



# Cisco Secure Cloud Analytics

## Sensor Installation Guide



---

# Table of Contents

<b>Introduction</b>	<b>4</b>
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	7
Checking Your Sensor Version	7
Sensor Access Requirements	7
Network Device Configuration	9
Flow Configuration	10
<b>Sensor Media Installation and Configuration</b>	<b>11</b>
Creating Boot Media	11
Download the sensor ISO file	11
Create a Bootable Optical Disc	12
Create a Bootable USB Flash Drive	12
Installing the Sensor	12
What to Do Next	17
Attaching Sensors to the Web Portal	17
Finding and Adding a Sensor's Public IP Address to a Portal	18
Manually Add a Portal's Service Key to a Sensor	19
Configuring Proxy	20
Confirming a Sensor's Portal Connection	20
Configuring a Sensor to Collect Flow Data	22
Configuring Sensors for Flow Collection	23
<b>Troubleshooting</b>	<b>24</b>
Capture Packets from the Sensor	24

---

Analyze the Packet Capture in Wireshark .....	24
<b>Additional Resources</b> .....	<b>25</b>
<b>Contacting Support</b> .....	<b>26</b>
<b>Change History</b> .....	<b>27</b>

# Introduction

Cisco Secure Cloud Analytics (now part of Cisco XDR) 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.



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.



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.





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](#).



The sensor does not support IPv6.

## 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> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <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> </div>
RAM	4 GB
CPU	at least two cores
Storage Space	<p>60 GB</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Disk space is used to cache production NetFlow data prior to sending records to Secure Cloud Analytics.</p> </div>
Internet Access	required to download packages for the installation process

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"> <li>• 1 USB port, plus a USB flash drive</li> <li>• 1 optical disc drive, plus a writeable optical disc (such as a CD-R disc)</li> </ul>



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.



When deploying the sensor in a VMWare 8 environment, the sensor will fail to load when using the default UEFI boot setting. To fix this issue, on the **Customize Hardware** step, select **VM Options > Boot Options**, then choose **BIOS** from the **Firmware** drop-down list.

### 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 5.1.3), you can check an existing sensor's version from the command line. If you need to upgrade, reinstall the sensor.

1. SSH into the deployed sensor.
2. At the prompt, enter `cat /opt/obsrvbl-ona/version` and press Enter. If the console does not display 5.1.3, 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, domain and port, or configuration
Outbound HTTPS traffic from	yes	<ul style="list-style-type: none"> <li>• port 443 and the IP address is</li> </ul>

<p>the sensor's Control interface to the Secure Cloud Analytics service hosted on Amazon Web Services</p>		<p>your portal IP address</p> <ul style="list-style-type: none"> <li>• AWS S3 IP addresses for your Secure Cloud Analytics region. As the AWS IP addresses can change, refer to the <a href="#">AWS IP address ranges</a> help topic and search for S3 service and your AWS region in the provided JSON file. To find your AWS region, go to your Secure Cloud Analytics dashboard and scroll to the bottom of the page. A field in the footer displays the name of the region for your portal which corresponds to the following AWS regions: <ul style="list-style-type: none"> <li>◦ North America (N. Virginia): us-east-1</li> <li>◦ Europe (Frankfurt): eu-central-1</li> <li>◦ Australia (Sydney): ap-southeast-2</li> </ul> </li> </ul>
<p>Enforce the sensor to only communicate with known Cisco addresses</p>	<p>no</p>	<ol style="list-style-type: none"> <li>1. SSH into the sensor as an administrator.</li> <li>2. In the command prompt, enter this command:  <pre>sudo nano opt/obsrvbl-ona/config.local</pre> and press <b>Enter</b> to edit the configuration file.</li> <li>3. Update the <code>OBSRVBL_SENSOR_EXT_ONLY</code> setting to be the following: <code>OBSRVBL_SENSOR_EXT_ONLY=true</code>.</li> <li>4. Press <b>Ctrl + O</b> to save the changes.</li> </ol>

		<ol style="list-style-type: none"> <li>5. Press Ctrl + x to exit.</li> <li>6. At the command prompt, enter <code>sudo service obsrvbl-ona restart</code> to restart the sensor.</li> </ol>
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"> <li>• us.archive.ubuntu.com:443/TCP</li> <li>• us.archive.ubuntu.com:80/TCP</li> </ul>
Outbound traffic from the sensor's Control interface to a DNS server for hostname resolution	yes	<ul style="list-style-type: none"> <li>• [local DNS server]:53/UDP</li> </ul>
Inbound traffic from a remote troubleshooting appliance to your sensor	no	<ul style="list-style-type: none"> <li>• 54.83.42.41:22/TCP</li> </ul>



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	<a href="#">Configuration Examples and TechNotes</a>

	Analyzer (SPAN)	
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/](https://configurenetflow.info/) or [https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco\\_NetFlow\\_Configuration.pdf](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.

# 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 on 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 Secure Cloud Analytics as an administrator.
2. Select **Help (?) > On-Prem 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**.

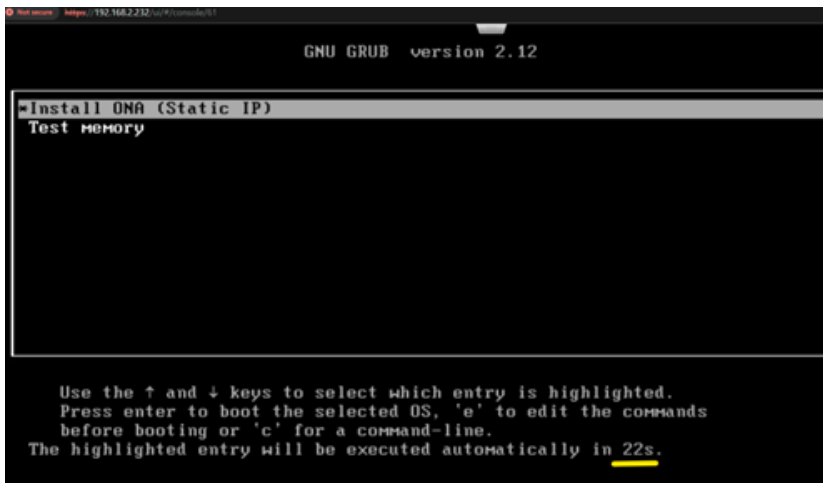


Creating a bootable USB flash drive deletes all information on the flash drive. Ensure that the flash drive does not have any other information on it.

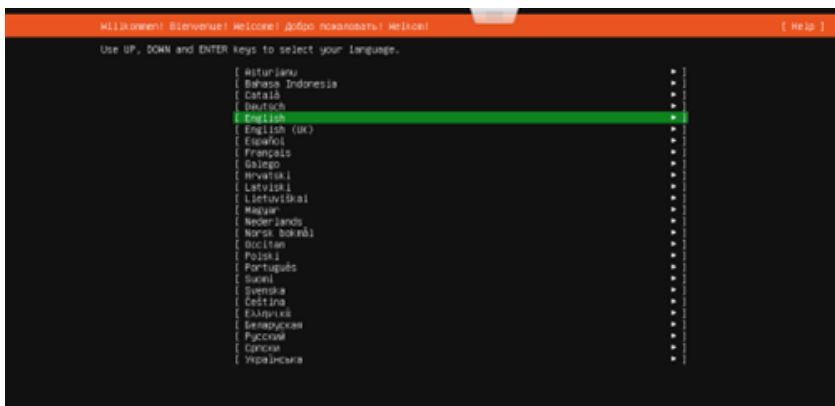
## Installing the Sensor

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.

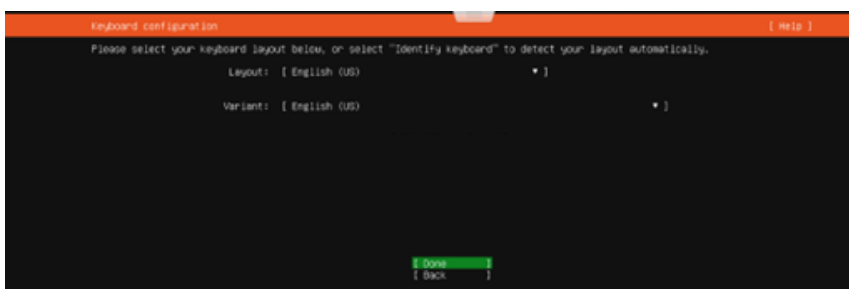
2. Select **Install ONA (Static IP)** at the initial prompt, then press Enter.



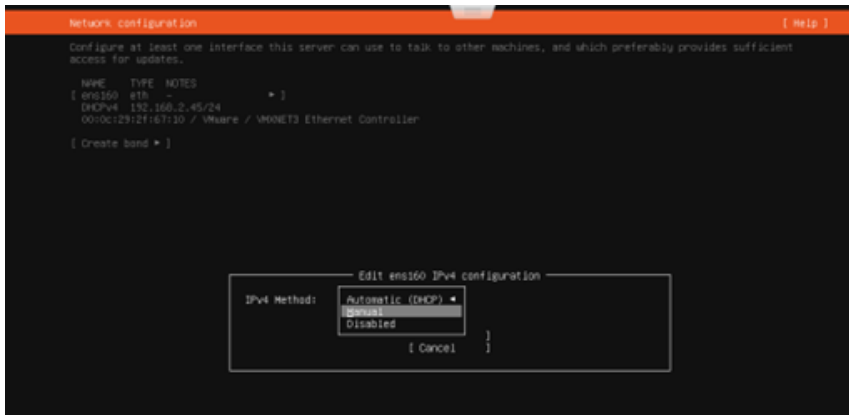
3. Select a language from the language list using the arrow keys, then press Enter.



4. For the **Keyboard configuration**, you have the following options:
  - Select a **Layout** and **Variant** to configure the keyboard, then press Enter.
  - Select **Identify keyboard**, then press Enter.



- For the **Network configuration**, select **Manual** and press Enter.

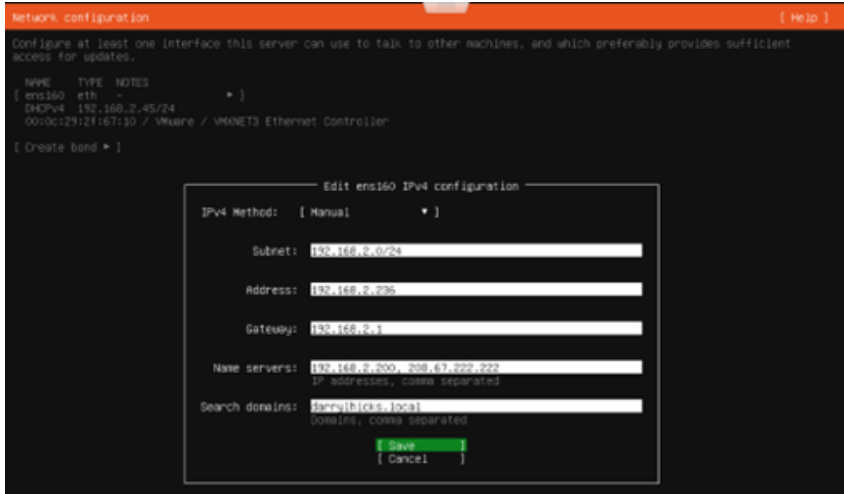


**i** All other network interfaces are automatically configured as Mirror interfaces.

- Enter a **Subnet** for the appliance, select **Continue** with the arrow keys, and press Enter.
- Enter an **IP address** for the appliance, select **Continue** with the arrow keys, and press Enter.
- Enter a **Gateway** router IP address, select **Continue** with the arrow keys, and press Enter.
- (Optional) For **Search domains**, enter the domain(s) that will be automatically appended to the hostname when attempting to resolve to an IP address, select **Continue** with the arrow keys, and press Enter.

**i** 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.

**i** 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 administrative permissions, then select **Continue** with the arrow keys and press Enter.
11. Enter **Your servers name**, which is the name the sensor will use when communicating with other computers and will be visible in the Secure Cloud Analytics portal, then select **Continue** with the arrow keys and press Enter.
12. Enter the **Username for your account**, which is the non-root account with administrative permissions, then select **Continue** with the arrow keys and press Enter.
13. **Choose a password for the new user**, then select **Continue** with the arrow keys and press Enter.
14. **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.

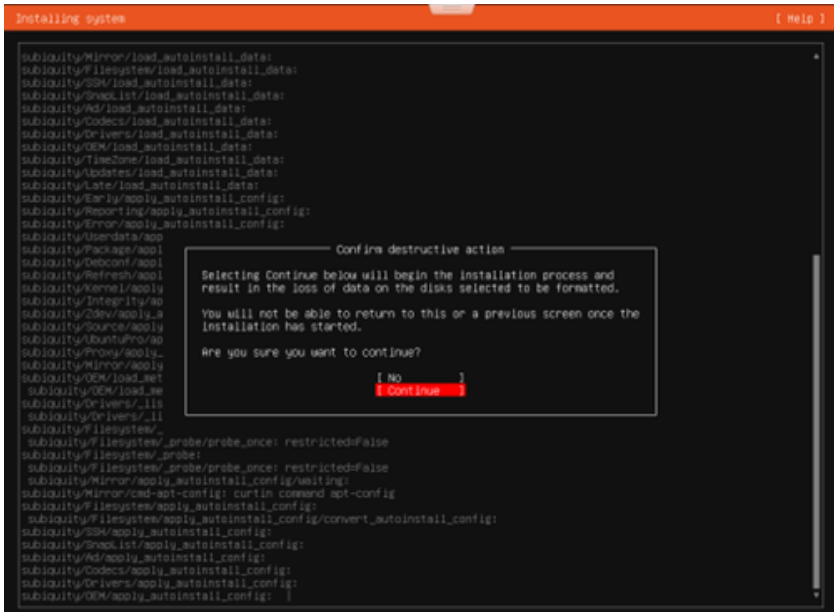


The account you create during setup is the only account you can use to access the virtual machine. This installation does not create a separate Secure Cloud Analytics portal account.



15. To confirm the installation process, select **Continue**, 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.

16. When the installer displays **Installation Complete**, select **Reboot Now** with the arrow keys, then press Enter to restart the appliance.

```

Installation complete! [ Help ]

Installing missing packages
Installing packages on target system: ['grub-pc']
configuring lscl service
configuring raid (raid1) service
configuring WME over TCP
Installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring mailpath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system boot loader
installing grub to target devices
copying metadata from /cdrom
final system configuration
calculating extra packages to install
installing openssh-server
retrieving openssh-server
curtin command system-install
unpacking openssh-server
curtin command system-install
configuring cloud-init
downloading and installing security updates
curtin command in-target
restoring apt configuration
curtin command in-target
subiquity/late/main:
subiquity/late/main/command_0: rm -f /target/var/cache/apt
subiquity/late/main/command_1: cp -r /cdrom/apt /target/var/cache/
subiquity/late/main/command_2: curtin in-target --target /target -- apt-get -y install apt-transport-https
ipables-persistent ipset libjansson4 libidn11 liblz0-2 libnet1 libyaml-0-2 nano ntp ntpdate snmp tcpdump net-tools
libnmap-dev python-dnswalk
subiquity/late/main/command_3: if [ -d /sys/firmware/efi ]; then
apt-get install -y efibootmgr
efibootmgr -o $efibootmgr | perl -n -e '/boot(.+)+\s+ubuntu/ && print $1'
fi
subiquity/late/main/command_4: cp -r /cdrom/ona/ /target/root/
subiquity/late/main/command_5: curtin in-target --target /target -- bash -xv /root/ona/configure.sh
Power Off Now
Reboot Now

```

17. 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. See [Sensor Access Requirements](#) for more information.
- 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.ext.eu-prod.observbl.com> (EU)
- <https://sensor.ext.anz-prod.observbl.com> (Australia)

**i** 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.

**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.

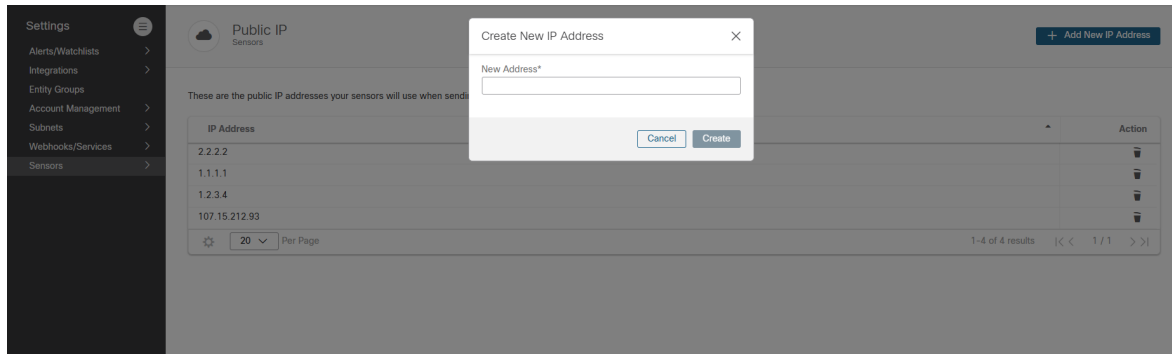
## Finding and Adding a Sensor's Public IP Address to a Portal

1. SSH into the sensor 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$
```

**i** Your service host url may be different based on your location. In your Secure Cloud Analytics portal, go to **Settings > Sensors** and scroll to the bottom of the page to find your service host url.

3. Copy the `identity` IP address.
4. Log out of the sensor.
5. Log in to the Secure Cloud Analytics as a site administrator.
6. Select the **Settings > Sensors > Public IP**.
7. Click **Add New IP Address**.
8. Enter the `identity` IP address in the **New Address** field.



9. Click **Create**. 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 20 minutes before a new sensor is reflected in the portal.

## Manually Add a Portal's Service Key to a Sensor

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 in to Secure Cloud Analytics 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.

**Service Key:** ..... (show)

**Service Host:** `https://sensor. .... .obsrvbl.com`

4. SSH into 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. Add the following lines, replacing `<service-key>` with the portal's service key and `<service_host_url>` with your regional service host url:

```
# Service Key
```

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

**i** In your Secure Cloud Analytics portal, go to **Settings > Sensors** and scroll to the bottom of the page to find your service host url.

See the following image for an example:

```
# Service Key
OBSRVBL_SERVICE_KEY="[REDACTED]"
OBSRVBL_HOST="https://sensor.[REDACTED].obsrvbl.com"
```

7. Press Ctrl + 0 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.

**i** It can take up to 20 minutes before a new sensor is reflected in the portal.

## 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 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"`
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.

**i** It can take up to 20 minutes before a new sensor is reflected in the portal.

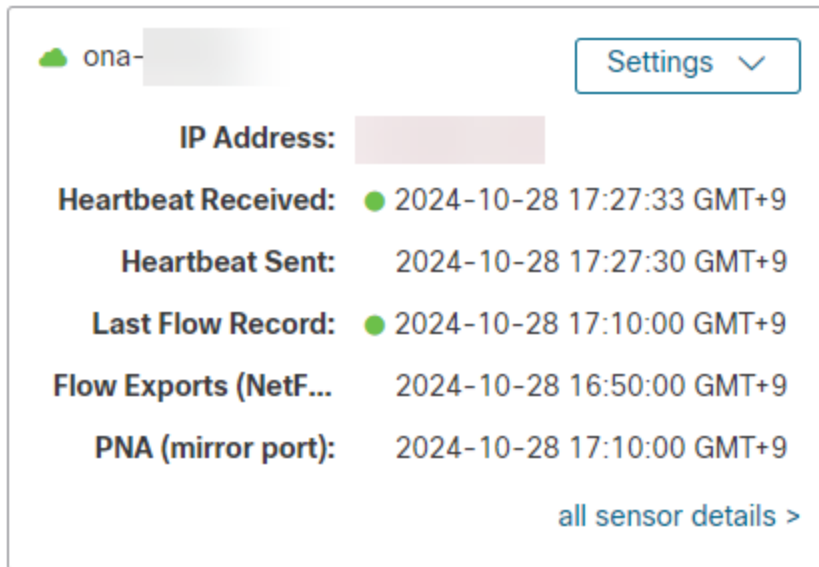
## Confirming a Sensor's Portal Connection

After a sensor is added to the portal, confirm the connection in Secure Cloud Analytics.

**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. Log in to Secure Cloud Analytics.
2. Select **Settings > Sensors**. The sensor appears in the list.

### Cloud Configured On Premises Sensors - ONA



ona- Settings ▾

**IP Address:** [REDACTED]

**Heartbeat Received:** ● 2024-10-28 17:27:33 GMT+9

**Heartbeat Sent:** 2024-10-28 17:27:30 GMT+9

**Last Flow Record:** ● 2024-10-28 17:10:00 GMT+9

**Flow Exports (NetF...:** 2024-10-28 16:50:00 GMT+9

**PNA (mirror port):** 2024-10-28 17:10:00 GMT+9

[all sensor details >](#)

If you do not see the sensor on the **Sensors** page, log into the sensor to confirm the connection.

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

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

**i** Your service host url may be different based on your location. In your Secure Cloud Analytics portal, go to **Settings > Sensors** and scroll to the

 bottom of the page to find your service host url.

3. Log out of the sensor.


## 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. If you want to use additional UDP ports, you must configure them in the web portal.


You can configure collection of the following flow types in the web portal UI:

- NetFlow v5 - Port 2055/UDP (open by default)
- NetFlow v9 - Port 9995/UDP (open by default)
- IPFIX - Port 4739/UDP (open by default)
- sFlow - Port 6343/UDP

 We have provided the default ports, but these can be configured to your preferred ports in the web portal UI.


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 Secure Cloud Analytics as an administrator.
2. Select **Settings** > **Sensors**.
3. Click the **Settings** drop-down menu for the sensor you added.
4. Choose **configure NetFlow/IPFIX**.

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

5. Click **Add New Probe**.
6. Choose a flow type from the **Probe Type** drop-down menu.
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. Choose a **Protocol** from the drop-down menu.
9. Choose a **Source** from the drop-down menu.
10. Click **Save**.

 It can take up to 30 minutes for sensor configuration updates to be reflected in the portal.

---

# 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 into the sensor as an administrator.
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/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>

## 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>
1_4	April 8, 2024	<ul style="list-style-type: none"> <li>Updated the introduction in the <i>Sensor Media Installation and Configuration</i> section.</li> <li>Minor formatting changes.</li> </ul>
1_5	October 30, 2024	Updated the <i>Sensor Access Requirements</i> section.
2_0	December 4, 2024	Updated the sensor version, <i>Installing a Sensor</i> section, <i>Finding and Adding a Sensor's Public IP Address to a Portal</i> section, and <i>Sensor Prerequisites</i> section.
2_1	April 21, 2025	<ul style="list-style-type: none"> <li>Added VMware boot option note to the <i>Virtual Machine Additional Requirements</i> section.</li> <li>Updated the <i>Manually Add a Portal's Service Key to a Sensor</i> section to include the <code>OBSRVBL_HOST</code> configuration information.</li> </ul>
2_2	October 17, 2025	Removed the North America only limitation for enforcing the sensor to only communicate with known Cisco addresses.

---

# 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)

