- With this trial plan, you gain access to all Security Analytics and Logging features for 90 days.
- During the 90-day trial period, your onboarded firewalls send events to Security Analytics and Logging. Monitor your event ingestion rates, understand your storage requirements, and evaluate performance. This data helps you to plan and select the most appropriate paid subscription.
- If you activate a paid Security Analytics and Logging subscription while a trial is active, Security Cloud Control replaces the trial license for the product instance with the paid license and ends the trial.

- If you choose not to apply the paid subscription to the trial, event ingestion automatically stops after 90 days. After this, you cannot access Security Analytics and Logging features. However, your existing log data remains in the Security Analytics and Logging cloud for an additional 90 days from the trial expiry date.

Note If you do not subscribe to a paid Security Analytics and Logging license within this 90-day grace period, all your trial data is permanently deleted.

Order a paid Security Analytics and Logging subscription

To continue using Security Analytics and Logging after your trial, or to upgrade your existing logging capabilities:

1. Use the insights that you gained from your trial (daily ingest rate, required retention, storage volume) to determine the most suitable Security Analytics and Logging subscription plan.
2. Work with your Cisco representative or authorized partner to purchase the appropriate Security Analytics and Logging subscription.

Claim your Security Analytics and Logging subscription

After you purchase a new Security Analytics and Logging subscription, you receive a claim code to activate it within Security Cloud Control. A welcome email containing your subscription claim code is automatically sent to the Provisioning Contact you specified during the purchasing process. If you included an End Customer contact, they also receive a copy. You will receive this email on the requested start date of your subscription.

A Security Cloud Control administrator uses the claim code to activate the subscription for their organization. For detailed instructions on claiming and activating subscriptions, refer to Claim a Subscription.

Renew your Security Analytics and Logging subscription

Maintaining an active Security Analytics and Logging subscription ensures continuous logging and access to your historical data.

- If your Security Analytics and Logging subscription expires without renewal, event ingestion from your firewalls stops immediately.
- You can continue to view and search existing event data for 90 days after the subscription expires. After 90 days, event data is no longer accessible.
- Your existing data remains in the Security Analytics and Logging cloud for a 180-day grace period from the subscription expiry date.
- If the Security Analytics and Logging subscription is not renewed within this 180-day grace period, all your event data is permanently deleted from the Security Analytics and Logging cloud.

View Security Analytics and Logging license information

View your Security Analytics and Logging license information such as the entitled monthly storage limit and the event storage retention period. If you do not have a separate Security Analytics and Logging license and data plan, you see the 90-day rolling data storage details in the licensing information.

Procedure

Step 1 Choose **Settings** > **Logging SettingsAdministration** > **Logging Settings**.

Step 2 Click **View Logging Storage Usage**.

Tip
Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** and then click the **Storage Utilization** button to view the Security Analytics and Logging license information.

The **Event Logging Insights and Storage Usage** dashboard provides a comprehensive overview of your Security Analytics and Logging license subscription:

- **Retention policy**: Displays the event log retention period according to your subscription. Event data that is older than your retention period is removed daily, and you always retain access to all event data within your full retention period.
- **Storage capacity**: Displays the total entitled data under your Security Analytics and Logging license, the amount of storage currently used, and the remaining available storage.

View Security Analytics and Logging Storage usage and event ingest rate

View the current Security Analytics and Logging storage utilization and analyze event logging trends. You can analyze the storage utilization trends by event type, device type, and individual devices to gain deeper insights into storage utilization patterns. Use the data visualizations for quick and easy analysis. This helps you assess the current storage capacity and take measures to reduce the logging rate if the storage utilization approaches the limits that are specified in your Security Analytics and Logging license.

Procedure

Step 1 Choose **Administration** > **Logging Settings**.

Step 2 Click **View Logging Storage Usage**.

Tip
Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** from the left navigation bar, and then click the **Storage Utilization** button to view the Security Analytics and Logging storage usage and event ingestion trends.

Step 3 Use these dashboards to customize and analyze storage utilization and gain insights into event logging trends in your firewall deployment:

- **Usage Trends**: Displays the event logging storage usage for the last 12 months. Hover over a bar to see the data usage for the corresponding month.
- **Events per second (EPS) trends**: Displays the event ingest rate for the onboarded devices. Customize your events per second trends view for a specific time period or device to get more granular data. You can filter the data for the past 1 week, 2 weeks, 3 weeks, or 1 month.

Note
The device drop-down list displays the managed firewall devices that are sending events to the Cisco Security Cloud.

- **Utilization by event type trends**: Displays event data storage used, in bytes per day, for different event types. Use this widget to monitor storage use by event types and identify surges, if any, or unusual changes in storage use for specific event types. This insight enables you to adjust logging settings for a specific event type and manage storage use.
- **Utilization by device type trends**: Displays event data storage used, in bytes per day, for each managed device type. Use this widget to monitor storage use by the device type and identify surges, if any, or unusual changes in storage use for a specific type of device.
- **Utilization by device trends**: Displays event data storage used, in bytes per day, for each security device that sends events to Security Cloud Control. This widget focuses on devices with storage use exceeding the average bytes per second value, showing only the top five devices to improve usability. Use this widget to monitor storage use for each device and identify surges or unusual changes. This insight allows you to adjust logging settings for specific devices and manage storage use effectively.

Extend event storage duration and increase event storage capacity

To extend your rolling event storage or increase your event cloud storage, follow these steps:

Procedure

Step 1 Log in to your account on Cisco Commerce.

Step 2 Select your Security Cloud Control PID.

Step 3 Follow the prompts to upgrade the duration or capacity of your storage.

The increased cost will be prorated based on the term remaining on your existing license. See the Guidelines for Quoting Cisco Defense Orchestrator Products for detailed instructions.

View Security Analytics and Logging alerts

View alerts and notifications for the Security Analytics and Logging configurations and event settings for the managed firewall devices.

Procedure

Step 1 Choose **Settings** > **Logging SettingsAdministration** > **Logging Settings**.

Step 2 Click the **View Logging Storage Usage** button.

Tip

Alternatively, navigate to **Events & Logs** > **Events** > **Event Logging** from the left navigation bar, and then click **Storage Utilization** to view the Security Analytics and Logging license information.

The **Alerts and Notifications** section displays alerts about the settings that impact event logging. These alerts enable you to take action to resolve any issues. Some of these settings include:

- Sending events to cloud setting is disabled.
- Sending events to the cloud setting is disabled at device level.
- Secure Event Connector becomes unavailable.
- Increase in events ingestion rate.

Frequently asked questions about Security Analytics and Logging license

Which data gets counted against my Security Analytics and Logging allotment?

All events sent to the Cisco cloud directly or to the Secure Event Connector accumulate in Security Analytics and Logging and count against your data allotment.

Filtering the events viewer does not decrease the number of stored events in Security Analytics and Logging. It only reduces the number of events you see in the events viewer.

We're using up our storage allotment quickly. What should I do?

Here are two approaches to address that problem:

- Request more storage.
- Consider reducing the number of rules that log events. You can log events from SSL policy rules, security intelligence rules, access control rules, intrusion policies, and file and malware policies. Review your current logging settings to determine if you need to log events from all the rules and policies that you have configured.

What happens to my data if my Security Analytics and Logging license expires?

If your paid Security Analytics and Logging license expires, event ingestion from your firewalls stops immediately. However, your existing data remains accessible in the Security Analytics and Logging cloud for a 180-day grace period. If you renew your paid license during this grace period, your service continues without interruption. If you do not renew within these 180 days, all your data is permanently deleted.

If I purchase a Security Analytics and Logging subscription with a 1-year retention period and a 5-year term, will my data be stored for all 5 years?

The retention period defines how long each log is stored. With a 1-year retention period, only the most recent 1-year log data is available at any given time. Log data older than 1 year is overwritten or deleted when new data is collected. A 5-year term means that data for that duration will continue to be ingested, but the retention limit is applicable to the log data itself.