



Cisco Secure Cloud Analytics

Sensor Installation Guide



Table of Contents

| | |
|---|-----------|
| Introduction | 4 |
| Sensor Deployment Considerations | 4 |
| Sensor Prerequisites | 4 |
| Physical Appliance Additional Requirements | 5 |
| Virtual Machine Additional Requirements | 6 |
| VMware hypervisor | 6 |
| VirtualBox | 6 |
| Sensor Deployment Suggestions | 6 |
| Checking Your Sensor Version | 7 |
| Sensor Access Requirements | 7 |
| Network Device Configuration | 8 |
| Flow Configuration | 9 |
| Cisco Defense Orchestrator and Sensor Deployment | 9 |
| Sensor Media Installation and Configuration | 11 |
| Creating Boot Media | 11 |
| Download the sensor ISO file | 11 |
| Create a Bootable Optical Disc | 12 |
| Create a Bootable USB Flash Drive | 12 |
| Installing a Sensor | 12 |
| What to Do Next | 15 |
| Attaching Sensors to the Web Portal | 15 |
| Finding and Adding a Sensor's Public IP Address to a Portal | 16 |
| Manually Add a Portal's Service Key to a Sensor | 17 |
| Configuring Proxy | 18 |
| Confirm a Sensor's Portal Connection | 18 |
| Configuring a Sensor to Collect Flow Data | 19 |
| Configuring Sensors for Flow Collection | 20 |
| What to Do Next | 21 |

| | |
|---|-----------|
| Troubleshooting | 22 |
| Capture Packets from the Sensor | 22 |
| Analyze the Packet Capture in Wireshark | 22 |
| Additional Resources | 23 |
| Contacting Support | 24 |
| Change History | 25 |

Introduction

Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) is a SaaS-based security service that detects and responds to threats in IT environments, both on-premises and in the cloud. This guide explains how to deploy Secure Cloud Analytics sensors as part of your private network monitoring service, for use in enterprise networks, private data centers, branch offices, and other on-premises environments.

i If you plan to use Secure Cloud Analytics only in public cloud environments, such as Amazon Web Services, Microsoft Azure, or Google Cloud Platform, you do not need to install a sensor. Go to the [public cloud monitoring guides](#) for more information.

i This guide provides instructions for installing the sensor on Ubuntu Linux. For installation instructions on other operating systems, refer to the [Secure Cloud Analytics Sensor Advanced Configuration Guide](#).

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.

i 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 | <p>at least one network interface, designated as the Control interface, for passing information to the Secure Cloud Analytics service</p> <p>i 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) |



Virtual machines can boot directly to the .iso file without additional requirements.

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.

i 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">• varies |

| | | |
|--|-----|---|
| 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 sensor's Control interface to a DNS server for hostname resolution | yes | <ul style="list-style-type: none"> [local DNS server]:53/UDP |
| 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, and 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_Reportin/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_Reportin/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

If you install a sensor on a physical appliance, you must create bootable media using the .iso file, then restart the appliance and boot from that media.

If you install a sensor on a virtual machine, you can boot from the .iso file directly.

 The install process wipes the disk on which the sensor will be installed, before installing the sensor. Ensure that the physical appliance or virtual machine on which you will 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 a Sensor

1. If you are installing a physical appliance, insert the bootable media, restart the appliance, and boot from the bootable media.

If you are installing on a virtual machine, boot from the .iso file.

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 install process uses DHCP to configure the primary network interface you selected as the Control interface. If your network does not use DHCP, do the following:

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.

i 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 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.obsrvbl.com> (US)
- <https://sensor.eu-prod.obsrvbl.com> (EU)
- <https://sensor.anz-prod.obsrvbl.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

i 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

i 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.obsrvbl.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/obsrvbl-ona/logs/ipfix$ curl https://sensor.ext.obsrvbl.com
{
 "error": "unknown identity",
 "identity": "72.163.2.237"
}observable@ona-e37255:/opt/obsrvbl-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 (cloud)** icon > **Public IP**.
  7. Enter the `identity` IP address in the Public IP field. See the following image for an example.

Sensors

**Sensor List**   **Public IP**

Enter the public IP address your sensor will use when sending data.

**Public IP:**

+ Add IP

8. 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.

Manually adding a portal's service key to a sensor is intended primarily for older

- i** 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.

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



4. SSH login to the sensor as an administrator.
5. At the command prompt, enter this command:  
`sudo nano opt/obsrvbl-on/a/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=""`

See the following for an example.

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"`

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

4. Press Ctrl + O 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

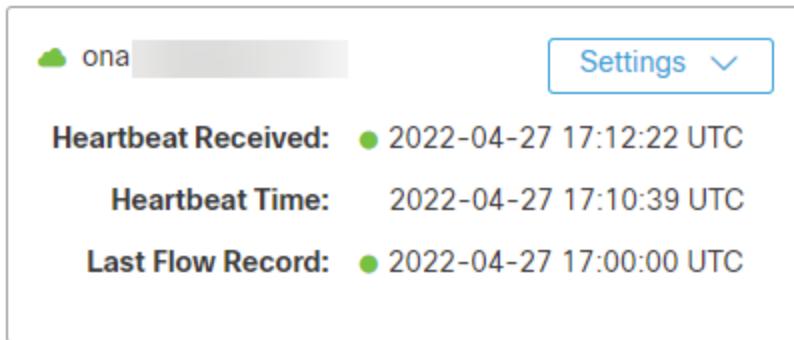
After a sensor is added to the portal, confirm the connection.

**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\\_Reportin/Cisco\\_Security\\_Analytics\\_and\\_Logging](https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reportin/Cisco_Security_Analytics_and_Logging) for more information.

# Troubleshooting

## Capture Packets from the Sensor

Occasionally, Cisco Support may need to verify the flow data being received by the sensor. We recommend that you do this by generating a packet capture of the flows. You can also open the packet capture in Wireshark to review the data.

1. SSH log into the sensor.
2. At the prompt, enter `sudo tcpdump -D` and press Enter to view a list of interfaces. Note the name of your sensor's Control interface.
3. At the prompt, enter `sudo tcpdump -i <control_interface> -n -c 100 "port <port_number>" -w <pcap_name>`, replace **<control\_interface>** with your Control interface name, **<port\_number>** with the port number corresponding to your configured flow data, and **<pcap\_name>** with a name for the generated pcap file, then press Enter. The system generates a pcap file with the specified name for that interface's traffic, over the specified port.
4. Log out of your sensor.
5. Using an SFTP program, such as PuTTY SFTP (PSFTP), or WinSCP, log into the sensor.
6. At the prompt, enter `get <pcap_name>`, replace **<pcap\_name>** with your generated pcap file name, and press Enter to transfer the file to your local workstation.

## Analyze the Packet Capture in Wireshark

1. Download and install Wireshark, then open Wireshark.
2. Select **File > Open**, then select your pcap file.
3. Select **Analyze > Decode As**.
4. Click **+** to add a new rule.
5. Select **CFLOW** from the **Current** drop-down, then click **OK**. The UI updates to display only packets that are related to NetFlow, IPFIX, or sFlow. If no results appear, the pcap does not contain NetFlow-related packets, and flow data collection is incorrectly configured on the sensor.

## 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/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> to sign up for a 60-day Free Trial
- <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](mailto: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>
- For Secure Cloud Analytics Free Trial customers, open a case by email: [swatchc-support@cisco.com](mailto:swatchc-support@cisco.com)

# Change History

| Document Version | Published Date    | Description                                                                                                                    |
|------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 1_0              | April 27, 2022    | Initial version                                                                                                                |
| 1_1              | August 1, 2022    | <ul style="list-style-type: none"><li>• Updating Cisco Support information.</li><li>• Added note for public IPs.</li></ul>     |
| 1_2              | February 17, 2023 | <ul style="list-style-type: none"><li>• Added Proxy Configuration section.</li><li>• Updated Meraki sensor settings.</li></ul> |
| 1_3              | June 21, 2023     | <ul style="list-style-type: none"><li>• Fixed a typo.</li><li>• Updated numbering for procedures.</li></ul>                    |

---

# 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)



© 2023 Cisco Systems, Inc. and/or its affiliates.

All rights reserved.