



Cisco Secure Cloud Analytics

Initial Deployment Guide



Table of Contents

Deployment Overview	13
Functionality Overview	14
Deployment	14
Dynamic Entity Modeling	14
Alerts and Analysis	15
Quick Start - Secure Cloud Analytics Deployment	16
Initial Signup	16
Private Network Monitoring Deployment and Initial Configuration	17
Public Cloud Monitoring Deployment and Initial Configuration	17
Recommended System Configuration	17
Optional System Configuration	18
Using the Web Portal	18
Private Network Monitoring Deployment and Configuration	20
Sensor Deployment Considerations	20
Sensor Prerequisites	20
Physical Appliance Additional Requirements	21
Virtual Machine Additional Requirements	22
VMware hypervisor	22
VirtualBox	22
Sensor Deployment Suggestions	22
Checking Your Sensor Version	23
Sensor Access Requirements	23
Network Device Configuration	24
Flow Configuration	25
Cisco Defense Orchestrator and Sensor Deployment	25
Sensor Media Installation and Configuration	26
Creating Boot Media	26
Download the sensor ISO file	27

Create a Bootable Optical Disc	27
Create a Bootable USB Flash Drive	27
Installing the Sensor	28
What to Do Next	30
Attaching Sensors to the Web Portal	30
Finding and Adding a Sensor's Public IP Address to a Portal	31
Manually Add a Portal's Service Key to a Sensor	32
Configuring Proxy	33
Confirm a Sensor's Portal Connection	34
Configuring a Sensor to Collect Flow Data	35
Configuring Sensors for Flow Collection	35
What to Do Next	36
Private Network Monitoring Integration for Kubernetes	36
Configuring Kubernetes Integration	37
Configure integration with Kubernetes	37
Viewing Deployed Sensors from the Secure Cloud Analytics Web UI	37
View deployed Sensors from the Secure Cloud Analytics Web UI	37
Public Cloud Monitoring Configuration	38
Public Cloud Monitoring Configuration for Amazon Web Services	39
Configuring S3 Bucket Flow Log Data Storage	39
Associate an S3 Bucket with a VPC	40
Configure S3 Bucket to Minimize Cost (Recommended)	40
Configuring AWS Permission to Access Flow Log Data	41
Create a Policy with Permission to Access Flow Log Data	41
Configuring an IAM Role to Access Flow Log Data	42
Configure an IAM Role with Permission to Access Flow Log Data	42
Configuring Secure Cloud Analytics to Access Flow Log Data from an S3 Bucket	43
Configure Secure Cloud Analytics to Ingest Flow Log Data Stored in a S3 Bucket	43
Configure the S3 Bucket Policy to Allow Secure Cloud Analytics to Ingest Flow	44

Log Data	
Verifying AWS Integration	45
Verify AWS Integration	45
Public Cloud Monitoring Configuration for Google Cloud Platform	46
Single GCP Project Configuration	46
Multiple GCP Project Configuration	46
Configure a Service Account to View VPC Flow Logs	47
Configuring a Single Service Account to View VPC Flow Logs for Multiple Projects	48
Locate Your Service Account's Email Address	49
Enable the Cloud Resource Manager API for an Additional Project	49
Add a Service Account to an Additional Project	49
What To Do Next	49
Configure GCP to Generate VPC Flow Logs and Enable Permissions	50
Configure a GCP Subnet to Generate VPC Flow Logs	50
Enable the Stackdriver Monitoring API (Recommended)	50
What To Do Next	50
Upload JSON Credentials	50
What To Do Next	51
Identifying a High-throughput Environment	51
Review the GCP Logging Quota	51
Creating a GCP Pub/Sub Subscription	51
Find Your GCP Project ID	51
Create a GCP Log Export Sink for the Project	51
Create a GCP Pub/Sub Subscription for the Project	52
Configuring Pub/Sub Topics and Subscriptions	52
Create a GCP Log Export Sink for Additional Projects	52
Create a GCP Pub/Sub Subscription for Additional Projects	53
Public Cloud Monitoring Configuration for Microsoft Azure	54
Azure User Roles	54

Activate Using a Bash Script	54
Create an Azure Resource Group	55
Obtain the Azure Active Directory URL and Subscription ID	55
Create an Azure AD Application	55
Grant Access to an Application	56
Create an Azure Storage Account to Store Flow Log Data	56
Create a Blob Storage Account	57
Enable Internet Access to the Blob Storage Account	57
Generate an Azure Storage Account Shared Access Signature URL	57
Enable Azure Network Watcher	58
Register Insights Provider	58
Enable Azure NSG Flow Logs	59
Secure Cloud Analytics Configuration with Azure	59
Configure Secure Cloud Analytics to Ingest Flow Log Data from Azure	59
Secure Cloud Analytics Web Portal Configuration	61
Private Network Monitoring Sensor Configuration	61
Adding a Sensor Using its Public IP Address	61
Obtain a sensor's Public IP Address	61
Add a sensor Using its Public IP Address	62
Configuring a Sensor's Display Label	62
Configure a sensor's Display Label	62
Configuring a Sensor's Monitoring Settings	62
Configure a sensor's Monitoring Settings	63
Configuring a Sensor's Syslog Settings	63
Configure a sensor's Syslog Settings	63
Configuring a Sensor's SNMP Reporting Settings	63
Configure a sensor's SNMP Reporting Settings	64
Viewing a Sensor's Logs	64
View a sensor's Logs	64
Download a Comma-Separated File Containing the Information	64

Alerts Configuration	64
Alert Priority Configuration	65
Update Alert Priority	65
Configuring the Country Watchlist	65
Modify the Country Watchlist Entries	65
Watchlist Configuration	65
Configuring the Internal Connections Watchlist	66
Add an Entry to the Internal Connections Watchlist	66
Remove an Entry	67
Download a Comma-Separated File Containing the Information	67
Configuring Third-party Watchlists	67
Add an Entry to the Third Party Watchlist	67
Manually Expire an Entry	68
Reinstate an Expired Entry	68
Configuring the IPs and Domains Watchlist	68
Add an Entry to the IPs and Domains Watchlist:	68
Manually expire an entry:	68
Remove an expired entry:	69
Uploading an IPs and Domains Watchlist Entries File	69
Upload a Domain Name or IP Address Watchlist Entry File	70
Configuring the AWS CloudTrail Event Watchlist	70
Add an Entry to the AWS CloudTrail Alert Watchlist	70
Download a Comma-Separated File Containing the Information	71
Configuring the GCP Logging Watchlist	71
Add an Entry to the GCP Logging Watchlist	71
Download a Comma-Separated File Containing the Information	71
Configuring IP Scanner Rules	71
Configure IP Scanner Rules	71
Configuring the Azure Activity Log Watchlist	72
Add an Entry to the GCP Logging Watchlist	72

Download a Comma-Separated File Containing the Information	72
Configuring the Azure Advisor Watchlist	72
Enable Azure Advisor Recommendations to be Ingested As Observations	72
Download a Comma-Separated File Containing the Information	72
Updating Alert Expiration	73
Update the Alert Expiration Period	73
Reviewing the Cloud Posture Watchlist	73
Review the Cloud Posture Watchlist	73
Entity Group Settings	73
Configuring Entity Groups	74
Create an Entity Group	74
Modify an Entity Group	74
Delete an Entity Group	75
Subnet Configuration	75
Configuring Local Subnet Alert Settings	77
Add an Entry to the Local Subnet Alert Settings	78
Search for a Local Subnet Alert Settings Entry	78
Modify a Local Subnet Alert Settings Entry	79
Uploading a Local Subnet Settings File	80
Upload a Subnet Alert Settings File	81
Modifying Virtual Cloud Subnet Settings	81
Search for a Virtual Cloud Subnet Alert Settings Entry	82
Modify a Virtual Cloud Subnet Alert Settings Entry	82
Configuring Trusted External Networks Subnet Alert Settings	82
Add an Entry to the Trusted External Networks Subnet Alert Settings	83
Search for a Trusted External Networks Subnet Alert Settings Entry	83
Modify a Trusted External Networks Subnet Alert Settings Entry	83
User and Site Management	83
Managing Users	84
Send an Invite Email	84

Modify a User Account	84
Configuring Session Timeout	85
Configure the Session Timeout	85
Web Portal Use	86
Dashboard Overview	86
Alerts Overview	86
Alerts Workflow	87
Alert Next Steps	88
Triage Open Alerts	88
What to Do Next	88
Snooze Alerts for Later Analysis	88
Update the Alert for Further Investigation	89
What to Do Next	89
Review the Alert and Start your Investigation	89
What to Do Next	89
Review the Supporting Observations and Contextual Detail	90
Examine the Entity and Users	91
Remediate the Issue	92
Fine-tune your Secure Cloud Analytics Settings	92
Update and Close the Alert	93
Reopen a Closed Alert	93
Unsnnooze a Snoozed Alert	94
Alerts Summary	94
Alert Summary Fields	94
Configuring Alert-related Settings	94
Using the Alerts Summary	95
View Alerts Based on Status	95
View an Alert's Detail	95
Sort the Displayed Alerts	95
Filter the Displayed Alerts	95

Manage the Alert Tags	96
Download a Comma-Separated File Containing the Information	96
Taking Actions in the Alert Summary	96
View Alerts Based on Status	96
Update Alerts from the Alerts Summary	96
Alert Detail	96
Related Alert Observations	97
Working with an Alert's Detail Page	97
View an Alert's Detail	97
Assign a user from an alert's detail page:	97
Set this Alert Type's Priority	97
Add Tags from an Alert's Detail Page	97
Create a New Cisco SecureX Incident	97
View context on MITRE ATT&CK Tactics and Techniques	97
Download a Comma-Separated File Containing the Information	98
View Additional Information for a Source Entity	98
View Additional Observations from an Alert's Detail Page	98
View Additional Information for an External Entity	98
Snooze an Alert:	99
Unsnuzzle a Snoozed Alert	99
Close an Alert	99
Reopen a Closed alert	100
Enter a Comment on this alert	100
Entity Detail	100
Entity Detail Fields	100
Viewing Entity Detail	103
View an Entity's Detail	103
Use the Summary Tab	103
Use the Traffic Tab	104
Use the Profiling Tab	104

Use the DNS Tab	104
Download a Comma-Separated File Containing the Information	105
Observations Overview	105
Recent Highlight Observations	105
Viewing the Recent Highlight Observations	105
View the Recent Highlights Observations	105
Filter the Recent Highlights Observations	105
View more Information About an Observation Type	105
View all Observations of a Type	106
View More Information about a Source Entity	106
View More Information About an External Entity	106
Observation Types	107
Viewing Observations by Type	107
View Observations by Type	107
View All Observations of a Type	107
Observations by Device	107
Viewing Observations by Source	108
View Observations by Source	108
View All Observations of a Type	108
Selected Observations	108
Viewing Selected Observations	108
Investigate Overview	108
Session Traffic Model	109
External Services Model	109
Device Model	109
IP or Domain Search	110
Encrypted Traffic Report	110
User Activity Model	110
Roles Model	110
Event Viewer	111

Session Traffic and Rejected Traffic Fields	111
Cloud Posture	112
Cloud Posture Fields	112
Configuring AWS Cloud Posture Permissions	114
Review Cloud Posture Permissions for AWS	114
Update the Secure Cloud Analytics IAM Policy in AWS	115
Accessing the Event Viewer	115
Access the Event Viewer	115
Showing and Hiding Columns	115
Show and Hide Columns	115
Viewing Additional Field Information	115
View Additional Field Information	116
Event Viewer Filtering	116
Event Viewer Query Syntax	116
Query Syntax Options	116
Order of Evaluation	117
Query Syntax Examples	118
Event Viewer Nested Field Searches	121
Inline Filtering the Event Viewer	122
Change the Time Selection	122
Filter a Column	122
Switch to Query Filtering	122
Query Filtering the Event Viewer	122
Change the Time Selection	122
Query Your Events	123
Switch to Inline Filtering	123
Viewing an IP Address's Additional Context	123
View Additional Information for a Source Entity	123
View Additional Information for an External Entity	123
Downloading Event Information	124

Generate and Download a CSV.GZ File	125
Report Menu	125
AWS Visualizations	125
Metering Report	125
Monthly Flows Report	126
Subnet Report	126
Traffic Model	126
Visibility Assessment	127
Additional Resources	128
Contacting Support	129
Change History	130

Deployment Overview

Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) is a visibility and advanced threat detection service. Secure Cloud Analytics collects traffic from an on-premises network or public cloud to identify hosts, build an understanding of normal host behavior, and generate alerts when device behavior changes in a manner that is relevant to an organization's network security. Secure Cloud Analytics collateral refers to this data analysis as Dynamic Entity Modeling.



The Secure Cloud Analytics PoV is not the same as Security Online Visibility Assessment (SOVA), a more general security assessment tool.

Cisco provides Secure Cloud Analytics “as a service,” operating and maintaining Secure Cloud Analytics and all associated services. The customer is responsible for uploading traffic information to the cloud platform via a virtual appliance deployed on-premises, or a cloud security policy that grants access.

Secure Cloud Analytics requires an initial 36-day learning period to employ dynamic entity modeling and create a full baseline model of your hosts' and other entities' traffic. During this initial learning period, approximately half of the alert types are available. As the learning period progresses, and the system collects more data, additional alerts become available. After the 36th day, the system is fully baselined, and all alerts are available.

Functionality Overview

Secure Cloud Analytics is a software as a service (SaaS) solution that monitors your on-premises and cloud-based network deployments. By gathering information about your network traffic, 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.

Deployment

Secure Cloud Analytics supports two deployment types to support your network:

- **Public Cloud Monitoring** (formerly Stealthwatch Cloud Public Cloud Monitoring): Agent-less monitoring of workloads by ingesting native cloud logs, and API integration to deliver threat detection and configuration monitoring
- **Private Cloud Monitoring** (formerly Stealthwatch Cloud Private Network Monitoring): Virtual Cisco Secure Cloud Analytics sensor (formerly Stealthwatch Cloud Sensor) deployment to ingest network flow data, SPAN/mirror port traffic, and NGFW log information.

You can deploy either or both at the same time, and review the configuration and alerts from both in a single Secure Cloud Analytics web portal UI. The web portal displays all sensors and monitored cloud deployments from the same page, so you can quickly review the state of your monitoring.

Dynamic Entity Modeling

Secure Cloud Analytics uses dynamic entity modeling to track the state of your network. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network, or a Lambda function in your AWS deployment. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they perform on your network. Secure Cloud Analytics can ingest native cloud log data and industry-standard telemetry, and use cloud provider APIs to identify entities and the types of traffic entities usually transmit. Secure Cloud Analytics updates these models over time, as the entities continue to send traffic, and potentially send different traffic, to keep an up-to-date model of each entity.

From this information, Secure Cloud Analytics identifies:

- roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, an interaction with an entity on a watchlist, or a remote access session established with another entity. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Alerts and Analysis

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system.

To build on the previous example, a New Internal Device observation on its own does not constitute possible malicious behavior. However, over time, if the entity transmits traffic consistent with a Domain Controller, then the system assigns a Domain Controller role to the entity. If the entity subsequently establishes a connection to an external server that it has not established a connection with previously, using unusual ports, and transfers large amounts of data, the system would log a New Large Connection (External) observation and an Exceptional Domain Controller observation. If that external server is identified as on a Talos watchlist, then the combination of all this information would lead Secure Cloud Analytics to generate an alert for this entity's behavior, prompting you to take further action to research, and remediate malicious behavior.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available. You can also see other observations and alerts that entities were involved with, and determine if this behavior is tied to other potentially malicious behavior.

Quick Start – Secure Cloud Analytics Deployment

The following provides an overview of how to deploy Secure Cloud Analytics, and how to use it to inspect possible malicious behavior on your network.

Initial Signup

1. Go to <https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> to sign up for Secure Cloud Analytics.
2. If you have an AWS cloud deployment, go to <https://aws.amazon.com/marketplace/pp/B075MWZVBM> to sign up for Secure Cloud Analytics.
3. Wait for an invitation email to arrive within several hours, or up to 12 hours depending on the time when you signed up.
4. When you receive the invitation email, click the invitation link to access your customer web portal and create your initial administrator login credentials.



The invitation link is one-time use, and disables after you create the initial administrator login credentials.

Determine the type of network you want to monitor:

- If you want to monitor on-premises deployments, see [Private Network Monitoring Deployment and Initial Configuration](#) for more information on configuring private network monitoring.
- If you want to monitor public cloud networks, see [Public Cloud Monitoring Deployment and Initial Configuration](#) for more information on configuring public cloud monitoring.
- If you want to monitor both on-premises deployments and public cloud network; see [Private Network Monitoring Deployment and Initial Configuration](#) for more information on configuring private network monitoring and [Public Cloud Monitoring Deployment and Initial Configuration](#) for more information on configuring public cloud monitoring.

Private Network Monitoring Deployment and Initial Configuration

1. Deploy sensors to monitor your on-premises network. See [Sensor Deployment Considerations](#) and [Sensor Media Installation and Configuration](#) for more information. See [Private Network Monitoring Integration for Kubernetes](#) for more information on deploying sensors to Kubernetes clusters.
2. Log into the Secure Cloud Analytics web portal UI with the initial administrator login credentials you created from the invitation email.
3. Verify and complete your sensor configuration. Update the configuration to monitor specific subnets, output to syslog, and configure SNMP reporting. See [Private Network Monitoring Sensor Configuration](#) for more information.

See [Recommended System Configuration](#) for more information on additional required system configuration.

Public Cloud Monitoring Deployment and Initial Configuration

1. Configure your cloud deployment to allow the Secure Cloud Analytics service to ingest flow logs. See [Public Cloud Monitoring Configuration for Amazon Web Services](#) for more information on configuring PCM for AWS. See [Public Cloud Monitoring Configuration for Google Cloud Platform](#) for more information on configuring PCM for GCP. See [Public Cloud Monitoring Configuration for Microsoft Azure](#) for more information on configuring PCM for Azure. Contact [Cisco Support](#) for more information on other cloud deployments.
2. Log into the Secure Cloud Analytics web portal UI with the initial administrator login credentials you created from the invitation email.
3. Verify and complete your public cloud monitoring configuration. See [Public Cloud Monitoring Configuration for Amazon Web Services](#), [Public Cloud Monitoring Configuration for Google Cloud Platform](#), and [Secure Cloud Analytics Configuration with Azure](#) for more information.

See [Recommended System Configuration](#) for more information on additional required system configuration.

Recommended System Configuration

1. Configure the system's sensitivity for alert generation, including subnet sensitivity and alert priority.

- Higher subnet sensitivity means that the system requires a lower threshold to generate an alert. See [Subnet Configuration](#) for more information.
 - Similarly, higher alert priority means that the system requires a lower threshold to generate an alert. See [Alert Priority Configuration](#) for more information.
2. Configure user accounts. See [User and Site Management](#) for more information.

Continue with optional system configuration, or start using the system:

- See [Optional System Configuration](#) for more information on configuring optional alert generation settings, including IP scanner and third-party watchlists, and country blacklists.
- See [Using the Web Portal](#) for more information on using the Secure Cloud Analytics web portal UI.

Optional System Configuration

1. Configure third-party watchlists to ingest external intelligence into Secure Cloud Analytics and improve alert generation. See [Configuring Third-party Watchlists](#) for more information.
2. Configure country blacklists to define which countries the system will generate observations for, if it detects traffic to those countries. See [Watchlist Configuration](#) for more information.
3. Configure IP scanner watchlist rules for known and approved network scanners. See [Configuring IP Scanner Rules](#) for more information.

See [Using the Web Portal](#) for more information on using the Secure Cloud Analytics web portal UI.

Using the Web Portal

1. Log into the Secure Cloud Analytics web portal UI.



You can login using the initial administrator login credentials you created from the invitation email, or as a different user that you created.

2. View the Secure Cloud Analytics Main Dashboard, which displays open alerts, entity counts, and recent traffic statistics. See [Dashboard Overview](#) for more information.
3. View all alerts from the Alerts menu option. See [Alerts Overview](#) for more information.

4. Investigate an alert by viewing context about entities involved with the alert, and related observations, then close the alert and mark it as helpful or not helpful. See [Alert Detail](#), [Observations Overview](#), and [Alerts Workflow](#) for more information.
5. View the system's models to identify trends and review your network's traffic. See [Investigate Overview](#) for more information.
6. View the report menu for more information on reporting on monitored traffic and usage. See [Report Menu](#) for more information.

Private Network Monitoring Deployment and Configuration

The following sections describe private network monitoring sensor deployment and configuration, including:

- system prerequisites, network environment prerequisites, and recommendations for deploying sensors
- instructions for installing a sensor on a physical appliance or virtual machine, configuring the sensor, and attaching it to the web portal
- instructions for configuring a Kubernetes cluster for private network monitoring

Sensor Deployment Considerations

You can deploy sensors to collect flow data, such as NetFlow, or to ingest network traffic that is mirrored from a router or switch on your network. You can also configure a sensor to both collect flow data and ingest mirrored network traffic. There is no limit on the number of sensors deployed.

If you want to configure a sensor to collect flow data, see [Configuring a Sensor to Collect Flow Data](#) for more information.

If you want to configure a sensor to ingest traffic from a mirror or SPAN port, see [Network Device Configuration](#) for more information on configuring your network devices to mirror traffic.



Sensor version 4.0 or greater can collect enhanced NetFlow telemetry. This allows Secure Cloud Analytics to generate new types of observations and alerts. For more information, see the [Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#).

Sensor Prerequisites

You can install a sensor on a physical appliance or virtual machine, with the following requirements:

Component	Minimum Requirement
Network interface	at least one network interface, designated as the Control interface, for passing information to the Secure Cloud Analytics service

	<p>Optionally, if you want to configure the sensor to ingest network traffic from a network device that replicates it over a mirror port, you need one or more network interfaces, designated as Mirror interfaces.</p>
RAM	2 GB
CPU	at least two cores
Storage Space	32 GB
Internet Access	required to download packages for the installation process

See this [white paper](#) for performance metrics and recommendations.

Note the following about designated Mirror interfaces:

- Mirror interfaces receive a copy of all inbound and outbound source traffic to the destination. Ensure that your peak traffic is less than the capacity of the sensor's Mirror interface link.
- Many switches drop packets from the source interfaces if a mirror port destination is configured with too much traffic.

Physical Appliance Additional Requirements

Component	Minimum Requirement
Installation File Upload	<p>one of the following to upload the installation .iso file:</p> <ul style="list-style-type: none"> • 1 USB port, plus a USB flash drive • 1 optical disc drive, plus a writeable optical disc (such as a CD-R disc) <p>Virtual machines can boot directly to the .iso file without additional requirements.</p>

Virtual Machine Additional Requirements

If your sensor is deployed as a virtual machine, ensure that the virtual host and network are configured for promiscuous mode on the second network interface if you plan to ingest traffic from a mirror or SPAN port.

VMware hypervisor

If you are running the virtual machine on a VMware hypervisor, configure the virtual switch for promiscuous mode:

1. Select the host in the inventory.
2. Select the Configuration tab.
3. Click **Networking**.
4. Click **Properties** for your virtual switch.
5. Select the virtual switch and click **Edit**.
6. Select the Security tab.
7. Select *Accept* from the **Promiscuous Mode** drop-down.

See the VMware knowledge base for more information on promiscuous mode. You may need to set the **VLAN ID** to 4095.

VirtualBox

If you are running the virtual machine in VirtualBox, configure the adapter for promiscuous mode:

1. Select the adapter for the Mirror interface from the **Network** Settings.
2. Set promiscuous mode to *Allow* in the **Advanced Options**.


See the VirtualBox documentation on virtual networking for more information.

Sensor Deployment Suggestions

Because network topologies can vary greatly, keep the following general guidelines in mind when deploying your sensors:

1. Determine if you want to deploy sensors to:
 - collect flow data
 - ingest mirrored network traffic
 - have some collect flow data, and others ingest mirrored network traffic
 - both collect flow data and ingest mirrored network traffic

2. If collecting flow data, determine what formats your network devices can export, such as NetFlow v5, NetFlow v9, IPFIX, or sFlow.

 Many firewalls support NetFlow, including [Cisco ASA firewalls](#) and [Cisco Meraki MX Appliances](#). Consult with your manufacturer's support documentation to determine if your firewall also supports NetFlow.

3. Ensure that the network port on the sensor can support the Mirror ports capacity.

Contact [Cisco Support](#) if you need help with deploying multiple sensors to your network.

Checking Your Sensor Version

To ensure you have the most recent sensor deployed on your network (version 5.1.1), you can check an existing sensor's version from the command line. If you need to upgrade, reinstall the sensor.

1. SSH log into a deployed sensor.
2. At the prompt, enter `cat /opt/obsrvbl-ona/version` and press Enter. If the console does not display 5.1.1, your sensor is out of date. Download the most recent sensor ISO from the web portal UI.

Sensor Access Requirements

The physical appliance or virtual machine must have access to certain services over the internet. Configure your firewall to allow the following traffic between a sensor and the external internet:

Traffic type	Required	IP address or domain and port
Outbound HTTPS traffic from the sensor's Control interface to the Secure Cloud Analytics service hosted on Amazon Web Services	yes	<ul style="list-style-type: none"> port 443 and the IP address is your portal IP address
Outbound traffic from the sensor's Control interface to Ubuntu Linux server for downloading Linux OS and related updates	yes	<ul style="list-style-type: none"> us.archive.ubuntu.com:443/TCP us.archive.ubuntu.com:80/TCP
Outbound traffic from the	yes	<ul style="list-style-type: none"> [local DNS server]:53/UDP

sensor's Control interface to a DNS server for hostname resolution		
Inbound traffic from a remote troubleshooting appliance to your sensor	no	<ul style="list-style-type: none"> 54.83.42.41:22/TCP



If you use a proxy service, create a proxy exception for sensor Control interface IP addresses.

Network Device Configuration

You can configure your network switch or router to mirror a copy of traffic, then pass it to the sensor.



Because the sensor sits outside the normal flow of traffic, it cannot directly influence your traffic. Configuration changes that you make in the web portal UI influence alert generation, not how your traffic flows. If you want to allow or block traffic based on alerts, update your firewall settings.

See the following for information on network switch manufacturers, and resources to configure mirrored traffic:

Manufacturer	Mirrored traffic name	Configuration Example
Cisco	Switch Port Analyzer (SPAN)	Configuration Examples and TechNotes
Juniper	port mirror	See Juniper's TechLibrary documentation for an example of Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches
NETGEAR	port mirror	See Netgear's knowledge base documentation for an example of port mirroring and how it works with a managed switch
ZyXEL	port mirror	See ZyXEL's knowledge base documentation for

		information on How to use Mirroring on ZyXEL switches
other	monitor port, analyzer port, tap port	See Wireshark's wiki documentation for a switch reference for multiple manufacturers

You can also deploy a network test access point (tap) device to pass a copy of traffic to the sensor. See the following for information on network tap manufacturers, and resources to configure the network tap.

Manufacturer	Device Name	Documentation
NetOptics	network tap	See Ixia's resources page for documentation and other information
Gigamon	network tap	See Gigamon's resources and knowledge pages for documentation and other information

Flow Configuration

You must configure your network device to pass NetFlow data. [See https://configurenetflow.info/](#) or https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf for more information on configuring NetFlow on Cisco network devices.

Cisco Defense Orchestrator and Sensor Deployment

If you use Cisco Defense Orchestrator (CDO) and deploy Firepower appliances to your network, you can purchase a Cisco Security Analytics and Logging (SaaS) license (**Firewall Analytics and Monitoring** or **Total Network Analytics and Monitoring**) and apply Secure Cloud Analytics dynamic entity modeling to your Firepower event data. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

With a **Firewall Analytics and Monitoring** or **Total Network Analytics and Monitoring** license, you can associate an existing Secure Cloud Analytics portal with your CDO deployment, or have Cisco provision a new Secure Cloud Analytics portal for you. As you configure Security Analytics and Logging (SaaS), Cisco automatically provisions a sensor named `connection-events`, dedicated to your Firepower event data. See

https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging/0201_Request_a_Stealthwatch_Cloud_Portal for more information.

Because the **Firewall Analytics and Monitoring** license applies dynamic entity modeling to Firepower event data only, you do not need to deploy additional sensors to your network for this license. In contrast, because the **Total Network Analytics and Monitoring** license applies dynamic entity modeling to both Firepower event data and on-premises network traffic, to take full advantage of the license capabilities, deploy additional sensors to your network.



Contact [Cisco Support](#) if you complete your CDO configuration and do not see the `connection-events` sensor in your Secure Cloud Analytics portal.

Sensor Media Installation and Configuration

Before you start the installation, review the instructions to understand the process as well as the preparation, time, and resources you'll need for the installation and configuration.

There are two options for this installation:

- **Installing the Sensor on a Virtual Machine:** If you install a sensor on a virtual machine, you can boot from the .iso file directly.
- **Installing the Sensor on a Physical Appliance:** If you install a sensor on a physical appliance, you'll create bootable media using the .iso file, then restart the appliance and boot from that media.



The installation process wipes the disk on which the sensor will be installed, before installing the sensor. Before you start the installation, confirm that the physical appliance or virtual machine where you're planning to install the sensor does not contain any data you want to save.

Creating Boot Media

If you are deploying a sensor to a physical appliance, you deploy an .iso file which installs the sensor, based in Ubuntu Linux.

If you write the .iso file to an optical disc, such as a CD or DVD, you can reboot the physical appliance with the optical disc in an optical disc drive, and choose to boot from the optical disc.

If you create a USB flash drive with the .iso file and the Rufus utility, you can reboot the physical appliance, insert the USB flash drive into a USB port, and choose to boot from the USB flash drive.



If you deploy a sensor without using an ISO, you may need to update the local appliance's firewall settings to allow traffic. We highly recommend that you deploy the sensor using the provided ISO.



Creating a bootable USB flash drive deletes all information on the flash drive. Ensure that the flash drive does not have any other information on it.

Download the sensor ISO file

Download the latest version of the sensor ISO from the web portal. Use this either to install (for a new sensor) or reinstall (to upgrade an existing sensor).

1. Log in to your web portal UI as an administrator.
2. Select **Help (?) > Sensor Install**.
3. Click the .iso button to download the latest ISO version.
4. Go to [Create a Bootable Optical Disc](#) or [Create a Bootable USB Flash Drive](#).

Create a Bootable Optical Disc

Follow your manufacturer's instructions to copy the .iso file to an optical disc.

Create a Bootable USB Flash Drive

1. Insert a blank USB flash drive into a USB port on the appliance you want to use to create the bootable USB flash drive.
2. Log in to the workstation.
3. In your web browser, go to the Rufus utility website.
4. Download the latest version of the Rufus utility.
5. Open the Rufus utility.
6. Select the USB flash drive in the **Device** drop-down.
7. Select `Disk` or `ISO image` from the **Boot selection** drop-down.
8. Click **SELECT** and select the sensor ISO file.
9. Click **START**.



Creating a bootable USB flash drive deletes all information on the flash drive. Ensure that the flash drive does not have any other information on it.

Installing the Sensor

1. Choose the boot method for the .iso as follows:
 - **Virtual Machine:** If you are installing on a virtual machine, boot from the .iso file.
 - **Physical Appliance:** If you are installing on a physical appliance, insert the bootable media, restart the appliance, and boot from the bootable media.
2. Select **Install Observable Network Appliance** at the initial prompt, then press Enter.
3. **Select a language** from the language list using the arrow keys, then press Enter.
4. **Select your location** from the country list using the arrow keys, then press Enter.
5. You have the following options:
 - **Configure the keyboard** by selecting `Yes` using the arrow keys, press Enter, then select your **Keyboard layout** and press Enter.
 - If you use a standard US-English keyboard, select `No` to accept the default, then press Enter.
6. Select the **Country of origin for the keyboard** using the arrow keys, then press Enter.
7. Select your **Keyboard layout** using the arrow keys, then press Enter.
8. **Configure the Network** and select the primary network interface to be used as the Control interface (for managing the sensor and for collecting flow data from network devices) using the arrow keys, then press Enter.


 All other network interfaces are automatically configured as Mirror interfaces.


9. Wait for the installation process to detect appliance components and perform additional setup. The installation process uses DHCP to configure the primary network interface you selected as the Control interface.

If your network does not use DHCP, or the system displays a Network auto configuration failed message, do the following:

- Select **Configure network manually** and press Enter.
- Enter an IP address for the appliance, select **Continue** with the arrow keys, and press Enter.
- Enter a **Netmask**, select **Continue** with the arrow keys, and press Enter.

- Enter a **Gateway** router IP address, select **Continue** with the arrow keys, and press Enter.
- Enter up to 3 domain **Name server addresses**, select **Continue** with the arrow keys, and press Enter.


 By default, the install will automatically use DHCP and proceed with the install. To override the DHCP IP address, you will need to manually edit the interface after the install is complete.

 We recommend that you enter a local authoritative name server address if you have one deployed in your network.

10. Enter the **Full name for the new user**, which is associated with a non-root account for non-administrative permissions, then select **Continue** with the arrow keys and press Enter.
11. Enter the **Username for your account**, which is the non-root account with non-administrative permissions, then select **Continue** with the arrow keys and press Enter.
12. **Choose a password for the new user**, then select **Continue** with the arrow keys and press Enter.
13. **Re-enter password to verify**, then select **Continue** with the arrow keys and press Enter.

If you did not enter the same password twice, try again.

14. Select **Yes** with the arrow keys to **Encrypt your home directory**, then press Enter.
15. **Select your time zone** with the arrow keys, then press Enter.

 The account you create during setup is the only account you can use to access the virtual machine. This installation does not create a separate Secure Cloud Analytics portal account.

16. Select **Guided - use entire disk** to partition the disk drive, then press Enter. Select the other options if you want to perform advanced disk configuration.
17. **Select disk to partition**, then press Enter.
18. Select **Finish partitioning and write changes to disk** with the arrow keys, then press Enter.
19. Select **Yes** to confirm your action, then press Enter.

 This action deletes all data on the drive. Ensure it is empty before proceeding.

Wait several minutes for the installer to install the required files.

20. Enter **HTTP proxy information** if you use an HTTP proxy, or leave the field blank if you do not use one, then select **Continue** with the arrow keys and press Enter.

Wait for the installer to perform configuration.

21. Select an update policy from the list with the arrow keys, then press Enter. Cisco recommends you select **Install security updates automatically**.

Wait for the installer to perform configuration and install additional packages.


22. Select **Yes to Install the GRUB boot loader to the master boot record** using the arrow keys, then press Enter.

Wait for the installer to install the GRUB boot loader, then finish configuration.

23. When the installer displays **Installation Complete**, select **Continue** with the arrow keys, then press Enter to remove the boot media, finish configuration, and restart the appliance.

24. After the appliance restarts, log in with the created account to ensure your credentials are correct.

What to Do Next

- If restricting access to your private environments, make sure that communication with the relevant IPs is allowed. Go to your Secure Cloud Analytics web portal, click the  (**Help**) icon and select **On-Prem Sensor Install** to see the list of public IPs used by Secure Cloud Analytics.
- If you are using the sensor to collect network flow traffic, such as NetFlow, see [Configuring a Sensor to Collect Flow Data](#) for more information on configuring the sensor.
- If you are using the sensor and attaching it to SPAN or mirror ports to collect mirrored traffic, see [Attaching Sensors to the Web Portal](#) for more information on adding sensors in the Secure Cloud Analytics web portal.
- If you are configuring the sensor to pass Enhanced NetFlow telemetry, see the [Cisco Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#) for more information.

Attaching Sensors to the Web Portal

Once a sensor is installed, it will need to be linked with your portal. This is done by identifying the sensor's public IP address and entering it into the web portal. If you cannot

determine the sensor's public IP address, you can manually link the sensor to your portal using its unique service key.

The sensor can connect to the following portals:

- <https://sensor.ext.observbl.com> (US)
- <https://sensor.eu-prod.observbl.com> (EU)
- <https://sensor.anz-prod.observbl.com> (Australia)



If multiple sensors are staged in a central location, such as an MSSP, and they are intended for different customers, the public IP should be removed after each new customer is configured. If a public IP address of the staging environment is used for multiple sensors, a sensor could be incorrectly attached to the wrong portal.



If you are using proxy server, complete the steps in the [Configuring Proxy](#) section to enable communication between the sensor and the Secure Cloud Analytics web portal.

Finding and Adding a Sensor's Public IP Address to a Portal

1. SSH into the sensor and login as an administrator.
2. At the command prompt, enter `curl https://sensor.ext.observbl.com` and press **Enter**. The `error` value of `unknown identity` means that the sensor is not associated with a portal. See the following image for an example.

```
observable@ona-e37255:/opt/observbl-ona/logs/ipfix$ curl https://sensor.ext.observbl.com
{
  "error": "unknown identity",
  "identity": "72.163.2.237"
}observable@ona-e37255:/opt/observbl-ona/logs/ipfix$
```

3. Copy the `identity` IP address.
4. Log out of the sensor.
5. Log into the web portal as a site administrator.
6. Select the **sensor (🟢) icon > Public IP**.
7. Enter the `identity` IP address in the Public IP field. See the following image for an example.

- Click **Add IP**. After the portal and sensor exchange keys, they establish future connections using the keys, not the public IP address.

i It can take up to 10 minutes before a new sensor is reflected in the portal.

Manually Add a Portal's Service Key to a Sensor

This procedure is **not** required if you already added a sensor's public IP address to the web portal. We recommend you try that before trying this procedure.

- i** Manually adding a portal's service key to a sensor is intended primarily for older sensors that you deployed before ISO version

`ona-18.04.1-server-amd64.iso`

available as of December 2018. You can also redeploy older sensors using the current version of the sensor ISO, available in the web portal.

If you cannot add a sensor's public IP address to the web portal, or you are an MSSP managing multiple web portals, edit a sensor's `config.local` configuration file to manually add a portal's service key to associate the sensor with the portal.

- i** This key exchange is done automatically when using the public IP address in the previous section.

- Log into the portal web UI as an administrator.
- Select **Settings > Sensors**.
- Navigate to the end of the sensor list and copy the **Service key**. See the following image for an example.

Service key: `7785YGXksPsBfltfAZuiD7uA3Ya73V8j613bWX`

4. SSH login to the sensor as an administrator.
5. At the command prompt, enter this command:
`sudo nano opt/obsrvbl-ona/config.local` and press **Enter** to edit the configuration file.

6. Beneath the line `# Service Key`, add the following line, replacing `<service-key>` with the following portal's service key:

```
OBSRVBL_SERVICE_KEY="<service-key>"
```

See the following for an example.

```

observable@ona-e37255: ~
GNU nano 2.5.3 File: opt/obsrvbl-ona/config.local
# Service Key
OBSRVBL_SERVICE_KEY="7785YGXksPsBfltfAZuiD7uA3Ya73V8j613bWX"

```

7. Press `Ctrl + O` to save the changes.
8. Press `Ctrl + X` to exit.
9. At the command prompt, enter `sudo service obsrvbl-ona restart` to restart the Secure Cloud Analytics service.

Configuring Proxy

If you are using proxy server, complete the following steps to enable communication between the sensor and the web portal.

1. SSH into the sensor and login as an administrator.
2. At the command prompt, enter this command:
`sudo nano opt/obsrvbl-ona/config.local` and press **Enter** to edit the configuration file.
3. Add the following line, replacing `proxy.name.com` with your proxy server's hostname or IP address and `Port` with your proxy server's port number:
`HTTPS_PROXY="proxy.name.com:Port"`

i HTTP may be supported in certain situations. [Contact Support](#) for more information.

4. Press Ctrl + 0 to save the changes.
5. Press Ctrl + x to exit.
6. At the command prompt, enter `sudo service obsrvbl-ona restart` to restart the Secure Cloud Analytics service.

Confirm a Sensor's Portal Connection

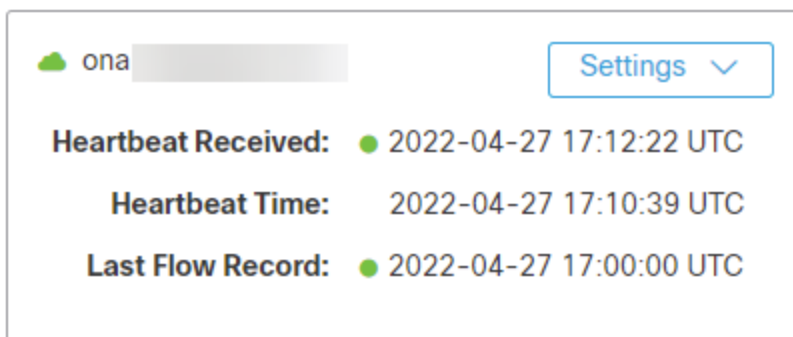
After a sensor is added to the portal, confirm the connection.

i If you manually linked a sensor to the web portal by updating the `config.local` configuration file using a service key, using the `curl` command to confirm the connection from the sensor may not return the web portal name.

1. SSH into the sensor as an administrator.
2. At the command prompt, enter `curl https://sensor.ext.obsrvbl.com` and press **Enter**. The sensor returns the portal name. See the following image for an example.

```
observable@ona-e37255:/opt/obsrvbl-ona$ curl https://sensor.ext.obsrvbl.com
{"welcome": "cisco-demo"}
observable@ona-e37255:/opt/obsrvbl-ona$
```

3. Log out of the sensor.
4. Log into the portal web UI.
5. Select **Settings > Sensors**. The sensor appears in the list.



Configuring a Sensor to Collect Flow Data

A sensor creates flow records from the traffic on its Ethernet interfaces by default. This default configuration assumes that the sensor is attached to a SPAN or mirror Ethernet port. If other devices on your network can generate flow records, you can configure the sensor in the web portal UI to collect flow records from these sources and send them to the cloud.

If the network devices generate different types of flows it is recommended to configure the sensor to collect each type over a different UDP port. This also makes troubleshooting easier. By default, the local sensor firewall (`iptables`) has ports 2055/UDP, 4739/UDP, and 9995/UDP open. You must open additional UDP ports in the web portal UI if you want to use them.

You can configure collection of the following flow types, with the following ports:

- NetFlow v5 - Port 2055/UDP (open by default)
- NetFlow v9 - Port 9995/UDP (open by default)
- IPFIX - Port 9996/UDP
- sFlow - Port 6343/UDP

Certain network appliances must be selected in the web portal UI before they will work properly:


- Cisco Meraki - Port 9998/UDP
- Cisco ASA - Port 9997/UDP
- SonicWALL - Port 9999/UDP




Meraki firmware version 14.50 aligns Meraki log export format with NetFlow format. If your Meraki device runs firmware version 14.50 or greater, configure your sensor with a **Probe Type** of `NetFlow v9` and a **Source** of `Standard`. If your Meraki device runs a firmware version older than 14.50, configure your sensor with a **Probe Type** of `NetFlow v9` and a **Source** of `Meraki MX` (below ver. 14.50).

Configuring Sensors for Flow Collection

1. Log in to your portal web UI as an administrator.
2. Select **Settings > Sensors**.
3. Click **Change settings** for the sensor you added.
4. Select **NetFlow/IPFIX**.

 This option requires an up-to-date sensor version. If you do not see this option, select **Help (?) > Sensor Install** to download a current version of the sensor ISO.

5. Click **Add New Probe**.
6. Select a flow type from the **Probe Type** drop-down.
7. Enter a **Port** number.

 If you want to pass Enhanced NetFlow to your sensor, ensure that the UDP port you configure is not one that is also configured for Flexible NetFlow or IPFIX in your sensor configuration. For example, configure port 2055/UDP for Enhanced NetFlow, and port 9995/UDP for Flexible NetFlow. See the [Configuration Guide for Enhanced NetFlow](#) for more information.

8. Select a **Protocol**.
9. Select a **Source device** from the drop-down.
10. Click **Save**.

What to Do Next

- If you purchased a Cisco Defense Orchestrator (CDO) **Total Network Analytics and Monitoring** license, and are integrating CDO with Secure Cloud Analytics, see https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Private Network Monitoring Integration for Kubernetes

You can integrate Secure Cloud Analytics with a Kubernetes cluster to provide additional information in the Secure Cloud Analytics web UI about the nodes within that cluster. To integrate Kubernetes with Secure Cloud Analytics, create a Kubernetes secret for your cluster which contains an integration service key. Then, create a new service account and bind it to the read-only cluster role. Then, configure a DaemonSet configuration file to schedule sensors as pods for deployment to nodes within the cluster. Finally, create the DaemonSet. After several minutes, the deployed sensors appear in the Secure Cloud Analytics web UI.

Configuring Kubernetes Integration

Configure integration with Kubernetes

1. Install `kubectl` on your cluster. See the Kubernetes Tasks documentation for installing and setting up `kubectl` for more information.
2. Log in to your Kubernetes cluster as an administrator.
3. Log in to your Secure Cloud Analytics web portal UI as an administrator.
4. In the Secure Cloud Analytics web portal, select **Settings > Integrations > Kubernetes**.
5. Follow the instructions to configure Kubernetes integration.

Viewing Deployed Sensors from the Secure Cloud Analytics Web UI

After you verify that your sensors are deployed to nodes within the cluster, wait several minutes, then log in to your Secure Cloud Analytics web UI. The sensors list updates to display your newly deployed sensors within the Kubernetes cluster.

View deployed Sensors from the Secure Cloud Analytics Web UI

1. Log in to your Secure Cloud Analytics web UI as an administrator.
2. Select **Settings > Sensors** to view the deployed sensors.

Public Cloud Monitoring Configuration

The following sections describe the steps for configuring public cloud monitoring and the Secure Cloud Analytics web portal for the following integrations:

- [Amazon Web Services \(AWS\)](#)
- [Google Cloud Platform \(GCP\)](#)
- [Microsoft Azure cloud deployment](#)

Public Cloud Monitoring Configuration for Amazon Web Services

Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring) is a visibility, threat identification, and compliance service for Amazon Web Services (AWS). Secure Cloud Analytics consumes network traffic data, including Virtual Private Cloud (VPC) flow logs, from your AWS public cloud network. It then performs dynamic entity modeling by running analytics on that data to detect threats and indicators of compromise. Secure Cloud Analytics consumes VPC flow logs directly from your AWS account using a cross-account IAM role with the proper permissions. In addition, Secure Cloud Analytics can consume other sources of data, like CloudTrail and IAM, for additional context and monitoring.

To configure an **S3 bucket** to store your flow logs, and Secure Cloud Analytics to ingest these flow logs:

1. In AWS, enable VPC flow logging for a VPC, then configure an S3 bucket to which you export the flow logs. See [Configuring S3 Bucket Flow Log Data Storage](#) for more information.
2. In AWS, configure an IAM access policy and IAM role to allow Secure Cloud Analytics the permission to access and ingest the flow logs. See [Configuring AWS Permission to Access Flow Log Data](#) and [Configuring an IAM Role to Access Flow Log Data](#) for more information.
3. In the Secure Cloud Analytics web portal, update the configuration with the S3 bucket and IAM role to enable AWS flow log data ingestion. See [Configuring Secure Cloud Analytics to Access Flow Log Data from an S3 Bucket](#) for more information.

Configuring S3 Bucket Flow Log Data Storage


You can store your flow log data in an existing S3 bucket, or you can create a new S3 bucket when you enable flow logging. Then, we recommend you configure the bucket to delete the flow logs after they are no longer needed to reduce the storage costs of flow log monitoring.




To configure VPC Flow Logs on multiple existing VPCs, a script is available to assist with configuration: <https://github.com/obsrvbl-oss/aws-setup>. For more information on how to use AWS CloudShell to run the script, go to <https://docs.aws.amazon.com/cloudshell/latest/userguide/getting-started.html>.

Associate an S3 Bucket with a VPC


1. Log in to your AWS Management Console, then access the VPC dashboard.
2. Select **Your VPCs**.
3. Right-click a VPC, then select **Create Flow Log**.
4. Select one of the following options from the **Filter** drop-down:
 - Select `All` to log both accepted and rejected IP traffic, allowing Secure Cloud Analytics to see both types of traffic.
 - Select `Accept` to log only accepted IP traffic, allowing Secure Cloud Analytics to see only accepted traffic.
5. Select the `Send to an S3 bucket` **Destination**.
6. Enter an **S3 bucket ARN** in which you want to store flow log data.

 If the S3 bucket does not exist, AWS creates it after you commit your changes.


7. In the Log record format pane, select **Custom format**.
8. Select all attributes from the **Log format** drop-down list.

 Make sure to follow Steps 7 and 8. The [Troubleshooting: Virtual Private Cloud \(VPC\) Flow Logs](#) section provides information that may help if these steps are missed.

9. Click **Create**.

 If restricting access to this S3 bucket based on IP, make sure that communication with the relevant IPs is allowed. Go to your Secure Cloud Analytics web portal, select **Settings > Integrations > AWS > About** to see the list of public IPs used by Secure Cloud Analytics.

Configure S3 Bucket to Minimize Cost (Recommended)

 The following configuration will delete any objects in the bucket, including flow logs, after 1 day. We recommend this configuration if you are only storing VPC flow logs in this bucket for use with Secure Cloud Analytics.

1. Log in to the AWS Console for S3.
2. In the **Buckets** list, choose the name of the bucket where you want to store VPC flow logs.

-
3. Select the **Management** tab.
 4. In the Lifecycle rules section, click **Create lifecycle rule**.
 5. Enter a unique name for the Lifecycle rule, for example `Expire after 1 day`.
 6. For the scope of the lifecycle rule, select **This rule applies to all objects in the bucket**.
 7. Check the **I acknowledge that this rule will apply to all objects in the bucket** check box.
 8. Under Lifecycle rule actions, select **Permanently delete previous versions of objects**.
 9. Under Permanently delete noncurrent versions of objects, set **Days after objects become noncurrent** to **1**.
 10. Click **Create rule**.
 11. Back in Lifecycle Configuration, click the radio button next to the rule just created, and in the Actions drop-down, click **Enable rule**.

Configuring AWS Permission to Access Flow Log Data

Create a new IAM policy, using the JSON configuration displayed in the Secure Cloud Analytics web portal. This policy contains permissions to allow Secure Cloud Analytics access to the flow log data.

To evaluate your AWS cloud posture, you must grant additional permissions to the IAM policy in AWS. The AWS About page in Secure Cloud Analytics lists the required permissions in the JSON object that starts with "Sid": "CloudCompliance".

If you are a customer integrating Secure Cloud Analytics with AWS for the first time, and do not want to grant these additional permissions, you can remove this object, but you will not be able to use the Cloud Posture report.

Create a Policy with Permission to Access Flow Log Data

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Integrations > AWS > About**.
3. Review the instructions to access AWS resources.
4. Copy the **Policy Document** JSON configuration and paste it into a plaintext editor.
5. Review the JSON object that starts with "Sid": "CloudCompliance" for the additional permissions Secure Cloud Analytics requires to evaluate your AWS cloud posture. You have the following options:


-
- If you do not want to grant these additional permissions, delete the JSON object that starts with "Sid": "CloudCompliance". You will not be able to evaluate your AWS cloud posture in Secure Cloud Analytics. Continue to the next step.
 - If you want to grant these additional permissions to evaluate your AWS cloud posture, continue to the next step.
6. Log in to your AWS Management Console, and access the IAM dashboard.
 7. Select **Policies**.
 8. Click **Create policy**.
 9. Select the **JSON** tab.
 10. Copy the policy JSON configuration from your plaintext editor and paste it into the JSON editor.
 11. Click **Review policy**.
If the policy validator throws an error, review the text that you copied and pasted.
 12. Enter `swc_policy` in the Name field.
 13. Enter a Description, such as `Policy to allow Secure Cloud Analytics to read events and log data.`
 14. Click **Create policy**.

Configuring an IAM Role to Access Flow Log Data

After you create the IAM policy, create an IAM role that allows Secure Cloud Analytics to access flow log data.

Configure an IAM Role with Permission to Access Flow Log Data

1. Log in to your AWS Management Console, then access the IAM dashboard.
2. Select **Roles**.
3. Select **Create role**.
4. Select the `Another AWS account role type`.
5. Enter `757972810156` in the Account ID field.
6. Select the `Require external ID` option.
7. Enter your Secure Cloud Analytics web portal name as the **External ID**.

 Your web portal name is embedded in the portal URL, in the format `https://portal-name.obsrdbl.com`. For example, if your web portal URL is `https://example-client.obsrdbl.com`, enter `example-`



`client` as the External ID. The integration configuration fails if you enter the entire URL.

8. Click **Next: Permissions**.
9. Select the `swc_policy` policy that you just created.
10. Click **Next: Tagging**.
11. Click **Next: Review**.
12. Enter `swc_role` as the **Role name**.
13. Enter a **Description**, such as `Role to allow cross-account access`.
14. Click **Create role**.
15. Copy the role ARN and paste it into a plaintext editor.

Configuring Secure Cloud Analytics to Access Flow Log Data from an S3 Bucket

To complete your flow log configuration, enter the IAM role and S3 bucket name in the Secure Cloud Analytics web portal, then modify the S3 bucket policy in AWS using the configuration provided by Secure Cloud Analytics when you add the S3 bucket name.

If you recently enabled VPC flow logging in your account, wait ten minutes before configuring Secure Cloud Analytics to ingest flow log data. The system may return an error when you add the **S3 Path** name, if the S3 bucket contains no logs; AWS generates VPC flow logs approximately every ten minutes.

Configure Secure Cloud Analytics to Ingest Flow Log Data Stored in a S3 Bucket

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Integrations > AWS > Credentials**.
3. Click **Add New Credentials**.
4. Enter a descriptive **Name**.
5. Copy the saved role ARN from the plaintext editor and paste it into the **Role ARN** field.
6. Click **Create**.
7. Select **Settings > Integrations > AWS > VPC Flow Logs**.
8. Click **Add VPC Flowlog**.
9. Enter the name of the S3 bucket that contains your flow log data in the **S3 Path** field.



You can add more than one configured S3 bucket. You only need to configure one IAM access policy and role for your Secure Cloud Analytics integration with AWS.

10. Select **Credentials** for the S3 bucket, then click **Setup Instructions**.

The system displays a bucket policy JSON configuration, updated with the S3 bucket path and credentials.

11. Copy the displayed bucket policy JSON configuration and paste it into a plaintext editor.



Keep this browser window open. You complete the Secure Cloud Analytics web portal configuration after configuring the S3 bucket policy.

Configure the S3 Bucket Policy to Allow Secure Cloud Analytics to Ingest Flow Log Data

1. Log in to your AWS Management Console, then access the IAM dashboard.
2. In the IAM dashboard, select **Policies**.
3. Click **Create Policy**.
4. Select the JSON tab.
5. Copy the bucket policy JSON configuration from the plaintext editor and paste it into the policy editor, overwriting the existing bucket policy.
6. Click **Review policy**.
7. Enter a policy **Name**.
8. Enter an optional policy **Description**.
9. Click **Create policy**.
10. In the IAM dashboard, select **Roles**.
11. Select `swc_role`.
12. In the Permissions tab, click **Attach policies**.
13. Select the policy name you entered in step 6.
14. Click **Attach policy**.
15. In the Secure Cloud Analytics web portal, click **Create** for the S3 bucket path and credentials you just entered.



The system displays an error if it does not have the correct permissions to ingest flow log data from the S3 bucket. For assistance, contact [Cisco Support](#) with your portal name and S3 bucket name.

Verifying AWS Integration

After you complete the AWS integration, in the **Settings** menu, the Sensors page displays a new sensor with the following name:

AWS: *s3-bucket-name*

This sensor entry displays the health of the integration, or the S3 bucket name, but does not directly allow configuration from the sensors page.



It may take the web portal up to 24 hours after you complete AWS configuration to start displaying traffic and entity data.

Verify AWS Integration

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Sensors**. Verify that the page displays the S3 bucket name.
3. Select **Integrations > AWS > Permissions**. Verify that the displayed AWS permissions match your expectations.

Public Cloud Monitoring Configuration for Google Cloud Platform

Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring) is a visibility, threat identification, and compliance service for Google Cloud Platform (GCP). Secure Cloud Analytics consumes network traffic data, including Virtual Private Cloud (VPC) flow logs, from your GCP public cloud network. It then performs dynamic entity modeling by running analytics on that data to detect threats and indicators of compromise. Secure Cloud Analytics consumes VPC flow logs directly from your GCP account using a cross-account IAM service account with the proper permissions.

Single GCP Project Configuration

To configure GCP to generate and store flow log data for **a single project**, and Secure Cloud Analytics to ingest that data:

1. In GCP, configure a service account with the proper permissions to view flow log and other data, and save the JSON credentials. See [Configure a Service Account to View VPC Flow Logs](#) for more information.
2. In GCP, enable flow logging and the Stackdriver monitoring API for metrics gathering. See [Configure GCP to Generate VPC Flow Logs and Enable Permissions](#) for more information.
3. In the Secure Cloud Analytics web portal UI, upload the service account JSON credentials. See [Upload JSON Credentials](#) for more information.

If you have a high-throughput GCP environment, you can optionally configure Pub/Sub to deliver flow log data to Secure Cloud Analytics:



We strongly recommend configuring Pub/Sub to prevent the integration from exceeding GCP Stackdriver API quotas and dropping flow data.

1. Determine if your deployment is high-throughput. See [Identifying a High-throughput Environment](#) for more information.
2. Configure a Pub/Sub topic to ingest flow log data, and a Pub/Sub subscription for the topic to deliver the flow log data. See [Creating a GCP Pub/Sub Subscription](#) for more information.

Multiple GCP Project Configuration

To configure GCP to generate and store flow log data for **multiple projects**, and Secure Cloud Analytics to ingest that data:

1. In GCP, configure a service account with the proper permissions to view flow log and other data, and save the JSON credentials. Configure the additional projects to use a single service account. See [Configure a Service Account to View VPC Flow Logs](#) for more information.
2. In GCP, configure the additional projects to use the service account. See [Configuring a Single Service Account to View VPC Flow Logs for Multiple Projects](#) for more information.
3. In GCP, enable flow logging and the Stackdriver monitoring API for metrics gathering. See [Configure GCP to Generate VPC Flow Logs and Enable Permissions](#) for more information.
4. In the Secure Cloud Analytics web portal UI, upload the service account JSON credentials. See [Upload JSON Credentials](#) for more information.

If you have a high-throughput GCP environment, you can optionally configure Pub/Sub to deliver flow log data to Secure Cloud Analytics:



We strongly recommend configuring Pub/Sub to prevent the integration from exceeding GCP Stackdriver API quotas and dropping flow data.

1. Determine if your deployment is high-throughput. See [Identifying a High-throughput Environment](#) for more information.
2. Configure a Pub/Sub topic to ingest flow log data, and a Pub/Sub subscription for the topic to deliver the flow log data. See [Creating a GCP Pub/Sub Subscription](#) for more information.
3. Configure additional Pub/Sub topics and subscriptions for the additional projects. See [Configuring Pub/Sub Topics and Subscriptions](#) for more information.

Configure a Service Account to View VPC Flow Logs

To configure the IAM service account, create a custom role with permissions required to gather information for Secure Cloud Analytics. Then, create the service account, and associate several roles, including the custom role. GCP creates the account with private key information. Save the private key in a secure location.

1. In your GCP console, select **IAM & Admin > IAM > Service Accounts**.
2. Click **Create service account**.
3. In the **Service account name** field, enter `logs-viewer`.
The Cloud console generates a service account ID based on this name. Edit the ID if necessary. You cannot change the ID later.
4. Click **Create and continue**.

5. Click the **Select a role** drop-down, then select the **Logs Viewer** role.
6. Click **Add another role**.
7. Click the new **Select a role** drop-down, then select the **Compute Viewer** role.
8. Repeat steps 6 and 7 to add the following roles: **Monitoring Viewer** and **Pub/Sub Subscriber**.
9. **(Optional)** For cloud posture analysis, repeat steps 6 and 7 to add the following roles: **Security Center Service Agent** and **Security Reviewer**.
10. Click **Continue**.
11. Click **Create key**.
12. Select `JSON` as the **Key type**, then click **Create**.



Save the generated JSON private key file in a secure location, as it contains the information necessary for the account to access the VPC flow logs.

13. Click **Close** after saving the JSON private key.
14. Click **Done**.



If restricting access to your GCP environment, make sure that communication with the relevant IPs is allowed. Go to your Secure Cloud Analytics web portal, select **Settings > Integrations > GCP > About** to see the list of public IPs used by Secure Cloud Analytics.

What To Do Next

- If you want to monitor a **single project**, enable flow logging in your deployment. See [Configure GCP to Generate VPC Flow Logs and Enable Permissions](#) for more information.
- If you want to monitor **multiple projects**, associate your service account with each additional project before you enable flow logging in your deployment. See [Configuring a Single Service Account to View VPC Flow Logs for Multiple Projects](#) for more information.

Configuring a Single Service Account to View VPC Flow Logs for Multiple Projects

If you want to **monitor multiple projects** in your GCP deployment, you can use a single service account to monitor the projects. Enable the cloud resource manager API for each project you want to monitor, then add the created service account email address and proper role permissions to that project.

Locate Your Service Account's Email Address

1. In your GCP console, select **IAM & Admin > IAM**.
2. Click the edit icon for your new service account.
3. Copy the **Member** email address, in the following format, and paste this into a plain text editor:

```
[account-name]@[project-id].[gcp-info].com
```

Enable the Cloud Resource Manager API for an Additional Project

1. In your GCP console, select **APIs & Services > Library**.
2. Click **Select** for your project.
3. Search for `Cloud Resource Manager API`, select **Cloud Resource Manager API**, and click **Enable**.

Add a Service Account to an Additional Project

1. In your GCP console, select **IAM & Admin > IAM**.
2. Select an additional project from the project drop-down.
3. Click **Add**.
4. Copy the Member service account email address from the plaintext editor and paste it in the New members field.
5. Click the **Select a role** drop-down. Enter, then select the **Logs Viewer** role.
6. Click **Add Another Role**.
7. Click the new **Select a role** drop-down. Enter, then select the **Compute Viewer** role.
8. Repeat steps 6 and 7 to add the following roles: **Monitoring Viewer** and **Pub/Sub Subscriber**.
9. **(Optional)** For cloud posture analysis, repeat steps 6 and 7 to add the following roles: **Security Center Service Agent** and **Security Reviewer**.
10. Click **Save**.
11. Repeat steps 2-9 for each additional project.

What To Do Next

- Enable flow logging in your deployment. See [Configure GCP to Generate VPC Flow Logs and Enable Permissions](#) for more information.

Configure GCP to Generate VPC Flow Logs and Enable Permissions

After you configure the service account, enable flow logging in your GCP deployment per subnet before making them available for ingestion by Secure Cloud Analytics. Then, enable the Stackdriver Monitoring API, to gather various GCP metrics.

Configure a GCP Subnet to Generate VPC Flow Logs

1. In your GCP console, select **VPC network**.
2. Select a subnet.
3. Click **Edit**.
4. Select **On** from **Flow logs**.
5. Click **Save**. Repeat steps 1-4 for each additional subnet you want to setup.

Enable the Stackdriver Monitoring API (Recommended)



Secure Cloud Analytics uses this permission for the GCP Cloud Function Invocation Spike alert and to monitor the health and status of the integration.

1. In your GCP console, select the Cloud project for which you want to enable the API, and then go to the **APIs & Services** page.
2. Click **Enable APIs and Service**.
3. In the search field, enter **Monitoring**, then select **Stackdriver Monitoring API**.
4. Click **Enable** if the API is not enabled.
5. Click **Save**.

What To Do Next

- Upload the saved JSON credentials to the Secure Cloud Analytics portal. See for more information. [Upload JSON Credentials](#) for more information.

Upload JSON Credentials

To complete configuration, upload your JSON service account credentials to the Secure Cloud Analytics web portal UI.

1. Log in to the Secure Cloud Analytics web portal as a site administrator.
2. Select **Settings > Integrations > GCP > Credentials**.
3. Click **Upload Credentials File**, then select your JSON credentials file.

What To Do Next

- Determine if you have a high-throughput environment, and if so, [configure Pub/Sub to ingest flow log data](#).

Identifying a High-throughput Environment

You can configure a Pub/Sub topic and subscription to guarantee transmission of your flow data in a high-throughput environment. GCP Pub/Sub collection is ideal if your VCP flow data exceeds the logging read limits imposed by GCP and is highly recommended for large GCP deployments.

Review the GCP Logging Quota

To check if your environment is exceeding GCP logging limits with an existing log-based GCP integration:

1. Log in to <https://console.cloud.google.com/apis/api/logging.googleapis.com/quotas>.
2. Select your project.
3. Search for *Quota exceeded errors count (1 min) - Read requests per minute*. If you exceed the quota, see [Creating a GCP Pub/Sub Subscription](#) for more information on configuring Pub/Sub.

Creating a GCP Pub/Sub Subscription

If your GCP deployment has high traffic throughput, we recommend that you configure Pub/Sub for flow log data delivery. To configure Pub/Sub for flow log data ingestion, obtain your primary project ID, create a log export sink, then create a Pub/Sub subscription for the topic.

Find Your GCP Project ID

1. In your GCP console, select **Manage resources**.
2. Select your primary project, and copy the **Project ID**.
3. Paste the Project ID into a text editor.

Create a GCP Log Export Sink for the Project

1. In your GCP console, select **Stackdriver Logging > Logs Router**.
2. Click **Create Sink**.
3. Select **Convert to advanced filter** from the **Filter by label or text search** drop-down field, above the log entries.
4. Copy the following and paste it into a plaintext editor:

```
resource.type="gce_subnetwork"  
logName="projects/MY_PROJECT_  
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

5. Replace `MY_PROJECT_NAME` with your Project ID.
6. Copy the updated text and paste it in the **Filter by label or text search** field, overwriting any existing text.
7. In the Edit Sink pane, enter `vpc_flows-sink` in the **Sink Name** field.
8. Select `Pub/Sub` from the **Sink Service** drop-down.
9. Select `Create new Cloud Pub/Sub topic` from the **Sink Destination** drop-down.
10. Enter `vpc_flows-topic` in the **Name** field, then click **Create**.
11. Click **Create Sink**.

Create a GCP Pub/Sub Subscription for the Project

1. In your GCP console, select **Pub/Sub > Topics**.
2. Select **Create subscription** from `vpc_flows-topic`'s menu.
3. Enter `swc_subscription` in the **Subscription Name** field.
4. Select the `Pull` **Delivery Type**.
5. Enter `600 Seconds` in the **Acknowledgment Deadline** field.
6. Enter `2 hours` in the **Message Retention Duration** field.
7. Uncheck **Retain Acknowledged Messages**.
8. Click **Create**.

What To Do Next

- If you are monitoring **multiple projects**, configure a Pub/Sub topic and subscription for each additional project. See [Configuring Pub/Sub Topics and Subscriptions](#) for more information.

Configuring Pub/Sub Topics and Subscriptions

If you want to monitor multiple projects in your GCP deployment, after you configure Pub/Sub for your primary project, create a log export sink and Pub/Sub subscription for each additional project that references your primary project ID.

Create a GCP Log Export Sink for Additional Projects

1. In your GCP console, select a project other than the primary project.
2. Select **Stackdriver Logging > Logs Router**.

-
3. Click **Create Sink**.
 4. Select **Convert to advanced filter** from the **Filter by label or text search** drop-down field, above the log entries.
 5. Copy the following and paste it into a plaintext editor:

```
resource.type="gce_subnetwork"  
logName="projects/MY_PROJECT_  
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

6. Replace MY_PROJECT_NAME with your **primary** project ID.
7. Copy the updated text and paste it in the **Filter by label or text search** field, overwriting any existing text.
8. In the **Edit Sink** pane, enter vpc_flows-sink in the **Sink Name** field.
9. Enter vpc_flows-sink in the **Sink Name** field.
10. Select Pub/Sub from the **Sink Service** drop-down.
11. Select **Create new Cloud Pub/Sub topic** from the **Sink Destination** drop-down.
12. Enter vpc_flows-topic in the **Name** field, then click **Create**.
13. Click **Create Sink**.
14. Repeat steps 1-13 for each additional project.

Create a GCP Pub/Sub Subscription for Additional Projects

1. In your GCP console, select a project other than the primary project.
2. Select **Pub/Sub > Topics**.
3. Select **Create subscription** from vpc_flows-topic's menu.
4. Enter swc_subscription in the **Subscription Name** field.
5. Select the **Pull Delivery Type**.
6. Enter 600 seconds in the **Acknowledgment Deadline** field.
7. Enter 2 hours in the **Message Retention Duration** field.
8. Uncheck **Retain Acknowledged Messages**.
9. Click **Create**.

Repeat steps 1-9 for each additional project.

Public Cloud Monitoring Configuration for Microsoft Azure

Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring) is a visibility, threat identification, and compliance service for Microsoft Azure. Secure Cloud Analytics consumes network traffic data, including Network Security Group (NSG) flow logs, from your Azure public cloud network. It then performs dynamic entity modeling by running analytics on that data to detect threats and indicators of compromise. Secure Cloud Analytics consumes NSG flow logs directly from your Azure storage account, and uses an application to gain additional context.

Azure User Roles

We recommend configuring the integration as a user with the **Global Administrator** Azure Active Directory (AD) role and **Owner** role for all monitored subscriptions. If that is not possible, contact your Azure AD administrator to ensure that:

1. The user is able to create app registrations. This is allowed by default for member users, although some Azure ADs may disable this. If this is guest user or app registration has been disabled, the **Application Developer** role must be assigned to the user.
2. For each monitored subscription, the user has access to the following Azure resources: authorization, network, storage accounts, and monitoring. These require the **User Access Administrator** and **Contributor** roles be assigned to the user.

See [Azure Permissions Required for Secure Cloud Analytics Integration](#) for more information.

Activate Using a Bash Script

We have developed an experimental Bash script that automates the configuration instructions.

You can download the script from the Secure Cloud Analytics web portal.

Go to **Settings > Integrations > Azure > About**.

To enable the Bash script:

1. Log in to your Azure portal.
2. Click the console icon next to the search bar to launch Azure Cloud Shell. Click **Bash** to open a bash console.
3. Upload the script using the Upload/Download files button.
4. Execute the script with `bash azure_setup.sh` and follow the instructions.



- The script will enable monitoring for all the subscriptions it can discover.
- The script will direct all Network Security Groups of a given location to store their flow logs to the storage account provided.

Create an Azure Resource Group

First, make sure you have one or more resource groups that you want to monitor. You can use existing resource groups, or create a new resource group and populate it with resources, such as virtual machines.

1. Log into your Azure portal.
2. Select **Resource Groups**.
3. Click **Add**.
4. Enter a **Resource group name**.
5. Select your **Subscription**.
6. Select a **Resource group location**.
7. Click **Review + create**.
8. Click **Create**.

Obtain the Azure Active Directory URL and Subscription ID

To provide Secure Cloud Analytics access to Azure metadata services, obtain your Azure Active Directory (AD) URL and Azure subscription ID. Record this information; you will upload this information to the Secure Cloud Analytics web UI at the end of this process to complete your integration with Azure.

1. Log into your Azure portal.
2. Select **Azure Active Directory > Overview**.
3. Copy your Primary domain (e.g., example.onmicrosoft.com) and paste it into a plaintext editor. This is the Azure AD URL.
4. Select **Subscriptions**, then select your subscription.
5. Copy the subscription ID and paste it into a plaintext editor.

Create an Azure AD Application

After you obtain the Active Directory URL and subscription ID, create an application to allow Secure Cloud Analytics to read metadata from your resource groups. Copy the application key after you finish creating the application.



Create **only one application** per Active Directory instance. You can monitor multiple subscriptions in an Active Directory instance by assigning roles to the application. See [Grant Access to an Application](#) for more information.

1. Log into your Azure portal.
2. Select **Azure Active Directory > App Registrations > New Registration**.
3. In the **Name** field, enter `swc-reader`. Leave the others as default.
4. Copy the **Application (client) ID** and paste it into a plain text editor.
5. Select **Certificates and Secrets > New Client Secret**.
6. In the **Description** field, enter `SWC Reader`.
7. In the **Expires** drop-down, select an appropriate expiration date or accept the default value.
8. Click **Add**.
9. Copy the application key **Value** and paste it into a plaintext editor.



Copy the application key now, as you cannot view the key after you navigate away from this page.

Grant Access to an Application

After you register the `swc-reader` app in AD, assign the Monitoring Reader role to it, which allows it to read metadata from your resource groups. Perform the following procedure for each subscription you want to monitor.

1. Log into your Azure portal.
2. Select **Subscriptions**, then select your subscription.
3. Select **Access Control (IAM)**.
4. Select **Add > Add role assignment**.
5. In the **Role** drop-down, select **Monitoring Reader**.
6. In the **Assign access to** drop-down, select **User, group, or service principal**.
7. In the **Search by name or email address** field, enter `swc-reader`.
8. Click **Save**.

Create an Azure Storage Account to Store Flow Log Data

After you assign the Monitoring Reader role to the `swc-reader` app, create a storage account to store the flow log data. Create a binary large object (blob) storage account in the same location as your resource groups.



You can reuse an existing Storage Account if it can store blobs and is in the same location as your resource groups.

After you create the blob storage account, ensure that the firewall rules allow access to the storage account from the internet, so that Secure Cloud Analytics can properly integrate with your Azure deployment.

Create a Blob Storage Account

1. Log into your Azure portal.
2. Select **Storage Accounts**.
3. Click **Add**.
4. Select your **Subscription**.
5. Select the **Resource group** you want to monitor.
6. Enter a **Storage account name**.
7. Select the same **Location** for the storage account as the resource group you specified.
8. Select `Storage v2 (general purpose)` for the **Account kind**.
9. Select a **Replication** option from the drop-down, based on your organization's requirements.
10. Select the `Hot` or `Cool` access tier, depending on how often you plan to have blobs accessed within the storage account.
11. Click **Review + create**.
12. Click **Create**.

Enable Internet Access to the Blob Storage Account

1. From the blob storage account, select the **Firewalls and virtual networks** setting.
2. Select **Allow access from** `All networks`, then save your changes.

Generate an Azure Storage Account Shared Access Signature URL

After you create a storage account, generate a shared access signature (SAS) for the storage account to allow Secure Cloud Analytics permission to retrieve the flow log data from the storage account. Then, copy the Blob service SAS URL. Secure Cloud Analytics uses the Blob service SAS URL to retrieve the flow log data from the storage account.



SAS permissions are time-limited, based on configuration. If your SAS permissions expire, Secure Cloud Analytics cannot retrieve flow log data from the storage account.

-
1. Log into your Azure portal.
 2. Select **More Services > Storage > Storage Accounts**.
 3. Select the storage account configured to store flow log data.
 4. Select **Shared access signature**.
 5. In the **Allowed services** field, select the **Blob**.
 6. In the **Allowed resource types** field, select **Service, Container, and Object**.
 7. In the **Allowed permissions**, select **Read and List**.
 8. Enter a **Start time** corresponding to your current time.
 9. Enter an **End time** corresponding to at least one year from the current time.
 10. In the **Allowed protocols** field, select the **HTTPS only**.
 11. Click **Generate SAS and connection string**.
 12. Copy the **Blob service SAS URL** and paste it into a plaintext editor.



If restricting access to this storage account based on IP, make sure that communication with the relevant IPs is allowed. Go to your Secure Cloud Analytics web portal, select **Settings > Integrations > Azure > About** to see the list of public IPs used by Secure Cloud Analytics.

Enable Azure Network Watcher

After you generate the blob storage SAS URL, enable Network Watcher in the region containing your resource groups, if you have not already enabled it. Azure requires Network Watcher to enable flow logs for your network security groups.

1. Log into your Azure portal.
2. Select **Network Watcher > Overview**.
3. Select the regions list to expand it.
4. Select the menu for the region containing your resource groups, then select **Enable Network Watcher**.

Register Insights Provider

Before activating NSG Flow Logs, enable the `microsoft.insights` provider.


1. Log into your Azure portal.
2. Go to **Subscriptions**, and select your subscription name.
3. Click **Settings > Resource Providers**.
4. Highlight the `microsoft.insights` provider, then click **Register**.

Enable Azure NSG Flow Logs

After you enable Network Watcher, enable network security group (NSG) flow logs for one or more network security groups. These network security groups should correspond with the resource groups you want to monitor.

 Blob storage accounts do not support NSG flow log retention periods.

1. Log into your Azure portal.
2. Select **Network Watcher > NSG flow logs**.
3. Select a network security group to display the Flow Logs settings page.
4. In the **Flow Logs version** field, select `Version 2`.
5. Select the blob **Storage account** for which you configured an SAS in **Generate an Azure Storage Account Shared Access Signature URL**.
6. Select `Off` for the **Traffic Analytics** status.

 Secure Cloud Analytics does not require enabling Traffic Analytics, but you can enable it if your organization wants the functionality.

7. In the **Retention (days)** field, enter a retention time for the logs.
8. Click **Save**.
9. Repeat steps 2 through 8 for each network security group for which you want to enable flow logging.

Secure Cloud Analytics Configuration with Azure

Enter the following information in the Secure Cloud Analytics web portal to complete your integration with Azure:

- [Azure AD URL](#)
- [Subscription ID](#)
- [Application ID](#)
- [Application Key](#)
- [Blob service SAS URL](#)

Configure Secure Cloud Analytics to Ingest Flow Log Data from Azure

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Integrations > Azure > Credentials**.
3. Click **Add New Credentials**.

-
4. Enter your **Azure AD URL**.
 5. Enter the Azure **Application ID**.
 6. Enter the Azure **Application Key**.
 7. Select the **Azure Cloud** environment from the drop-down list.
 8. Click **Create**.
 9. Click **Storage Access**.
 10. Click **New Integration**.
 11. Enter the **Blob Service SAS URL** in the **API Key** field.
 12. Click **Create**.
 13. Select Subscriptions and ensure that your subscription is listed.

Secure Cloud Analytics Web Portal Configuration

The following describes the recommended configuration options available in the Secure Cloud Analytics web portal for initial configuration. These options include:

- private network monitoring sensor configuration
- alert configuration
- subnet configuration
- user and site management

Private Network Monitoring Sensor Configuration

After you deploy sensors on your network, you can use the Secure Cloud Analytics web UI to configure:

- the sensor's display name
- network monitoring settings
- syslog output settings
- SNMP reporting settings

You can also add additional sensors based on the public IP address, and view a sensor's logs.


Adding a Sensor Using its Public IP Address

You can add sensors to the Secure Cloud Analytics web UI using their IP address. After you deploy a sensor, SSH into the sensor and log into retrieve its IP address.

Obtain a sensor's Public IP Address

1. Log in to your sensor's console as an administrator.
2. At the command prompt, enter `curl https://sensor.ext.observbl.com` and press Enter. The error value of `unknown identity` means that the sensor is not associated with a Secure Cloud Analytics deployment.
3. Copy the `identity` IP address.
4. Log out of the sensor.

Add a sensor Using its Public IP Address

1. Log in to your Secure Cloud Analytics web UI.
2. Select the  **(sensors) icon** > **Public IP**.
3. Enter the `identity` IP address in the Public IP field.
4. Click **Add IP**. After the portal and sensor exchange keys, they establish future connections using the keys, not the public IP address.



It can take up to 10 minutes for the Secure Cloud Analytics web UI to display the sensor.

Configuring a Sensor's Display Label

In the Secure Cloud Analytics web UI, you can configure a sensor's display label.

Configure a sensor's Display Label

1. Select **Settings** > **Sensors** > **Sensor List**.
2. Click **Change Settings** for the sensor you want to configure to output to syslog.
3. Select the **Label** tab.
4. Enter a **Label**.
5. Click **Save**.

Configuring a Sensor's Monitoring Settings

In the Secure Cloud Analytics web UI, you can configure which subnets a sensor monitors, and if you use passive DNS, how many packets per second to capture. Removing a subnet range from the sensor's configuration instructs the sensor to ignore packets that are sourced from that subnet.

Confusion arises as to why an entity may be created for an IP address that is not listed in the monitored networks on the sensor. This is because an entity that **is** listed on the monitored ranges has communicated with a non-listed range.

For example, consider a sensor that is configured to monitor only the `192.168.0.0/24` range. The system considers any IP address that transmits traffic in that range to be an entity. In addition, if an entity in the `192.168.0.0/24` range is observed communicating with an IP address in the `10.0.0.0/8` range, the sensor will monitor that traffic, as `192.168.0.0/24` is considered a monitored range. The system also creates an entity for the other IP address in the unmonitored `10.0.0.0/8` range because:

- the 10.0.0.0/8 range is part of the RFC 1918 space, and
- the IP address from that range was observed communicating with a monitored IP address.

If the 10.0.0.0/8 range was not defined for monitoring by the sensor, and two IP addresses in the 10.0.0.0/8 subnet only communicate with each other, neither would be considered an entity, as neither had directly communicated with a defined subnet.

Configure a sensor's Monitoring Settings

1. Select **Settings > Sensors > Sensor List**.
2. Click **Change Settings** for the sensor you want to configure.
3. Select the Monitoring tab.
4. Add one or more CIDR blocks in the **Networks to monitor** field, one per line.
5. Select a number of **Packets per second to capture for PDNS**.
6. Click **Save**.

Configuring a Sensor's Syslog Settings

In the Secure Cloud Analytics web UI, you can configure the sensor to send detected entity observations and alerts to a remote syslog server.

Configure a sensor's Syslog Settings

1. Select **Settings > Sensors > Sensor List**.
2. Click **Change Settings** for the sensor you want to configure to output to syslog.
3. Select the Syslog tab.
4. Select **Enable syslog publishing**.
5. Select the `user` **Syslog** facility.
6. Enter the **IP address of the syslog server**.
7. Enter a **Server port** used for communications between the sensor and syslog server.
8. Click **Save**.

Configuring a Sensor's SNMP Reporting Settings

In the Secure Cloud Analytics web UI, you can configure a sensor to report SNMP information, including OID, to an SNMP server.

Configure a sensor's SNMP Reporting Settings

1. Select **Settings > Sensors > Sensor List**.
2. Click **Change Settings** for the sensor you want to configure to output to syslog.
3. Select the SNMP tab.
4. Select **Enable SNMP reporting**.
5. Select an **SNMP version**.
6. Enter a **Community/User** and an associated **Passphrase**.
7. Enter a **Sensor engineID**.
8. Enter an **OID (ASN.1)**.
9. Enter an **SNMP server** you want the sensor to report to.
10. Enter a **Server port (TRAP)** used for communications between the sensor and SNMP server.
11. Click **Save**.

Viewing a Sensor's Logs

You can view a sensor's log messages in the Secure Cloud Analytics web UI, and download the log messages in a comma-separated value file.

View a sensor's Logs

1. Select **Settings > Sensors > Sensor List**.
2. Select **Sensor List**.
3. For the sensor whose logs you want to view, in the Access Logs pane, click **Most Recent**.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Alerts Configuration

The Alerts settings allow you to configure the following:

- alert expiration times
- alert priority
- IP scanner rules
- watchlist entries

Alert Priority Configuration

Alert types come with default priorities, which affect how sensitive the system is to generating alerts of this type. Alerts default to `low` or `normal` priority. You can configure any alert type to be `low`, `normal`, or `high` priority.

The alert priority is used in conjunction with subnet sensitivity to determine whether an alert will automatically close or not. For example, an Excessive Access Attempts (External) alert type defaults to `low` priority. This alert will be auto-closed for any subnet that is not set to `high`.

Update Alert Priority

1. You have the following options:
 - Select **Settings > Alerts > Priorities**.
 - Select **Monitor > Alerts**, then select **Related Config Links > Alert Priorities**.
2. For an alert type, select an alert **Priority** from the drop-down.

Configuring the Country Watchlist

You can configure the Country Watchlist to alert on traffic that involves countries on the list, based on geolocation information.

Modify the Country Watchlist Entries

1. Select **Settings > Alerts > Country Watchlist**.
2. Click the Filters pane to expand it.
3. Select a **Filter by watched status** from the drop-down to filter the countries, or enter a string in the **Search** field, then click Apply.
4. Select a country to add it to the Country Watchlist, or unselect a country to remove it from the Country Watchlist.

Watchlist Configuration

Watchlists control whether or not traffic from a specific entity will generate an alert. You can configure entries such that traffic involving those entities always causes the system to generate an alert. You can also configure those watchlist entries to expire after a configured time, at which point traffic involving those entities no longer causes the system to generate an alert.

Secure Cloud Analytics supports using third-party threat intelligence lists to generate alerts involving those entities.

Configuring the Internal Connections Watchlist

You can add connections between internal entities to the Internal Connections Watchlist, either by adding a CIDR block or an entity group. If the system detects traffic involving entries on this list, then it generates an alert. You can also set the entries to allow the traffic and not generate an alert.

You can download a comma-separated value file that contains all of your entries.

Add an Entry to the Internal Connections Watchlist

1. Select **Settings > Alerts > Internal Connections Watchlist**.
2. Click **New Watchlist Item**.
3. Enter a watchlist entry **Rule Name** and **Description**.
4. Select a **Connection Rule Type** of `Allowed` if you want connections that match this entry to not generate observations or alerts. Select `NOT Allowed` if you want connections that match this entry to generate observations or alerts.

You must add at least one `NOT Allowed` rule to the Internal Connection Watchlist before adding any `Allowed` rules.

5. Select a **Protocol** from the drop-down list..
6. Select **Source** to expand the field.
7. You have the following options:

Select **CIDR**, then enter an **IP** address and **Bytes/Length** to define the source CIDR block. Enter a **Bytes/Length** of 32 to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.

Select **Entity Groups**, click **Add Entity Group(s)**, select one or more Entity groups, and click **Add to Source**.


8. If you want to limit the source to certain ports, enter individual Source **Ports**, or port ranges.
9. Select **Destination** to expand the field.
10. You have the following options:

Select **CIDR**, then enter an **IP** address and **Bytes/Length** to define the destination CIDR block. Enter a **Bytes/Length** of 32 to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.

Select **Entity Groups**, click **Add Entity Group(s)**, select one or more Entity groups, and click **Add to Destination**.

11. If you want to limit the destination to certain ports, enter individual **Destination Ports**, or port ranges.
12. Click **Save**.

Remove an Entry

1. Select **Settings > Alerts > Internal Connections Watchlist**.
2. Next to the entry you want to remove, click the  **(Remove)** icon.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Configuring Third-party Watchlists


You can add third-party watchlists to Secure Cloud Analytics, using threat intelligence from trusted third-party sources to generate alerts.

You can set these entries to automatically expire, or manually expire a rule, at which point no more alerts are generated. You can also set them to never expire; the system always generates alerts if traffic involving these entities is detected. If a rule is expired, you can manually reinstate it.


Add an Entry to the Third Party Watchlist

1. Select **Settings > Alerts > Third Party Watchlist**.
2. Click **Add External URL**.
3. Enter a watchlist entry **Name**.
4. Enter a **Resource** URL where the third-party watchlist is posted.
5. If you want this entry to function indefinitely, select **Never Expire**. Otherwise, select an **Expiration Date** in the future.
6. Enter a **Threshold** value for the minimum number of entities on the watchlist to be detected before the system generates an alert. This value must be greater than 1.
7. Select **Bidirectional traffic only** if you want the system to generate an alert only if it detects bidirectional traffic involving this entity.
8. Enter an entry **Reason**.
9. Click **Create**.

Manually Expire an Entry

1. Select **Settings > Alerts > Third Party Watchlist**.
2. In the Active table, next to the entry you want to remove, click the  **(Remove)** icon.

Reinstate an Expired Entry

1. Select **Settings > Alerts > Third Party Watchlist**.
2. In the Expired table, next to the entry you want to reinstate, click the  **(Remove)** icon.

Configuring the IPs and Domains Watchlist

You can add external domain names or IP addresses to the IPs and Domain Watchlist. If the system detects traffic involving entities on this list, then it generates an alert.

You can set these entries to automatically expire, or manually expire a rule, at which point no more alerts are generated. You can also set them to never expire; the system always generates alerts if traffic involving these entities is detected. If a rule is expired, you can manually remove it.


Add an Entry to the IPs and Domains Watchlist:

Procedure

1. Select **Settings > Alerts > IPs and Domain Watchlist**.
2. Click **Add Domain or IP**.
3. Enter a watchlist entry **Name**.
4. Enter a **Resource** domain name or IP address whose traffic will trigger an alert.
5. If you want this entry to function indefinitely, select **Never Expire**. Otherwise, select an **Expiration Date** in the future.
6. Select **Bidirectional traffic only** if you want the system to generate an alert only if it detects bidirectional traffic involving this entity.
7. Enter an entry **Reason**.
8. Click **Create**.


Manually expire an entry:

Procedure

1. Select **Settings > Alerts > IPs and Domains Watchlist**.
2. In the Active table, click the  (**Edit**) icon next to an active entry you want to expire.
3. Uncheck **Never Expire**.
4. Enter an **Expiration Date**.
5. Click **Save**.

Remove an expired entry:

Procedure

1. Select **Settings > Alerts > IPs and Domain Watchlist**.
2. In the Expired table, next to the entry you want to remove, click the  (**Remove**) icon.

Uploading an IPs and Domains Watchlist Entries File

You can upload a comma-separated value file with multiple watchlist entries, one entry per line. A file may include domain names, IP addresses, or both. Each line should be in the following format:

```
<title>,<reason>,<identifier>,[is_bidirectional],[expires_on],[threshold]
```

See the following for more information:

Parameter	Required	Allowed Values
<title>	yes	Any alphanumeric characters.
<reason>	yes	Any alphanumeric characters.
<identifier>	yes	One of the following: <ul style="list-style-type: none"> • a valid domain name • a valid IPv4 address
[is_bidirectional]	no	One of the following: <ul style="list-style-type: none"> • <code>true</code> - the system generates an alert only if it detects bidirectional traffic involving this entity • <code>false</code> - the system generates an alert if it detects unidirectional or bidirectional

		<p>traffic involving this entity</p> <p>If undefined, this defaults to <code>false</code>.</p>
<code>[expires_on]</code>	no	<p>A timestamp in the following format:</p> <p><code>YYYY-MM-DDTHH:SS</code>.</p> <p>If undefined, this watchlist entry never expires.</p>
<code>[threshold]</code>	no	<p>A positive integer that represents the number of times the system detects this entity before generating an alert.</p> <p>If undefined, this defaults to 1.</p>

Upload a Domain Name or IP Address Watchlist Entry File

1. Select **Settings > Alerts > IPs and Domains Watchlist**.
2. Click **Upload CSV**.
3. Click **Upload File** to select your file for upload.

Configuring the AWS CloudTrail Event Watchlist

You can configure a watchlist to generate an alert for specific AWS CloudTrail events generated for specific AWS accounts.



When you enable AWS integration, ensure that the `obsrvbl_policy` policy contains the `cloudtrail:LookupEvents` permission. The AWS policy configuration provided by Cisco contains this permission.

You can also download a comma-separated value file containing the watchlist entries.

Add an Entry to the AWS CloudTrail Alert Watchlist

1. Select **Settings > Alerts > AWS CloudTrail Watchlist**.
2. Click **New Watchlist Item**.
3. Select an AWS **Account ID** from the drop-down, or select `<Any Account ID>` to generate an alert if the system detects the CloudTrail event in any of your monitored AWS accounts.
4. Enter a CloudTrail **Event**. See AWS documentation on CloudTrail events for more information on the supported events.
5. Click **Create**.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Configuring the GCP Logging Watchlist

You can configure a watchlist to generate an alert for specific GCP events generated for specific GCP projects.

You can also download a comma-separated value file containing the watchlist entries.

Add an Entry to the GCP Logging Watchlist

1. Select **Settings > Alerts > GCP Logging Watchlist**.
2. Click **New Watchlist Item**.
3. Enter a **GCP Action**. See GCP documentation for more information on the available actions.
4. Select a **GCP Project ID** from the drop-down, or select `<Any Account ID>` to generate an alert if the system detects the action in any of your monitored GCP projects.
5. Click **Create**.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Configuring IP Scanner Rules

You can configure IP scanner rules to suppress alerts for trusted, non-malicious scanners on your network. For example, if penetration testers are searching for vulnerabilities, you can add an IP scanner rules that matches their traffic.

Configure IP Scanner Rules

1. Select **Settings > Alerts > IP Scanner Rules**.
2. Click **Add Rule**.
3. If you want to suppress alerts for a specific IP address, enter an **IP Address**.
4. If you want to suppress alerts for a CIDR block, enter a **CIDR Length** from /1 through /32.
5. Enter **Connected Addresses** to be scanned and excluded from alerts, as an IP address, CIDR block range, IP address range, or comma-separated list of IP addresses, CIDR block ranges, or IP address ranges.

6. Enter **Connected Ports** to be scanned and excluded from alerts, as a port, port range, or comma-separated list of ports or port ranges.
7. If you want to describe the rule in the Secure Cloud Analytics web UI, enter a **Description**.
8. Click **Create**.

Configuring the Azure Activity Log Watchlist

You can configure a watchlist to generate an alert for specific Azure events.

You can also download a comma-separated value file containing the watchlist entries.

Add an Entry to the GCP Logging Watchlist

1. Select **Settings > Alerts > Azure Activity Log Watchlist**.
2. Click **New Watchlist Item**.
3. Select a **Subscription ID** from the drop-down, or select `<Any Subscription ID>` to generate an alert if the system detects the action in any of your monitored Azure projects.
4. Enter an **Operation (or Action)**. See Azure documentation for more information on the available actions.
5. Click **Create**.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Configuring the Azure Advisor Watchlist

You can configure Azure Advisor Recommendations are ingested as Secure Cloud Analytics observations. After ingesting these observations, the system can then generate alerts based on them.

You can also download a Comma Separated Value (CSV) file containing the watchlist entries.

Enable Azure Advisor Recommendations to be Ingested As Observations

1. Select **Settings > Alerts > Azure Advisor Watchlist**.
2. Select **Watching** for an Advisor Recommendation to allow Secure Cloud Analytics to ingest it as an observation.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Updating Alert Expiration

Alerts automatically close after the expiration period if no users have already closed them. You can reopen them after closing them if you need to make updates.

You can configure alerts to stay open indefinitely.

Update the Alert Expiration Period

1. Select **Settings > Alerts > Alert Expiration**.
2. Enter a number of **Days before alerts expire**. Enter 0 to have alerts stay open indefinitely.
3. Click **Save**.

Reviewing the Cloud Posture Watchlist

You can review the Cloud Posture frameworks and recommendations against which the system may evaluate your public cloud accounts.

Review the Cloud Posture Watchlist

1. Select **Settings > Alerts > Cloud Posture Watchlist**.
2. Click Filters to expand the Filters pane.
3. Filter the available framework recommendations based on **Description Keyword, Provider and Framework Version, Recommendation ID, Level, or Severity**.
4. Select a field to **Order By**, and select whether to display the results in **Ascending or Descending** order.
5. Click **Apply** to apply the filter.

Entity Group Settings

You can configure entity groups for your Secure Cloud Analytics deployment, which group user-defined subnets and CIDR blocks. You can then use these groups for Internal Connection Watchlist entries, to monitor multiple entities, or possible entities from a given block of IP addresses, rather than create individual entries for each entity.

To add subnets, first configure them in the Subnets setting. For more information, see [Subnet Configuration](#).

To add CIDR blocks, you can either define them individually, or upload a comma-separated value (CSV) file with multiple CIDR blocks. Each entry in the file must follow the format `prefix, length`, and only the first entry per line will be uploaded. If the system detects duplicate CIDR blocks, it will not add the duplicate blocks to the Entity Group.

Configuring Entity Groups

Create an Entity Group

1. Select **Settings > Entity Groups**.
2. Click **New Entity Group**.
3. Enter a **Name** and **Description** for your Entity Group.
4. Click **Next**.

The Subnets tab appears.

5. If you want to add subnets, you have the following options:
 - Select one or more subnets from the Add Subnets pane, then click **Add Selected to Group** to add them to the Entity Group.
 - Select one or more subnets from the Currently In Group pane, then click **Delete Selected** to remove them from the Entity Group.

See [Subnet Configuration](#) for more information on creating subnets.

6. Select the CIDRs tab.
7. If you want to add CIDR blocks, you have the following options:
 - Enter a **CIDR Prefix** and **Length**, then click Add to add one CIDR block to the Entity Group. Enter a **Length** of 32 to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.
 - Click **Browse** and select a CSV file that contains CIDR blocks in the format `prefix, length` with one entry per line, then click **Upload** to add the first CIDR block in each line to the Entity Group.
8. Click **Create**.

Modify an Entity Group

1. Select **Settings > Entity Groups**.
2. Click edit for an existing Entity Group.
3. Enter a different **Name** and **Description** for your Entity Group.
4. Select the Subnets tab.
5. You have the following options:
 - Enter a **CIDR Prefix** and **Length**, then click Add to add one CIDR block to the Entity Group. Enter a **Length** of 32 to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.

- Click **Browse** and select a CSV file that contains CIDR blocks in the format `prefix, length` with one entry per line, then click **Upload** to add the first CIDR block in each line to the Entity Group.
6. Select the CIDRs tab.
 7. You have the following options:
 - Select one or more subnets from the Add Subnets pane, then click **Add Selected to Group** to add them to the Entity Group.
 - Select one or more subnets from the Currently In Group pane, then click **Delete Selected** to remove them from the Entity Group.
- See [Subnet Configuration](#) for more information on creating subnets.
8. Click **Done** to save your changes.

Delete an Entity Group

1. Select **Settings > Entity Groups**.
2. Click the delete icon for an existing Entity Group and confirm your selection.

Subnet Configuration

You can configure how the system generates alerts for entities within local, virtual cloud, and trusted external networks subnet settings. You can also add a configured subnet to an entity group to facilitate adding a range of entities to that entity group at once.

Based on the settings and subnet type, you can configure the subnet sensitivity, which tunes the alerts that the system generates based on the subnet settings. You can also configure whether the system generates an alert if it detects a new entity within the subnet range.

The following table provides more information:

Subnet Type	Configuration Options	Recommended Subnet Ranges
Local	<ul style="list-style-type: none"> • subnet range • relative threshold for alert generation • whether IP addresses are statically or dynamically assigned within the subnet • whether to alert on new entities detected within the subnet range 	<ul style="list-style-type: none"> • local entities in your on-premises network deployment • entities external to

		your on-premises network deployment that you control
Virtual Cloud (AWS and GCP)	<ul style="list-style-type: none">• subnet range• relative threshold for alert generation• whether to alert on new entities detected within the subnet range	<ul style="list-style-type: none">• cloud entities in your cloud-based network deployment
Trusted External Networks	<ul style="list-style-type: none">• subnet range	<ul style="list-style-type: none">• entities within your trusted external networks that may require network translation due to overlap that you do not want to track• entities external to your network deployment that are controlled by third parties

Configuring Local Subnet Alert Settings

You configure local subnets primarily for on-premises deployments. Specifically, you can configure local subnets for entities that are local to your on-premises network, or entities that are external to your on-premises network that you control. You can add one entry at a time, or upload multiple entries in a comma-separated value (CSV) file.

You can configure the following local subnet alert settings when you add a local subnet:

Parameter	Description
Prefix	The subnet prefix, in IPv4 format.
Length	The subnet length, in CIDR notation, from 1-32. See https://tools.ietf.org/html/rfc4632 for more information.
Default Endpoint Sensitivity	The default subnet sensitivity, which influences the alerts that can be generated: <ul style="list-style-type: none"> • <code>high</code> - The system can generate <code>low</code>, <code>normal</code>, and <code>high</code> priority alerts. • <code>medium</code> - The system can generate <code>normal</code> and <code>high</code> priority alerts. • <code>low</code> - The system can generate <code>high</code> priority alerts.
Description	The local subnet description, displayed in the interface.

When adding a local subnet, you can configure the following alert generation settings:

Parameter	Description
Sensitivity	A subnet's sensitivity influences the alerts that can be generated: <ul style="list-style-type: none"> • <code>high</code> - The system can generate <code>low</code>, <code>normal</code>, and <code>high</code> priority alerts. • <code>medium</code> - The system can generate <code>normal</code> and <code>high</code> priority alerts. • <code>low</code> - The system can generate <code>high</code> priority alerts.
Static	Whether entities are statically assigned IP addresses in this subnet, or dynamically assigned IP addresses, such as through DHCP. If entities in

	this subnet receive statically assigned IP addresses, the system assumes that an IP address always correlates with the same entity.
New Device Alerts	<p>Whether the system generates an alert for this subnet if a new device appears on this subnet.</p> <p>We recommend that you enable this parameter only if you also enable Static IP assignment for this subnet. Dynamically assigned IP addresses may cause the system to generate an excessive amount of new device alerts each time an existing device is dynamically assigned a different IP address.</p>

Add an Entry to the Local Subnet Alert Settings

1. Select **Settings > Subnets > On-Premises**.
2. Click **Create On-Premises Subnet**.
3. Enter a CIDR block **Prefix** as an IPv4 address.
4. Enter a CIDR block **Length** from 1 to 32.
5. Enter an entry **Description**.
6. You have the following options:
 - Check **Static** to identify a subnet that statically assigns IP addresses.
 - Uncheck **Static** to identify a subnet that dynamically assigns IP addresses.
7. You have the following options:
 - Select **New Device Alerts** to receive a new device alert if the system detects a new device on this subnet.
 - Uncheck **New Device Alerts** to suppress new device alerts if the system detects a new device on this subnet.
8. Click **Create**.
9. Select a **Sensitivity** from the drop-down list:
 - `low` - The system requires a high relative threshold to generate alerts.
 - `normal` - The system requires a moderate threshold to generate alerts.
 - `high` - The system requires a low threshold to generate alerts.

Search for a Local Subnet Alert Settings Entry

1. Select **Settings > Subnets > On-Premises**.
2. Enter a **Subnet Prefix** and click **Apply** to locate a local subnet alert settings entry.

Modify a Local Subnet Alert Settings Entry

1. Select **Settings > Subnets > On-Premises**.
2. For an existing entry, select a **Sensitivity** from the drop-down list.
3. You have the following options:
 - Select **Static** to identify a subnet that statically assigns IP addresses.
 - Uncheck **Static** to identify a subnet that dynamically assigns IP addresses.
4. You have the following options:
 - Select **New Device Alerts** to receive a new device alert if the system detects a new device on this subnet.
 - Uncheck **New Device Alerts** to suppress new device alerts if the system detects a new device on this subnet.

Uploading a Local Subnet Settings File

You can upload a comma-separated value file with multiple local subnet entries, one entry per line. Each line should be in the following format:

```
<cidr-prefix>,<cidr-length>,<description>,[sensitivity],[static-ip-assign],[new-device-alerts]
```

See the following for more information:

Parameter	Required	Allowed Values
<cidr-prefix>	yes	An IPv4 address.
<cidr-length>	yes	An integer from 1 to 32.
<description>	yes	Any alphanumeric characters.
[sensitivity]	no	<p>One of the following:</p> <ul style="list-style-type: none"> low - The system requires a high relative threshold to generate alerts. normal - The system requires a moderate threshold to generate alerts. high - The system requires a low threshold to generate alerts.
[static-ip-assign]	no	<p>One of the following:</p> <ul style="list-style-type: none"> true - entities in the subnet receive statically assigned IP addresses false - entities in the subnet receive dynamically assigned IP addresses
[new-device-alerts]	no	<p>One of the following:</p> <ul style="list-style-type: none"> true - the system generates alerts for new devices detected in the subnet false - the system suppresses alerts for new devices detected in the subnet <p>We recommend that you set this parameter to <code>true</code> only if you also set <code>[static-ip-assign]</code> to <code>true</code>.</p>

		Dynamically assigned IP addresses may cause the system to generate an excessive amount of new device alerts each time an existing device is dynamically assigned a different IP address.
--	--	--

Upload a Subnet Alert Settings File

1. Select **Settings > Subnets > On-Premises**.
2. Click **Upload CSV**.
3. Click **Upload File** to select your file for upload.

Modifying Virtual Cloud Subnet Settings

If you configure Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring) for a cloud-based environment using the default policy configuration provided, Secure Cloud Analytics retrieves cloud subnet information via the configured permissions.

You can configure the following alert generation settings for a virtual cloud subnet after the system detects an entry:

Parameter	Description
Sensitivity	<p>A subnet's sensitivity influences the alerts that can be generated:</p> <ul style="list-style-type: none"> • <code>high</code> - The system can generate <code>low</code>, <code>normal</code>, and <code>high</code> priority alerts. • <code>medium</code> - The system can generate <code>normal</code> and <code>high</code> priority alerts. • <code>low</code> - The system can generate <code>high</code> priority alerts.
Static	<p>Whether entities are statically assigned IP addresses in this subnet, or dynamically assigned IP addresses, such as through DHCP. If entities in this subnet receive statically assigned IP addresses, the system assumes that an IP address always correlates with the same entity.</p>
New Device Alerts	<p>Whether the system generates an alert for this subnet if a new device appears on this subnet.</p> <p>Cisco recommends that you enable this parameter only if you also enable Static IP assignment for this subnet. Dynamically assigned IP</p>

addresses may cause the system to generate an excessive amount of new device alerts each time an existing device is dynamically assigned a different IP address.

After the system adds a virtual cloud subnet, you can search for the entry.

Search for a Virtual Cloud Subnet Alert Settings Entry

1. Select **Settings > Subnets**.
2. Select **Amazon Web Services, Google Cloud Platform, or Microsoft Azure**.
3. Enter a **Subnet Prefix**, then click **Apply** to locate a virtual cloud subnet alert settings entry.

Modify a Virtual Cloud Subnet Alert Settings Entry

1. Select **Settings > Subnets**.
2. Select **Amazon Web Services, Google Cloud Platform, or Microsoft Azure**.
3. For an existing entry, select a **Sensitivity** from the drop-down list.
4. You have the following options:
 - **New Device Alerts** to receive a new device alert if the system detects a new device on this subnet.
 - **New Device Alerts** to suppress new device alerts if the system detects a new device on this subnet.

Configuring Trusted External Networks Subnet Alert Settings

Trusted external networks subnets identify external IP address spaces that are considered an extension of the managed network, such as trusted third party affiliates. You can configure these subnets for external entities controlled by third parties that you do not want to track.

You can configure the following trusted external networks subnet alert settings:

Parameter	Description
Prefix	The subnet prefix, in IPv4 format.
Length	The subnet length, in CIDR notation, from 1-32. See https://tools.ietf.org/html/rfc4632 for more information.
Description	The local subnet description, displayed in the interface.

After you add a trusted external networks subnet, you can search for the entry.

In contrast with local subnet alert settings, you cannot modify the sensitivity, IP address assignment, or if an alert is generated when a new entity is detected for the trusted external networks subnet. You can only modify the description displayed in the interface.

Add an Entry to the Trusted External Networks Subnet Alert Settings

1. Select **Settings > Subnets > Trusted External Networks**.
2. Click **Create Subnet**.
3. Enter a CIDR block **Prefix** as an IPv4 address.
4. Enter a CIDR block **Length** from 1 to 32.
5. Enter an entry **Description**.
6. Click **Create**.

Search for a Trusted External Networks Subnet Alert Settings Entry

1. Select **Settings > Subnets > Trusted External Networks**.
2. Enter a **Subnet Prefix** and click **Search** to locate a trusted external networks subnet alert settings entry.

Modify a Trusted External Networks Subnet Alert Settings Entry

1. Select **Settings > Subnets > Trusted External Networks**.
2. Click the **Edit icon**.
3. Update the **Description**.
4. Click **Update**.

User and Site Management

The Site Management settings allow Site Managers to:

- send users an invitation email
- update user account permissions
- configure session timeout

For information on converting to Secure Sign-On, see [the Migration to Cisco Secure Sign-On guide](#) for more information.

Managing Users

Users create accounts in the Secure Cloud Analytics web UI after being invited from the Site Management page.

After a user creates their account, users with the Site Manager role permission can update the following aspects of a user account:

- whether it is active or disabled
- the email address
- the role membership

User accounts can have one of the following three roles:

- **Read-only User** - The user has read permissions to everything except the Site Management page.
- **Normal User** - The user has read/write permissions to everything except the Site Management page. User accounts have this role membership by default.
- **Site Manager** - The user has read/write permissions to all functionality.

For integration with Cisco Secure Sign-On, see the [Secure Sign-On Guide](#)

Send an Invite Email

1. Log in as a user with Site Manager permissions.
2. Select **Settings > Account Management > User Management**.
3. Click **Manage Users**.
4. Click **Invite**.
5. Enter an **Email** address.
6. Click **Invite**.

Modify a User Account

1. Log in as a user with Site Manager permissions.
2. Select **Settings > Account Management > User Management**.
3. Click **User Management**.
4. Toggle between **Cisco Secure Sign-On Users** and **Invited and [portal] Users** to view that type of user account.
5. You have the following options:

- Select **Site Manager** to add the user to the Site Manager role.
 - Select **Read-only User** to add the user to the Read-only User role.
 - Uncheck **Site Manager** and **Read-only User** to add the user to the Normal User role.
6. Click **Save**.

Configuring Session Timeout

The session timeout controls how long user sessions can remain logged in while being inactive before being logged out. You can set a minimum session of 5 minutes, or maximum session timeout of 20160 minutes (the equivalent of 14 days).

Configure the Session Timeout

1. Log in as a user with Site Manager permissions.
2. Select **Settings > Account Management > Session Timeout**.
3. Enter a **Session Timeout** in minutes.
4. Click **Save**.

Web Portal Use

The following describes how to use the Secure Cloud Analytics web portal to:

- view the overall health of your network from the dashboards
- view the open alerts and supporting observations and other context to determine whether network behavior is malicious
- view the models to detect historical patterns in entity, network, and other related behavior over time
- view reports in the Help menu to understand the breadth and depth of traffic monitored by the system

Dashboard Overview

The Dashboard menu option presents several different ways to view your network at a high level.

- The Dashboard provides a summary of alerts, entities on your network, and traffic statistics.
- The AWS Visualizations present AWS-related spider graphs, with your AWS resources, security groups, and IAM permissions as nodes.

Alerts Overview

The Alerts menu option presents the open, closed, and snoozed alerts generated by the system. It generates these alerts, representing potential malicious activity, based on an analysis of various information about your network, including:

- the different types of cloud deployments configured for Cisco Secure Cloud Analytics public cloud monitoring
- if you configured Cisco Secure Cloud Analytics private network monitoring for your on-premises network
- monitored entities roles, and the observations logged for those entities
- monitored subnet sensitivity
- alert type priority
- IP scanner rules
- the configured watchlists, geolocation information, and other threat intelligence

You can view a summary of all alerts generated. From the summary, you can view an alert's detail to gather further context about that alert, and use a workflow to track its progress.

Based on the alert's current status, you can change its status to move it through the workflow:

When an alert's status is:	You can change it to:
Open	Closed Snoozed
Snoozed	(Re-)Open
Closed	(Re-)Open

Alerts Workflow

An alert's workflow is based around its status. When the system generates an alert, the default status is **Open**, and no user is assigned. When you view the Alerts Summary, all open alerts are displayed by default, as these are of immediate concern.

As you review the Alerts Summary, you can assign, tag, and update status on alerts as an initial triage. You can use the filters and search functionality to locate specific alerts, or display alerts of different statuses, or associated with different tags or assignees.



When you close an alert, you can set the alert's status to **Snoozed**, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove **Snoozed** status from an alert, to display it as an open alert again.

As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

From the Alerts Summary, you can view an alert detail page. This page allows you to review additional context about the supporting observations that resulted in this alert, and additional context about the entities involved in this alert.

This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior. As you research within the Secure Cloud Analytics web portal UI and on your network, you can leave comments that describe your findings on the alert. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to **Closed** and have it no longer appear by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

Alert Next Steps

The following presents general guidelines and suggestions for how to investigate a given alert. Because Secure Cloud Analytics provides additional context when it logs an alert, you can use this context to help guide your investigation.



These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

In general, you can take the following steps when you review an alert:

Triage Open Alerts

Triage the open alerts, especially if more than one have yet to be investigated.

- Click **Alerts** to view the open alerts.

What to Do Next

- Ask the following questions:
 - Have you configured this alert type as high priority?
 - Did you set a high sensitivity for the affected subnet?
 - Is this unusual behavior from a new entity on your network?
 - What is the entity's normal role, and how does the behavior in this alert fit that role?
 - Is this an exceptional deviation from normal behavior for this entity?
 - If a user is involved, is this expected behavior from the user, or exceptional?
 - Is protected or sensitive data at risk of being compromised?
 - How severe is the impact to your network if this behavior is allowed to continue?
 - If there is communication with external entities, have these entities established connections with other entities on your network in the past?
- If this is a high priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

Snooze Alerts for Later Analysis

Snooze alerts when they are of lesser priority, as compared to other alerts. For example, if your organization is repurposing an email server as an FTP server, and the system generates an Emergent Profile alert, you can snooze this alert as it is intended behavior, and revisit it at a later date. A snoozed alert does not show up with the open alerts; you must specifically filter to review these snoozed alerts.

1. Click **Close Alert**.
2. In the Snooze this alert pane, select a snooze period from the drop-down.
3. Click **Save**.

Update the Alert for Further Investigation

1. Open the alert detail.
2. Select **Alerts**.
3. Click an alert type name.

What to Do Next

- Based on your initial triage:
 - Assign the alert, so a user can start investigating.
 - Add tags to the alert, to better categorize your alert's for future identification, as well as to try and establish long-term patterns in your alerts.
 - From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Review the Alert and Start your Investigation

If you are reviewing an assigned alert, review the alert detail to understand why Secure Cloud Analytics generated an alert.

Review the supporting observations to understand what these observations mean for the source entity. View all observations for the source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend.

- You have the following options:
 - Click the arrow icon next to an observation type to view all logged observations of that type.
 - Click the arrow icon next to All Observations to view all logged observations for this alert's source entity.

What to Do Next

- Review the Alert Summary, especially the description, to understand the basic situation.
- Review the supporting observations. Understand what these observations mean for the source entity.
- View all of the observations for this source entity to understand its general behavior and patterns, and see if this activity may be part of a longer trend.

- From the observations, view additional context surrounding the source entity, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting. Determine if this behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.
- From the observations, review the context for the entities with which the source entity established a connection. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.
- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Review the Supporting Observations and Contextual Detail

Review the supporting observations to understand what these observations mean for the source entity. Determine if the source entity behavior indicates malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet. View additional context surrounding the source entity, including other alerts and observations it may be involved in, information about the device itself, and what type of session traffic it is transmitting.

- From an observation, you have the following options:
 - Select Alerts from the IP address or hostname drop-down to view all alerts related to the entity.
 - Select Observations from the IP address or hostname drop-down to view all observations related to the entity.
 - Select Device from the IP address or hostname drop-down to view information about the device.
 - Select Session Traffic from the IP address or hostname drop-down to view session traffic related to this entity.
 - Select Copy from the IP address or hostname drop-down to copy the IP address or hostname.

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data or Umbrella data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior. Review the context for the entities with which the source entity established a connection:

- From an observation, you have the following options:
 - Select IP Traffic from the IP address or hostname drop-down to view recent traffic information for this entity.
 - Select Session Traffic from the IP address or hostname drop-down to view recent session traffic information for this entity.
 - Select AbuseIPDB from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
 - Select Cisco Umbrella from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
 - Select Google Search from the IP address or hostname drop-down to search for this IP address on Google.
 - Select Talos Intelligence from the IP address or hostname drop-down to view information on Talos's website.
 - Select Add IP to watchlist from the IP address or hostname drop-down to add this entity to the watchlist.
 - Select Find IP on multiple days from the IP address or hostname drop-down to search for this entity's traffic from the past month.
 - Select Copy from the IP address or hostname drop-down to copy the IP address or hostname.

Examine the Entity and Users

Gather additional context on the source entity, and any users that may have been involved with this alert.

- Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.

- Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.
- Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.
- Leave comments as to your findings. From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Remediate the Issue

If malicious behavior caused the alert, remediate the malicious behavior.

- If a malicious entity or user attempted to log in from outside your network, update your firewall rules to prevent the entity or user from accessing your network.
- If you identify a vulnerability or exploit, update or patch the affected entity to remove the vulnerability, or update your firewall settings to prevent unauthorized access. Determine if other entities on your network may similarly be affected, and apply the same update or patch to those entities. If the vulnerability or exploit currently does not have a fix, contact the appropriate vendor to let them know.
- If you identify malware, quarantine the entity and remove the malware. Determine if other entities on your network are at risk, and update the entities or your security solution to prevent this malware from spreading. Update your security intelligence with information about this malware, or the entities that caused this malware. Alert vendors as necessary.
- If malicious behavior resulted in data exfiltration, determine the nature of the data sent to an unauthorized source. Follow your organization's protocols for unauthorized data exfiltration.

Leave comments as to your remediation.

- From the alert detail, enter a **Comment on this alert**, then click **Comment**.

Fine-tune your Secure Cloud Analytics Settings

Based on the alert and remediation, update your Secure Cloud Analytics settings to help identify this behavior in the future.

- Add external entities to a watchlist if they caused malicious behavior. See [Watchlist Configuration](#) for more information.
- Add countries to the country watchlist if multiple entities from a country caused malicious behavior. See [Configuring the Country Watchlist](#) for more information.
- Update your sensor settings as necessary, to monitor additional subnets. See [Configuring a Sensor's Monitoring Settings](#) for more information.
- Update your subnet sensitivity if a particular subnet is targeted. See [Subnet Configuration](#) for more information.
- Update your alert type priority settings if a specific alert becomes a concern. See [Update Alert Priority](#) for more information.

Update and Close the Alert

Update the alert with additional tags and final comments, then close or snooze it.

1. From an alert's detail, select one or more **Tags** from the drop-down.
2. Enter a **Comment on this alert**, then click **Comment**.
3. Click **Close Alert**.
4. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. This does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
5. If you want to tune the alert priority, you have the following options:
 - Select `Do NOT adjust alert behavior to keep the priority at its current level`.
 - Select `Set this alert type's priority to low to change the alert priority to Low`. If the alert's priority is already Low, this has no effect.
 - Select `Disable this alert type to change this alert type from Enabled to Disabled`.
6. Select a value from the **Don't show the alert matching the above criteria for a period of to snooze this alert for the selected timeframe**, if you want to snooze the alert.

If you want to close the alert, select `Don't snooze` from this drop-down.
7. Click **Create**.

Reopen a Closed Alert

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can

then make changes as necessary to the alert, then close it again when your additional investigation is complete.

- From a closed alert, click **Reopen Alert**.

Unsnnooze a Snoozed Alert

When you are ready to review a snoozed alert, you can unsnnooze it. This sets the status to Open, and displays the alert alongside other Open alerts.

- From a snoozed alert, click **Unsnnooze Alert**.

Alerts Summary

The Alerts Summary presents an overview of the alerts reported by the system. You can search for specific text, or filter by status, tags, or assignee. You can also configure settings related to alert generation.

From the Alerts Summary, you can update the status, tags, and assignee for one or more alerts.

You can download a comma-separated value file that contains the Alerts Summary.

Alert Summary Fields

Field	Description
Alert type	The type of generated alert.
Source entity	The source entity that caused this alert to be generated.
Alert ID	The alert ID number.
Last update time	The time that this alert was last updated.
Number of comments	The number of comments associated with this alert.
Assignee	The user assigned to this alert.

Configuring Alert-related Settings

1. Select **Monitor > Alerts**.
2. Click **Related Config Links**. You have the following options:
 - Select **Alert Priorities** to configure alert priority levels. See [Alert Priority Configuration](#) for more information.

- Select **Country Watchlist** to configure the countries whose traffic should generate alerts, based on geolocation information. See [Configuring the Country Watchlist](#) for more information.
- Select Internal C
- Select **IP Scanner Rules** to configure allowed IP scanners on your network. See [Configuring IP Scanner Rules](#) for more information.
- Select **IPs and Domains Watchlists** to configure your watchlists. See [Watchlist Configuration](#) for more information.
- Select **Subnet Sensitivity** to configure the sensitivity of subnets for alert generation. See [Subnet Configuration](#) for more information.

Using the Alerts Summary

View Alerts Based on Status

1. Select **Monitor > Alerts**.
2. From the available tabs, select **Open** to view all open alerts, **Closed** to view all closed alerts, **Unpublished** to view all unpublished alerts, or **Snoozed** to view all snoozed alerts.


View an Alert's Detail

- From the Alerts Summary, click an alert type name.



Sort the Displayed Alerts

- From the Alerts Summary, click a column header to sort the values by ascending or descending.

Filter the Displayed Alerts

1. From the Alerts Summary, click  **Filters** to expand the pane.
2. Enter a **Search** term.
3. Select an **Alert Type** from the drop-down to search for an alert type.
4. Select an **Assignee** to search for alerts based on Assignee.
5. Select a **Tag** to search for alerts based on the assigned tag.
6. Select a **Start Date** and **Start Time** and **End Date** and **End Time** to find alerts generated within the defined timeframe.
7. Click **Apply** to filter the alerts.

Manage the Alert Tags

1. From the Alerts Summary, click the  (**Settings**) icon next to the **Assign Tag(s)** drop-down.
2. Enter a tag in the **Add new Tag** field, then click the **+** to add the tag.
3. Click the  (**Remove**) icon next to an existing tag to remove it.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Taking Actions in the Alert Summary

From the Alerts Summary, you can update an alert's status, tags, or assignee. You can also bulk update multiple alerts at the same time from the Alert Summary.

View Alerts Based on Status

1. Select **Monitor > Alerts**.
2. Select **Open** to view all open alerts, **Closed** to view all closed alerts, **Snoozed** to view all snoozed alerts, or **All** to view all alerts.

Update Alerts from the Alerts Summary

1. Select **Monitor > Alerts**.
2. Select the check box for one or more alerts, or select the check box in the header to select all alerts displayed on the page.
3. You have the following options:
 - Select a status from the **Change Status** drop-down to assign to the selected alerts.
 - Select a tag from the **Assign Tags** drop-down to assign the tag to the selected alerts.
 - Select a user from the **Assign User** drop-down to assign the user to the selected alerts.

Alert Detail

An alert's detail page provides in-depth information about the alert, including summary information and related observations.

The alert detail page also allows you to use a workflow to update status as you research the alert. You can also leave comments as a record for the alert.

Related Alert Observations

An alert's detail page displays a list of observations that led to this alert being generated. You can review these for more information about the network behavior that led to this alert.

From the alert's detail page, you can also see all observations generated for the affected entity.

Working with an Alert's Detail Page

View an Alert's Detail

1. Select **Monitor > Alerts**.
2. Click an alert type name.

Note that the **Status, ID, Updated, Created, Assignee, Tags, Post an Incident,** and **Close Alert** fields apply to this specific alert. **Description, Next Steps, MITRE Tactics, MITRE Techniques,** and **Alert Type Priority** apply to the alert type, in addition to this specific alert.

Assign a user from an alert's detail page:

- Select a user from the **Assignee** drop-down.

Set this Alert Type's Priority

- From the **Alert Type Priority** drop-down, select a priority level. Note that this selection applies to the alert type, not just this specific alert.

Add Tags from an Alert's Detail Page

- Select one or more **Tags** from the drop-down.

Create a New Cisco SecureX Incident

From an alert's detail, you can create a SecureX incident, and view it in SecureX.

 You must be logged into the SecureX ribbon to enable this.

- Click **Post to Threat Response**.

View context on MITRE ATT&CK Tactics and Techniques

- Hover your cursor over a **MITRE Tactic** or **MITRE Technique** for more information. Note that these apply to the alert type, not just this specific alert.

1. Click **All Observations for (entity)** to view all logged observations for this alert's source entity.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

View Additional Information for a Source Entity

View Additional Observations from an Alert's Detail Page

1. Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
2. Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
3. Select **Device** from the IP address or hostname drop-down to view information about the device.
4. Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
5. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
6. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

View Additional Information for an External Entity

1. Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
2. Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
3. Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
4. Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
5. Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
6. Select **Talos Intelligence** from the IP address or hostname drop-down to view information on Talos's website.

7. Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
8. Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
9. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
10. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

Snooze an Alert:

1. Click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. This does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. If you want to tune the alert priority, you have the following options:
 - Select `Do NOT adjust alert behavior to keep the priority at its current level`.
 - Select `Set this alert type's priority to low to change the alert priority to Low`. If the alert's priority is already Low, this has no effect.
 - Select `Disable this alert type to change this alert type from Enabled to Disabled`.
4. Select a time value from the **Don't show the alert matching the above criteria for a period of to snooze this alert for the selected timeframe**.
5. Click **Create**.

Unsnuzzle a Snoozed Alert

- From a snoozed alert, click **Unsnuzzle Alert**.

Close an Alert

1. Click **Close Alert**.
2. Select **Yes** if the alert was helpful, or **No** if the alert was unhelpful. This does not necessarily mean that the alert resulted from malicious behavior, just that the alert was helpful to your organization.
3. If you want to tune the alert priority, you have the following options:

- Select `Do NOT adjust alert behavior to keep the priority at its current level.`
 - Select `Set this alert type's priority to low to change the alert priority to Low.` If the alert's priority is already Low, this has no effect.
 - Select `Disable this alert type to change this alert type from Enabled to Disabled.`
4. Select `Don't snooze` from the **Don't show the alert matching the above criteria for a period of to snooze this alert for the selected timeframe.**
 5. Click **Create.**

Reopen a Closed alert

- From a closed alert, click **Reopen Alert.**

Enter a Comment on this alert

- Enter a **Comment on this alert**, then click **Comment.**

Entity Detail

An entity's detail page shows information about the entity, including the following:

- **History** - The History line graph displays the amount of traffic sent to and from an entity, and the number of connections it was involved in, per 1 day interval.
- **Summary** - The Summary tab displays an overview of the entity's model, stored by the system.
- **Traffic** - The Traffic line graph displays the amount of traffic sent to and from an entity, and the number of connections it was involved in, per 10 minute interval. The Traffic tab also contains information about the connections that the entity was involved with.
- **Profiling** - The Profiling tab displays information about the roles associated with this entity, and the traffic associated with each role.
- **DNS** - The DNS tab displays information about the DNS requests that the entity submitted, and IP resolution based on the DNS request.

The Summary, Traffic, Profiling, and DNS tabs display information for the current day. You can change to different days and view information collected by the system on that day.

Entity Detail Fields

Entity Summary Fields

Field	Description
Normally Active	The time period during which this entity is normally active.
IP Addresses	The IP addresses associated with the entity.
Connections	The number of connections this entity was involved in.
Internal Connections	The number of connections with internal entities this entity was involved in.
External Connections	The number of connections with external entities this entity was involved in.
Top Internal Connections	Up to the top 5 internal entities with which the entity established connections, based on total traffic transmitted.
Top External Connections	Up to the top 5 external entities with which the entity established connections, based on total traffic transmitted.
Traffic: Bytes In	The amount of traffic that the entity received.
Traffic: Bytes Out	The amount of traffic that the entity sent.
Traffic: Bytes Total	The amount of traffic that the entity transmitted in total.
Traffic Internal: Bytes In	The amount of traffic that the entity received from internal entities.
Traffic Internal: Bytes Out	The amount of traffic that the entity sent to internal entities.
Traffic External: Bytes In	The amount of traffic that the entity received from external entities.
Traffic	The amount of traffic that the entity sent to external entities .

External: Bytes Out	
DNS Names	DNS domain names associated with the entity.
Open Alerts	The open alerts associated with this entity.
Closed Alerts	The closed alerts associated with this entity.
Observations	The observations associated with this entity.
Roles	The roles associated with this entity.
Profiles	The percentage of time that the entity acted corresponding to the listed profile.

Entity Traffic Fields

Field	Description
Connected IP	The IP address that this entity established a connection with.
Hostname/PDNS Record	The hostname for this IP address, if available.
Bytes In	The bytes received by the entity from the connected entity.
Bytes Out	The bytes sent by the entity to the connected entity.
Bytes Total	The total bytes transmitted by the entity in this connection.
Time of First Connection	The time of the first connection with the connected IP on this day.
Time of Last Connection	The time of the last connection with the connected IP on this day.

Entity Profile Fields

Field	Description
-------	-------------

Name	The name of the profile associated with the entity.
Attendance	The percent of time during the day that this entity was active, consistent with this profile.
Bytes In	The bytes received by the entity, consistent with this profile.
Bytes Out	The bytes sent by the entity, consistent with this profile.
Bytes Total	The total bytes transmitted by the entity, consistent with this profile.
Connections	The number of connections this entity was involved in, consistent with this profile.

Entity DNS Fields

Field	Description
Time	The time of the DNS request.
Requested Domain	The domain in the DNS request.
Resulting IP	The resolved IP address, based on the DNS request.

Viewing Entity Detail

View an Entity's Detail

1. Next to a source or internal entity IP address, click the down arrow icon (▼) and select **Device**.
2. Hover your pointer over the History line graph to view details on the entity's traffic for that day.
3. Click **Previous Day** to view the prior day's statistics, or **Next Day** to view the next day's statistics. Note: The statistics default to the current day. You cannot select **Next Day** if the current day's statistics are displayed.

Use the Summary Tab

1. Click **Summary**.
2. Click the Attendance **IP Address** to view more information about the entity's traffic. See [Entity Traffic Detail](#) for more information.

3. Click the arrow icon (↩) next to Open Alerts to go to the Alerts page, filtered by open alerts involving this entity. See [Alerts Summary](#) for more information.
4. Click the arrow icon (↩) next to Closed Alerts to go to the Alerts page, filtered by closed alerts involving this entity. See [Alerts Summary](#) for more information.
5. Click the arrow icon (↩) next to Observations to go to the Observations page, filtered by observations involving this entity. See [Observations Overview](#) for more information.
6. If you want to suggest a role for this entity, click **Suggest Role for Device**, enter your recommendation in the **Suggest a role and provide optional details** field, and click **Suggest**.

Use the Traffic Tab

1. Click **Traffic**.
2. Hover your pointer over the History line graph to view details on the entity's traffic for that 10 minute interval.
3. To filter the connection details, you have the following options:
 - Click **All** to view information about all entities with which this entity established a connection.
 - Click **Internal** to view information about internal entities with which this entity established a connection.
 - Click **External** to view information about external entities with which this entity established a connection.
 - Click **New** to view information about new entities with which the entity had not previously established a connection.

Use the Profiling Tab

1. Click **Profiling**.
2. Hover your pointer over the pie chart to view the percentage of the entity's total connections established, consistent with that profile.

Use the DNS Tab

- Click DNS.

Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

Observations Overview

As the system inspects your traffic, it logs observations, or facts, about the entities on your network. You can view these observations from the Observations menu option. You can view and filter selected highlight observations, or observations by type or by source.

You can drill down and view all observations of that type. If you drill down, the system opens a new tab on this page that displays those observations. If you select a different observation type to drill down into, the system updates that new tab with these observations.

Recent Highlight Observations

Because observations are logged per entity, your network may generate more observations than can be reasonably reviewed. The system presents a subset of the most notable observations logged for your network. You can review and filter these to gain a better understanding of the types of behavior that may result in alerts being generated.



Alerts are generated from combinations of observations; observations in isolation do not necessarily constitute malicious behavior. The recent highlight observations, by themselves, do not necessarily mean there is malicious behavior on your network. Review your alerts for a better picture of the potential malicious behavior.

Viewing the Recent Highlight Observations

View the Recent Highlights Observations

1. Select **Monitor > Observations > Highlights**.

Filter the Recent Highlights Observations

1. Select **Monitor > Observations > Highlights**.
2. For a given observation type, enter a filter value in the search field, then press Enter.

View more Information About an Observation Type

1. Select **Monitor > Observations > Highlights**.
2. Hover your pointer over the information icon (i).

View all Observations of a Type

1. Select **Monitor > Observations**.
2. Select the Recent Highlights tab.
3. Click the arrow icon (➔) next to the observation type you want to view.

The system opens a new tab with these observations.

View More Information about a Source Entity

1. Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
2. Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
3. Select **Device** from the IP address or hostname drop-down to view information about the device.
4. Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
5. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
6. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

View More Information About an External Entity

1. Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
2. Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
3. Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
4. Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
5. Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
6. Select **Talos Intelligence** from the IP address or hostname drop-down to view information on Talos's website.

7. Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
8. Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
9. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
10. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

Observation Types

The Observation Types lists all of the types of observations that the system can log, along with a description, and a count of how many of that observation it has logged.


You can drill down and view all observations of that type. If you drill down, the system opens a new tab on this page that displays those observations. If you select a different observation type to drill down into, the system updates that new tab with these observations.

Viewing Observations by Type

View Observations by Type

1. Select **Monitor > Observations > Types**.



View All Observations of a Type

1. Select **Monitor > Observations > Types..**
2. Click the arrow icon () next to the observation type you want to view.

The system opens a new tab with these observations.

Observations by Device

The Observations by Device lists entities, the number of observations associated with that entity, and the last time the system logged an observation for that entity. You can use this to see the entities that have the most observations.

The system displays an open alert icon () next to entities associated with open alerts, and an information icon () with entities that are not currently associated with an open alert.



A high number of observations does not necessarily correspond with a high number of alerts, or even any alerts. For example, an entity with many observations may be passing a large amount of varied traffic, but Dynamic Entity Modeling may have identified this behavior as normal and expected for this entity. Similarly, a low number of observations does not necessarily correspond with a lack of alerts. For example, if the only activity detected for an entity is a continual attempt to log into a server with improper credentials, this may generate a relatively small number of observations, and an alert noting the multiple failed login attempts.

Viewing Observations by Source

View Observations by Source

1. Select **Monitor > Observations > By Device**.

View All Observations of a Type

1. Select **Monitor > Observations > By Device**.
2. Click the context menu next to an entity and select Observations to view observations associated with that entity.

The system opens a new tab with these observations.

Selected Observations

You can view all observations of a given type from the Selected Observation window. This allows you to review the observations that Secure Cloud Analytics is logging based on your network traffic.

Viewing Selected Observations

1. Select **Monitor > Observations > Selected Observation**.
2. Click Filters to expand the Filters pane.
3. Enter a filter value in the **Search** field.
4. Select an **Observation Type** from the drop-down.
5. Click Apply to filter the results.

Investigate Overview

The **Investigate** menu option displays various graphs and tables related to monitored entities, traffic, and users.

Session Traffic Model

The Session Traffic Model contains detailed information about specific session traffic that the system monitored. By default, the system displays information from the past 24 hours. You can change the timeframe of displayed information, and the criteria for displayed sessions.

Traffic

The Traffic table displays information about sessions that match the filter criteria.

Aggregate Traffic

The Aggregate Traffic table displays information about sessions that match the filter criteria, aggregating related sessions into a single line item.

Traffic Chart

The Traffic Chart displays a bar chart that represents transmitted data in matching sessions over the past 48 hours.

Rejects

The Rejects table displays information about sessions that matched the criteria, but were rejected for relevance reasons.

Connection Graph

The Connection Graph displays a web graph, showing entities as nodes, and edges as connections established between entities.

External Services Model

The Traffic Model contains session information over selected external services, including file storage applications, remote access applications, and social media sites.

Device Model

The Device model contains historical information about the entities monitored by Secure Cloud Analytics. The Endpoints model displays the following:

Device Graph

The Device Graph displays a count of monitored entities for the past 30 days. You can view more detailed information about a given day.

Device Overview

The Device Overview displays detailed information about each entity monitored by Secure Cloud Analytics on a given day, including possible roles for that entity.

Device Roles

The Device Roles displays a mosaic plot of the number of entities that fit a certain role on that day.

IP or Domain Search

The entity search allows you to view detailed information about the traffic an entity transmits.

Encrypted Traffic Report

The Encrypted Traffic Report uses encrypted traffic analytics to display detailed information about encrypted traffic that the system monitored, including source and destination entities, and encryption method details. By default, the system displays information from the past 24 hours. You can change the timeframe of displayed information, and filter the displayed encrypted connections. You can also download a comma-separated value (CSV) file containing details about the encrypted connections.

You must configure your sensor to pass Enhanced NetFlow data to the cloud in order to populate this model. See [Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#) for more information.

User Activity Model

The User Activity model contains information on users that used the system, including observations associated with that user.

Roles Model

The Roles model contains information about the entities that match roles. The Roles model displays the following:

Active Roles

The Active Roles list displays each role with at least one matching entity for the selected timeframe. The Active Roles list includes information based on telemetry types being ingested, which depends on your environment. The default timeframe is the last 7 days, with a maximum timeframe of the last 90 days.

Selected Roles

The Selected Roles list displays the roles you select for the matching entities.

Matching Sources

The Matching Sources list displays all entities that match the list of selected roles.



When you select Roles, the Matching Sources modal will display the devices associated with the Roles. You can then pivot from the device to investigate further.

Event Viewer

The Event Viewer allows you to view session traffic sent to the Cisco cloud for Secure Cloud Analytics, including both private network monitoring and public cloud monitoring traffic.

If you configure public cloud monitoring for AWS, you can also view your AWS rejected traffic in a separate Event Viewer tab.

If you configure public cloud monitoring for AWS or Azure, you can use the Cloud Posture report in the Event Viewer to evaluate your configuration against security recommendations. Secure Cloud Analytics evaluates your deployment once per day so you can refine your security settings and better secure your environment.



Cloud Posture for AWS requires additional configuration. See [Configuring AWS Cloud Posture Permissions](#) for more information.

Session Traffic and Rejected Traffic Fields

The following fields are available in the Event Viewer when you view Session Traffic or Rejected Traffic.

Field	Description
Time	The timestamp associated with the event.
IP	The IP address associated with this traffic.
Connected_IP	The other IP address associated with this traffic.
Port	The port associated with this traffic.
Connected_port	The other port associated with this traffic.
Protocol	The internet protocol associated with this traffic.
Bytes_to	The number of bytes transmitted from the IP to the Connected IP.
Bytes_from	The number of bytes transmitted from the Connected IP to the IP. Not available in Rejected Traffic.

Field	Description
Packets_to	The number of packets transmitted from the IP to the Connected IP.
Packets_from	The number of packets transmitted from the Connected IP to the IP. Not available in Rejected Traffic.

Cloud Posture

If you configure public cloud monitoring for AWS or Azure, you can use the Cloud Posture report in the Event Viewer to evaluate your configuration against security recommendations and provide recommendation verdicts. If you enabled native compliance checking within AWS or Azure, Cloud Posture may display additional recommendations and recommendation verdicts from the cloud provider. Secure Cloud Analytics evaluates your deployment once per day so you can refine your security settings and better secure your environment.

Evaluating your AWS Cloud Posture requires updating your IAM permissions. See [Configuring AWS Cloud Posture Permissions](#) for more information.

Evaluating your Azure Cloud Posture does not require updating any permissions.

Cloud Posture Fields

The following fields are available in the Cloud Posture report.

Field	Data Type	Description
Account_ID	String	The AWS Account ID or Azure Subscription ID against which this recommendation was checked.
Compliant	String	The recommendation verdict, which signifies whether your resource is compliant with this recommendation (<code>PASS</code>) or failed compliance or Secure Cloud Analytics received an access denied response (<code>FAIL</code>).
Description	String	A high-level description of the recommendation.
Details	Nested fields	A summary of information about the recommendation verdict.

Field	Data Type	Description
Framework	String	The associated compliance framework name.
Last_Scanned	String (date)	<p>One of the following:</p> <ul style="list-style-type: none"> The time at which Secure Cloud Analytics derived the recommendation verdict. If AWS or Azure native compliance, the time at which Secure Cloud Analytics retrieved the recommendation verdict. <p>Timestamps are in the format %Y-%m-%d %H:%M:%S</p>
Level	String	Context provided by The Center for Internet Security for CIS Framework Recommendations. Level 1 is intended to lower the attack surface of your organization while keeping machines usable and not hindering business functionality. Level 2 is considered to be “defense in depth” and is intended for environments where security is paramount.
Priority	String	The priority level assigned to the recommendation. See the security recommendation framework's documentation for more information on priority levels.
Provider	String	The cloud provider name, such as <code>AWS</code> or <code>Azure</code> .
Recommendation_ID	String	The ID of the recommendation. Click the Recommendation ID for more information.
Region	String	The region of the AWS or Azure resource against which this recommendation verdict applies.
Resource	Nested fields	The resource against which this recommendation verdict applies. This always displays name and type , and may also display additional information.
Resource.name	String	The resource name evaluated for the

Field	Data Type	Description
		recommendation verdict.
Resource.type	String	The resource type evaluated for the recommendation verdict.
Severity	String	The recommendation severity defined by the AWS or Azure native compliance checks.

Configuring AWS Cloud Posture Permissions

To evaluate your AWS cloud posture, you must grant additional permissions to the IAM policy in AWS. The AWS About page in Secure Cloud Analytics lists the required permissions in the JSON object that starts with "Sid": "CloudCompliance".

If you are a customer integrating Secure Cloud Analytics with AWS for the first time, and do not want to grant these additional permissions, you can remove this object, but you will not be able to use the Cloud Posture report.

If you already have Secure Cloud Analytics integrated with AWS and do not want to grant these additional permissions, make no changes to the IAM policy in AWS. You will not be able to use the Cloud Posture report. Perform the following procedures to update your existing IAM policy.

Review Cloud Posture Permissions for AWS

1. Log in to your Secure Cloud Analytics portal as an administrator.
2. Select **Settings > Integrations > AWS > About**.
3. In the **Policy Document** pane, review the JSON object that starts with "Sid": "CloudCompliance" for the additional permissions Secure Cloud Analytics requires to evaluate your AWS cloud posture. You have the following options:
 - If you do not want to grant these additional permissions, stop here. You will not be able to evaluate your AWS cloud posture in Secure Cloud Analytics.
 - If you want to grant these additional permissions to evaluate your AWS cloud posture, copy the **Policy Document** JSON configuration and paste it into a plaintext editor. Continue to the next procedure.

Update the Secure Cloud Analytics IAM Policy in AWS

1. Log in to your AWS console as an administrator.
2. From the IAM console, select **Policies**, then select your Secure Cloud Analytics IAM policy.
3. Click **Permissions**, then select **Edit policy**.
4. Select **JSON**, then copy the updated policy from the plaintext editor and paste it, overwriting any existing policy.
5. Click **Review policy**.
6. Click **Save changes**.

Accessing the Event Viewer

Access the Event Viewer

1. Log in to your Secure Cloud Analytics portal.
2. Select **Investigate > Event Viewer**.
3. You have the following options:
 - Select Event Viewer to view session traffic transmitted across your network deployment.
 - If you configured public cloud monitoring with AWS, select **Rejected Traffic** to view your AWS rejected traffic.

Showing and Hiding Columns

You can change the columns displayed in the Event Viewer.

Show and Hide Columns

1. From the Event Viewer, you have the following options:
 - Click the Settings icon in the lower left, then select **Manage Columns**.
 - Click the Settings icon in the upper right.
2. Check the columns you want to display, and uncheck the columns you want to hide.
3. Click the x when you are done to update the Event Viewer.

Viewing Additional Field Information

Certain events may contain additional fields. These fields may also contain multiple sub-fields and associated values. You can view these by expanding the line item.

View Additional Field Information

- For an event that contains additional fields, click the ▼ **(Move Down)** icon to expand the event and view the additional field information.

Event Viewer Filtering

The Event Viewer defaults to displaying all events from the past hour. The Event Viewer loads several results at a time. If more results are available than can be displayed at once, you can scroll down and the Event Viewer loads additional results.

The Event Viewer defaults to the inline filtering method. This allows you to add a value to and select one of several operators from the column filter, such as equals, greater or less than, or between. You can filter on multiple values using inline filtering; any matching events must match all of the evaluations that you add.



You can switch from inline filtering to query filtering, which allows you to create more advanced queries based on the Lucene query syntax. Note that the time selection option is still available with query filtering. Because you can use multiple Boolean operators (AND, OR, NOT), you can create more fine-tuned searches than with inline filtering.



Event Viewer Query Syntax

See the Lucene Query Syntax documentation for more information.

Query Syntax Options

You can use the following query syntax options:

Syntax Option	Syntax	Description
basic field/value evaluation	field1: "value1"	return results where field1 equals value1
single character wildcard	?	any character matches this ? <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Wildcard searches are only supported if the inline filter for a column accepts any alphanumeric string value. </div>
multiple character wildcard	*	any number of any characters match this * <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Wildcard searches are only supported if </div>

Syntax Option	Syntax	Description
		<div style="border: 1px solid #00a0e3; padding: 5px;">  the inline filter for a column accepts any alphanumeric string value. </div>
inclusive range search	<code>["value1" TO "value2"]</code>	return <code>value1</code> , <code>value2</code> , or any values in between
exclusive range search	<code>{"value1" TO "value2"}</code>	return any values between <code>value1</code> and <code>value2</code> , but not <code>value1</code> or <code>value2</code>
Boolean AND operator	AND	return results where both the evaluation before and after AND are true <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;">  If there is no syntax between two search parameters, the query will automatically interpret them as an AND. </div>
Boolean OR operator	OR	return results where either the evaluation before or after OR is true
Boolean NOT operator	NOT	return results where the evaluation before NOT is true, and after NOT is false
grouping	()	evaluate within the parentheses on their own
field grouping	<code>field1: ()</code>	evaluate multiple values and operators within the parentheses for a single field



Order of Evaluation

The system evaluates queries in the following order of precedence:

1. grouping, including () (parentheses), [] (inclusive range searches), and {} (exclusive range searches)
2. : (equals)
3. NOT Boolean operator
4. AND Boolean operator
5. OR Boolean operator

Query Syntax Examples

The following table provides generic query syntax examples.

Description	Example Syntax	Results Returned
one field, one value	<code>field1: "value1"</code>	all events where field1 equals value1
one field, one value, single character wildcard	<code>field1: "value?"</code>	all events where field1 equals "value?", where ? is any character
one field, one value, multiple character wildcard	<code>field1: "value*"</code>	all events where field1 equals "value*", where * is any number of any characters
one field, multiple values (field grouping)	<code>field1: ("value*1" AND "value*2")</code>	all events where field1 contains value*1 and value*2 <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> When searching for multiple values in one field, we recommend that you use wildcards in each value to increase the likelihood of getting a matching result.</p> </div>
one field, either value	<code>field1: ("value1" OR "value2")</code>	all events where field1 equals value1 or value2
two fields, AND operator	<code>field1: "value1" AND field2: "value2"</code>	all events where field1 equals value1 and field2 equals value2 <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> If you do not explicitly define an operator between multiple field value evaluations, the system implicitly interprets the AND operator between the evaluations.</p> </div>

Description	Example Syntax	Results Returned
two fields, OR operator	field1: "value1" OR field2: "value2"	all events where field1 equals value1 or field2 equals value2
two fields, NOT operator	field1: "value1" AND NOT field2: "value2"	all events where field1 equals value1 and field2 does not equal value2
two fields, OR NOT operator	field1: "value1" OR NOT field2: "value2"	all events where field1 equals value1 or field2 does not equal value2
one field, inclusive range search	field1:["value1" TO "value2"]	all events where field1 equals value1, value2, or any value between
one field, exclusive range search	field1:{"value1" TO "value2"}	all events where field1 equals any value between value1 and value2, but not value1 or value2
one field, mixed inclusive and exclusive range search	field1:["value1" TO "value2"]	all events where field1 equals value1, or any value between value1 and value2, but not value2
multiple fields, mixed operators	field1: "value1" OR field2: "value2" AND field3: "value3"	because the AND Boolean operator has greater precedence than the OR Boolean operator, all events where: <ul style="list-style-type: none"> • field2 equals value2 and field 3 equals value 3, or • field1 equals value1
multiple fields, mixed operators and parentheses	(field1: "value1" OR field2: "value2") AND field3: "value3"	because grouping has greater precedence than other operations and is evaluated first, all events where: <ul style="list-style-type: none"> • field1 equals value1 or field 2 equals value2, and

Description	Example Syntax	Results Returned
		<ul style="list-style-type: none"> field3 equals value3

The following table lists query examples that a user may run for their deployment:

Description	Example Syntax	Results Returned
internal devices that established successful non-HTTPS connections with an internal web server	<pre>Connected_ip: "192.168.105.28" AND IP: "192.168.0.0/16" AND NOT Port: "443" AND NOT Connected_ port: "443" AND Packets_from: { "10" TO * } AND Packets_to: { "10" TO * }</pre>	<p>all events with the following:</p> <ul style="list-style-type: none"> IP equal to the internal CIDR range of 192.168.0.0/16 (internal entities), Connected_ip equal to 192.168.105.28 (the internal web server) Port not equal to 443 (non-HTTPS traffic), Connected_port not equal to 443 (non-HTTPS traffic), Packets_from equal to 11 or more (successful connection, traffic passed), and Packets_to equal to 11 or more (successful connection, traffic passed)

Description	Example Syntax	Results Returned
connections related to remote desktop applications	<pre>Port: ("23" OR "3389" OR ["5800" TO "5803"] OR ["5900" TO "5903"] OR ["6000" TO "6063"]) AND NOT Connected_port: ["0" TO "1023"] AND Packets_from: ["10" TO *] AND Packets_to: ["10" TO *]</pre>	<p>all events with the following:</p> <ul style="list-style-type: none"> • Port equal to 23, 3389, 5800-5803, 5900-5903, or 6000-6063 (common remote desktop application ports), • Connected_port not equal to 0-1023 (connections using ephemeral ports), • Packets_from equal to 10 or more (successful connection, traffic passed), and • Packets_to equal to 10 or more (successful connection, traffic passed)

Event Viewer Nested Field Searches

If an event contains fields with sub-fields, you can search for these field values in the query filter by using dot notation to specify a sub-field.

For example a line-item entry may contain a **Details** field with two sub-fields: **credentials** and **issues**. If you want to search for `username1` in the **credentials** field, use the following dot notation syntax:

```
Details.credentials: "username1"
```

Note that certain fields in different recommendations may contain different sub-fields for each recommendation type.

Inline Filtering the Event Viewer

Change the Time Selection

1. From the Event Viewer, in the time field, click the calendar icon.
The timestamps default to your local time zone (displayed), or UTC if your local time zone is UTC.
2. Select one of the preset timeframes to automatically configure that timeframe.
3. Select **Custom** to select a custom timeframe.
4. Select a **From Date/Time** and a **To Date/Time**.
5. When you have selected your time frame, click the time field to update your results.

Filter a Column

1. From the Event Viewer, make sure the inline filtering method is selected.
2. You have the following options:
 - Click a value, click the copy icon, then paste that value in the column filter field.
 - Enter a value in the column filter field.
3. Click the column filter icon, and select an operator.
4. When you have entered a value and selected an operator, click the column filter field to filter your results.
5. Click the x next to a filter to remove it from your results.

Switch to Query Filtering

1. From the Event Viewer, with inline filtering selected, select **query** filtering.
2. If you want to preserve your current applied inline filters, check **Convert all applied filters to query syntax**.
3. Click **Confirm**.

Query Filtering the Event Viewer

Change the Time Selection

1. From the Event Viewer, in the time field, click the calendar icon.
2. Select **Show time** in either `Local` or `UTC`.
3. Select one of the preset timeframes to automatically configure that timeframe.
4. Select **Custom** to select a custom timeframe.

5. Select a **From Date/Time** and a **To Date/Time**.
6. When you have selected your time frame, click the time field to update your results.

Query Your Events

1. From the Event Viewer, make sure you have query filtering selected.
2. Enter your query in the query field. See [Event Viewer Query Syntax](#) and the Lucene syntax documentation for more information.
3. Click **Apply** to filter your results.

Switch to Inline Filtering

1. From the Event Viewer, with inline filtering selected, select **inline** filtering.
2. If you want to copy your current time range, click the **Time Range** copy icon.
3. If you want to copy your current applied query, click the **Query** copy icon.
4. Click **Confirm**.

Viewing an IP Address's Additional Context

You can view additional information about an IP address from the event viewer.

View Additional Information for a Source Entity

1. Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
2. Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
3. Select **Device** from the IP address or hostname drop-down to view information about the device.
4. Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
5. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
6. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

View Additional Information for an External Entity

Procedure

1. Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
2. Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
3. Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
4. Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
5. Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
6. Select **Talos Intelligence** from the IP address or hostname drop-down to view information on Talos's website.
7. Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
8. Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
9. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
10. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

Downloading Event Information

You can download events in a comma-separated value (CSV) file. Note the following:

- Secure Cloud Analytics adds the events to a .csv file and then compresses them in the .gz format.
- A single .csv file can accommodate up to approximately 50 GB of compressed information.
- Generation of downloadable files can be done in parallel.
- Once created, the .csv.gz files are stored in Secure Cloud Analytics and downloaded directly from there. These files do not affect your Secure Cloud Analytics billing subscription.
- Completed downloadable .csv.gz files are stored for 7 days and then deleted.
- A job in-progress can be canceled manually.

Generate and Download a CSV.GZ File

1. From the Event Viewer, click the Download icon, then click **Generate a file for export**.
2. Enter a **File Name**.
3. Click **Submit**. It may take several minutes or more to generate the file.



If you want to cancel the file generation in process, click the Download icon, then click **Cancel file export**.

4. When the file is ready for download, click the Download icon, then click the generated file name.

Report Menu

The Report menu allows you to generate reports that provide at-a-glance information about your network, including reports related to entities and throughput monitored to help you understand how much traffic your deployment monitors.

AWS Visualizations

The AWS Visualizations displays the following information about your AWS deployment:

- **CloudTrail** - The CloudTrail tab displays your AWS CloudTrail logs.
- **Network Graph** - The Network Graph tab displays a spider graph representing your AWS deployment.
- **Security Groups** - The Security Groups tab displays a spider graph representing your AWS deployment's security groups.
- **IAM** - The IAM tab displays a spider graph representing your IAM roles and permissions.
- **Inspector** - The Inspector tab displays the Inspector assessments for your EC2 instances.

Metering Report

The Metering Report page contains the average flows per second monitored by Secure Cloud Analytics if you are monitoring on-premises deployments using private network monitoring. The graph displays the past calendar month of FPS monitoring. This allows you to view your usage, as private network monitoring billing is based on average FPS per month.

Monthly Flows Report

The Monthly Flows Report page contains the number of effective flows monitored per day by Secure Cloud Analytics if you are monitoring cloud-based deployments using public cloud monitoring. By default, the system displays the past 30 days of EF monitoring. You can change the filter to display a different time range. This allows you to view your usage, as public cloud monitoring billing is based on effective mega flows (EMF), or roughly one million effective flows, per month.

Subnet Report

The Subnet Report page contains the subnets that the system detects as having transmitted traffic. The report contains an overview of:

- all of the active subnets
- the traffic these subnets generate
- the number of active IP addresses in the subnet
- a table displaying traffic transmitted between subnets

By default, the report displays the past 24 hours' worth of traffic. You can change the timestamps for which the system displays subnets and information related to those subnets. You can also download a comma-separated file containing the information from the report.

Traffic Model

The Traffic Model contains detailed information about traffic that the system monitored. By default, the system displays information from the past 24 hours. You can change the timeframe of displayed information.

Traffic Overview

The Traffic Overview displays a general overview of transmitted traffic, and information about the sources of that traffic.

Top IPs

The Top IPs table displays information about the internal and external IP addresses the transmitted the most traffic.

Top Ports

The Top Ports table displays information about the internal and external ports over which entities transmitted the most traffic.

Visibility Assessment

The Visibility Assessment page displays a report that provides insight into your network activity over the past 30 days. This report includes the following information:

- a traffic overview of your internal network
- a list of the most recent entities that have established excessive SMB connections with external hosts
- a list of the entities acting as unauthorized DNS servers
- a list of entities with an excessive number of connections with DNS servers
- a list of entities that provide remote network access, such as VNC or RDP
- a list of entities with excessive Telnet connections
- a list of entities with multiple connections to high-risk countries, as defined by Cisco

By default, the report displays information based on the past 30 days of traffic on your network. You can view the report in the web portal UI, or download a PDF with the information.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Document Version	Published Date	Description
1_0	August 7, 2018	Initial version.
1_1	November 26, 2018	Updated sensor flow collection.
1_2	January 22, 2019	Updated sensor flow collection configuration.
1_3	April 18 , 2019	Updated deprecated terms.
1_4	June 6, 2019	Updated PCM for AWS and Azure.
1_5	July 9, 2019	Updated terminology for updated UI.
1_6	October 8, 2019	Updated for Enhanced NetFlow integration.
1_7	October 22, 2019	Updated PCM for AWS configuration instructions.
1_8	January 6, 2020	Updated with additional information about Cisco Defense Orchestrator integration.
1_9	June 23, 2020	Corrected external connection watchlist information.
1_10	October 16, 2020	Updates based on UI updates.
1_11	October 22, 2020	Updates for Meraki configuration.
1_12	December 11 , 2020	Updates for event viewer, alerts, and observations.
1_13	January 26, 2021	Updates for Cloud Posture

		Management.
1_14	February 3, 2021	Updates for how to create Azure storage account for PCM.
1_15	February 18, 2021	Updates for PCM integration for AWS.
2_0	November 3, 2021	Updates for product branding.
2_1	August 1, 2022	Added Contacting Support section. Updated AWS, Azure, and GCP configuration steps. Updated sensor installation information. Updated Web Portal information. Added notes for public IPs.
2_2	January 20, 2023	Added Configuring Proxy section. Added Configure S3 Bucket to Minimize Cost section. Removed the Azure Activity Log Storage section. Updated GitHub repository links.
2_3	February 24, 2023	Updated Meraki sensor settings. Added Event Viewer default query behavior. Updated Alert summary to Alert Summary.
2_4	April 8, 2024	Updated the introduction in the <i>Sensor Media Installation and Configuration</i> section. Minor formatting changes.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

