

Security Analytics and Logging Licenses

This chapter provides information on Security Analytics and Logging licenses.

- Security Analytics and Logging licenses, on page 1

Security Analytics and Logging licenses

Security Analytics and Logging subscriptions offer flexible options for managing firewall logs in Security Cloud Control, including per-device licenses and customizable log storage and retention. Choose between Essentials, Advantage, and Premier tiers to meet operational and compliance requirements, with retention periods up to five years and storage capacities up to 10 TB.

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.

Subscribing to a Security Analytics and Logging license

Security Analytics and Logging trial provides full feature access for 90 days, allowing you to evaluate event logging performance, estimate daily ingest rates, and determine storage requirements. Gain valuable insights to select the optimal subscription and ensure continuous access to your firewall security data in the Cisco cloud.

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.

Summary

The key components involved in the Security Analytics and Logging subscription process are:

- Customer: Starts trial, evaluates performance, and determines subscription requirements
- Cisco representative or authorized partner: Facilitates subscription purchase
- Security Cloud Control administrator: Claims and activates subscription
- Trial period: 90 days with full feature access for evaluation
- Grace periods: 90 days for trial data retention, 180 days for paid subscription data retention

Workflow

These are the stages of subscribing to a Security Analytics and Logging license:

1. The customer starts a Security Analytics and Logging trial subscription to evaluate requirements and performance.
   - 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.

   This stage enables the customer to gain hands-on experience with Security Analytics and Logging capabilities and accurately determine their subscription requirements.

2. The customer orders a paid Security Analytics and Logging subscription based on trial insights.
   - 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.
   - Work with your Cisco representative or authorized partner to purchase the appropriate Security Analytics and Logging subscription.

   This stage ensures the customer selects a subscription plan that matches their actual usage requirements and establishes the commercial relationship.

3. The Security Cloud Control administrator claims the Security Analytics and Logging subscription to activate it.

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.

This stage completes the activation process and makes the paid subscription services available to the organization.

4. The customer maintains their Security Analytics and Logging subscription through timely renewal.

   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.

   This stage ensures continuous service availability and prevents data loss through proactive subscription management.

Result

The subscription process results in continuous access to Security Analytics and Logging logging services, properly sized to match actual usage requirements, with established renewal processes to prevent service interruption and data loss.

View Security Analytics and Logging license information

Monitor your Security Analytics and Logging license to track storage limits and retention periods to optimize event data management and prevent overages.

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 **View Dashboard** button to view the Security Analytics and Logging license information.

The **Event Logging Overview** 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.

The Security Analytics and Logging license information is displayed, showing your entitled monthly storage limit, event storage retention period, and current usage details.

View Security Analytics and Logging Storage usage and event ingest rate

Gain insights into storage usage and event trends in Security Cloud Control with interactive dashboards. Regular analysis helps you optimize event logging, adjust storage settings, prevent overages, and maintain efficient compliance and performance across your security environment.

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 **View Dashboard** 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.

You can view storage utilization and event logging trends across multiple dashboards, allowing you to monitor usage patterns and make informed decisions about storage settings and event logging configurations.

Monitor Security Analytics and Logging service availability

Monitor the availability and health of Security Analytics and Logging(SaaS) service, review Firewall Threat Defense device event logging status, and determine when Security Analytics and Logging last received events from managed devices.

Note The **Service Status** tab currently supports Firewall Threat Defense devices.

Before you begin

Enable the managed Firewall Threat Defense devices to send events to the Security Analytics and Logging cloud so you can view meaningful device logging status and last-event details.

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 **View Dashboard** button to view the Security Analytics and Logging service status.

Step 3 Click the **Service Status** tab.

Step 4 Review the **SAL Service Availability** widget to check the current Security Analytics and Logging service status.

If the Security Analytics and Logging service status displays **Degraded**, your Security Analytics and Logging service is affected and event ingestion might be delayed or disrupted.

Step 5 Check the **Last Event Received** widget to determine when Security Analytics and Logging last received an event from a device.

Step 6 Review the **Firewall Logging Status** widget to check Firewall Threat Defense device event logging status.

- **Connected**: Indicates the number of Firewall Threat Defense devices that are enabled to send events to the Security Analytics and Logging.
- **Disabled**: Indicates the number of Firewall Threat Defense devices that are disabled from sending events to the Security Analytics and Logging.

Step 7 In the **Firewall Details** list, check when each Firewall Threat Defense device last sent an event to Security Analytics and Logging.

Use this information along with **SAL Service Availability** and **Last Event Received** widgets to identify whether events might be delayed or not ingested.

If Firewall Threat Defense devices are disabled from sending events, review the device logging configuration. If the Security Analytics and Logging service status is **Unavailable** or **Degraded**, or if event ingestion appears delayed or disrupted, contact Cisco TAC for assistance.

You have reviewed the Security Analytics and Logging service status, device logging configuration, and last event timestamps to ensure proper event ingestion and identify any potential issues with the service or device connectivity.

Extend event storage duration and increase event storage capacity

Upgrade your Security Analytics and Logging license to extend event storage from the default 90 days to up to three years. Enhancing storage capacity ensures long-term data retention, compliance, and improved security visibility for network monitoring.

Perform this task when your organization needs increased event storage or retention.

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.

Your Security Analytics and Logging license is upgraded with extended event storage duration and increased storage capacity based on your selected options.

View Security Analytics and Logging alerts

Monitor and address Security Analytics and Logging configuration and event issues to maintain security compliance and prevent data loss.

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 **View Dashboard** 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.
- Security Analytics and Logging license is expired or the allotted data storage is exceeded.

The **Alerts and Notifications** section displays current alerts for Security Analytics and Logging configurations and event settings, enabling you to identify and resolve issues that may impact event logging.

Frequently asked questions about Security Analytics and Logging license

Learn which events count toward your Security Analytics and Logging data allotment, how to manage storage limits, what happens if your license expires, and how retention periods affect long-term data storage. Gain practical tips to optimize storage and maintain continuous access to your security event data.

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.