# Cisco Secure Cloud Analytics

Subnet Configuration Guide

# Table of Contents

# Subnet Monitoring and Alerting Overview

Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) uses dynamic entity modeling to track network entities, create observations on the traffic, and generate alerts based on these observations. The default configuration of Secure Cloud Analytics is to create an entity for any IP address in the RFC 1918 IP space that generates traffic. Secure Cloud Analytics allows for customization of the networks that are monitored and their sensitivity level.

## Dynamic Entity Modeling and Subnet Monitoring Configuration

Entity modeling is the process of learning behavior for entities on the network. Every IP address that transmits traffic is considered a monitored entity. If an IP address only receives traffic and never generates it, which is often the case when network scanners are used for IPs that do not exist, then it will not be considered a monitored entity. The default behavior of the systems is described below.

Predefined Internal Subnets, in the RFC 1918 IP space:

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`

As an example, assume that your Cisco Secure Cloud Analytics sensor (formerly Stealthwatch Cloud Sensor) is configured to monitor the default subnets, but not `198.51.100.0/24`. The following behavior is expected:

- If any entities within a defined subnet (such as `192.168.0.0/16`) establish a connection), the system tracks models the traffic for these entities. The system tracks each entity as a unique entity.
- If an entity within a defined subnet (`192.168.0.0/16`) establishes a connection with an entity in another defined subnet (such as `10.0.0.0/8`), the system tracks and models the traffic for these entities.
- If an entity within a defined subnet (`192.168.0.0/16`) establishes a connection with an external IP address not listed in the defined subnets (`198.51.100.0/24`), the system tracks that traffic, but models only the internal entity.
- If two IP addresses within a non-defined subnet (such as `198.51.100.0/24`) establish a connection, the system does not perform entity modeling on either entity, nor does it track that traffic, as this subnet is not by default a monitored subnet.

### Subnet Exclusion from Dynamic Entity Modeling

We recommend keeping the default RFC 1918 space in a subnet's configuration. The defined subnets can be changed for your network. You can also define additional subnets that are more specific, or add external IP spaces that should be treated as internal.

In addition to defining the subnet in the subnet configuration pages, you must also ensure the sensor has visibility to the traffic.

Some users may want to exclude a local subnet from entity modeling. However, if the system observes that subnet generating traffic, and the subnet is part of the RFC 1918 space, removing it from the defined subnets will not stop Secure Cloud Analytics from tracking an IP address as an entity, as this behavior is hard coded. To remove an RFC 1918 subnet, contact Cisco Support with the subnets you want excluded.

## Subnets and Alert Generation

An alert is the actionable item that represents possible malicious behavior as identified by the system. Subnet sensitivity can be configured as `low`, `normal`, and `high`. By default, all predefined subnets are set to `normal`, meaning any alert type with a priority of `normal` or `high` will be activated for that subnet, while an alert type with a priority of `low` would not be activated for that subnet and would automatically close if generated. If you lower the subnet's sensitivity to `low`, only high priority alerts can be generated. If you raise the subnet's sensitivity to `high`, any alert priority will result in open alerts being generated. See the following table for an example of which combinations of alert type priority and subnet sensitivity generate alerts.

| | **Low Alert Type Priority** | **Medium Alert Type Priority** | **High Alert Type Priority** |
|---|---|---|---|
| **Low Subnet Sensitivity** | No open alert | No open alert | Generates an open alert |
| **Normal Subnet Sensitivity** | No open alert | Generates an open alert | Generates an open alert |
| **High Subnet Sensitivity** | Generates an open alert | Generates an open alert | Generates an open alert |

*No open alert* means while an alert is still generated, it automatically closes showing up in the alert list under a closed status.

> Alerts with a network source are not influenced by the subnet's sensitivity and generate an open alert based on alert type priority only.

## Subnet Configuration Categories

Secure Cloud Analytics has three subnet categories that can be defined:

- local subnets, which contain entities in your on-premises environment
- virtual cloud subnets, which contain entities from your cloud-based deployment
- trusted external networks subnets, which contain third-party entities that you trust, but do not control

Normally, you manually edit local and trusted external networks subnet settings by importing a CSV file. In contrast, Secure Cloud Analytics retrieves virtual cloud subnets directly from your cloud provider (AWS, Azure, and GCP).

> Secure Cloud Analytics does not integrate with third-party IP management tools.

The trusted external networks subnets are used for external trusted entities, such as partners that your endpoints regularly communicate with, and are more trusted than other external IP addresses.

In addition to the sensitivity level, two optional settings can be configured per subnet:

- Static – Enable this when IP addresses on a subnet are mainly static and do not change.
- New Device Alerts – Enable this to generate an alert whenever a new entity is detected in the subnet range. This has the potential to create many alerts, and should only be used for very sensitive subnet ranges.

## Subnet Configuration Steps

Perform the following steps to configure subnet monitoring and alerting settings:

1. See Configuring a Sensor's Monitoring Settings to add subnets to a sensor's configuration.
2. See the following:
    - Subnet Configuration for an overview of subnet configuration.
    - Configuring Local Subnet Alert Settings to add local subnets and adjust subnet sensitivity.

- Modifying Virtual Cloud Subnet Settings to modify virtual cloud subnets and adjust subnet sensitivity.
- Configuring Trusted External Networks Subnet Alert Settings to add trusted external networks subnets.

3. See Updating Alert Priority to modify alert type priority.

# Sensor 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**.
2. Click **Settings > configuring monitoring** for the sensor you want to configure.
3. Add one or more CIDR blocks in the **Networks To Monitor** field, one per line.
4. Select a number of **Packets per second to capture for PDNS**.
5. Click **Save**.

# 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 | • subnet range<br>• relative threshold for alert generation<br>• whether IP addresses are statically or dynamically assigned within the subnet<br>• whether to alert on new entities detected within the subnet range | • local entities in your on-premises network deployment<br>• entities external to your on-premises network deployment that you control |
| Virtual Cloud (AWS and GCP) | • subnet range<br>• relative threshold for alert generation<br>• whether to alert on new entities detected within the subnet range | • cloud entities in your cloud-based network deployment |

| | | |
|---|---|---|
| Trusted External Networks | • subnet range | • entities within your trusted external networks that may require network translation due to overlap that you do not want to track<br>• 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:<br>• `high` - The system can generate `low`, `normal`, and `high` |

| | |
|---|---|
| | priority alerts.<br>• `medium` - The system can generate `normal` and `high` priority alerts.<br>• `low` - The system can generate `high` 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:<br>• `high` - The system can generate `low`, `normal`, and `high` priority alerts.<br>• `medium` - The system can generate `normal` and `high` priority alerts.<br>• `low` - The system can generate `high` 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 | Whether the system generates an alert for this subnet if a new device appears on this subnet.<br>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. |

## 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 | One of the following:<br>• `low` - The system requires a high relative threshold to generate alerts.<br>• `normal` - The system requires a moderate threshold to generate alerts.<br>• `high` - The system requires a low threshold to generate alerts. |
| `[static-ip-assign]` | no | One of the following:<br>• `true` - entities in the subnet receive statically assigned IP addresses<br>• `false` - entities in the subnet receive dynamically assigned IP addresses |
| `[new-device-alerts]` | no | One of the following:<br>• `true` - the system generates alerts for new devices detected in the subnet<br>• `false` - the system suppresses alerts for new devices detected in the subnet<br>We recommend that you set this parameter to `true` only if you also set `[static-ip-assign]` to true. |

| | | |
|---|---|---|
| | | 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 | A subnet's sensitivity influences the alerts that can be generated:<br>• `high` - The system can generate `low`, `normal`, and `high` priority alerts.<br>• `medium` - The system can generate `normal` and `high` priority alerts.<br>• `low` - The system can generate `high` 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 | Whether the system generates an alert for this subnet if a new device appears on this subnet.<br>Cisco recommends 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. |

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**.

# 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.

# 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.

## View the Subnet Report

- Select **Report > Subnet Report**.

### Change the Time Period Displayed in the Subnet Report

1. Expand the filters pane.
2. Enter a new **Start Date** and **Start Time**.
3. Enter a new **End Date** and **End Time**.
4. Click **Update**.

### Download a Comma-Separated File Containing the Report Information

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

# 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

| Revision | Revision Date | Description |
|---|---|---|
| 1.0 | May 19, 2019 | Initial version. |
| 1.1 | October 15, 2020 | Updates based on UI updates. |
| 2.0 | November 3, 2021 | Updated product branding. |
| 2.1 | August 1, 2022 | Updated subnet sensitivity options and added *Contacting Support* section. |
| 2.2 | March 25, 2024 | Changed the *Configuring VPN Subnet Alert Settings* section to the *Configuring Trusted External Networks Subnet Alert Settings* section. |

# Copyright Information