FORESCOUT

Forescout

eyeInspect Installation Guide v5.5.0

Contact Information

Forescout Technologies, Inc.
2400 Dallas Pkwy, Suite 230, Plano, TX 75093
https://www.forescout.com/support-hub/
Toll-Free (US): 1-866-377-8773
Tel (Intl): 1-708-237-6591

About the Documentation

- Refer to the Documentation Portal for additional technical documentation: https://docs.forescout.com/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

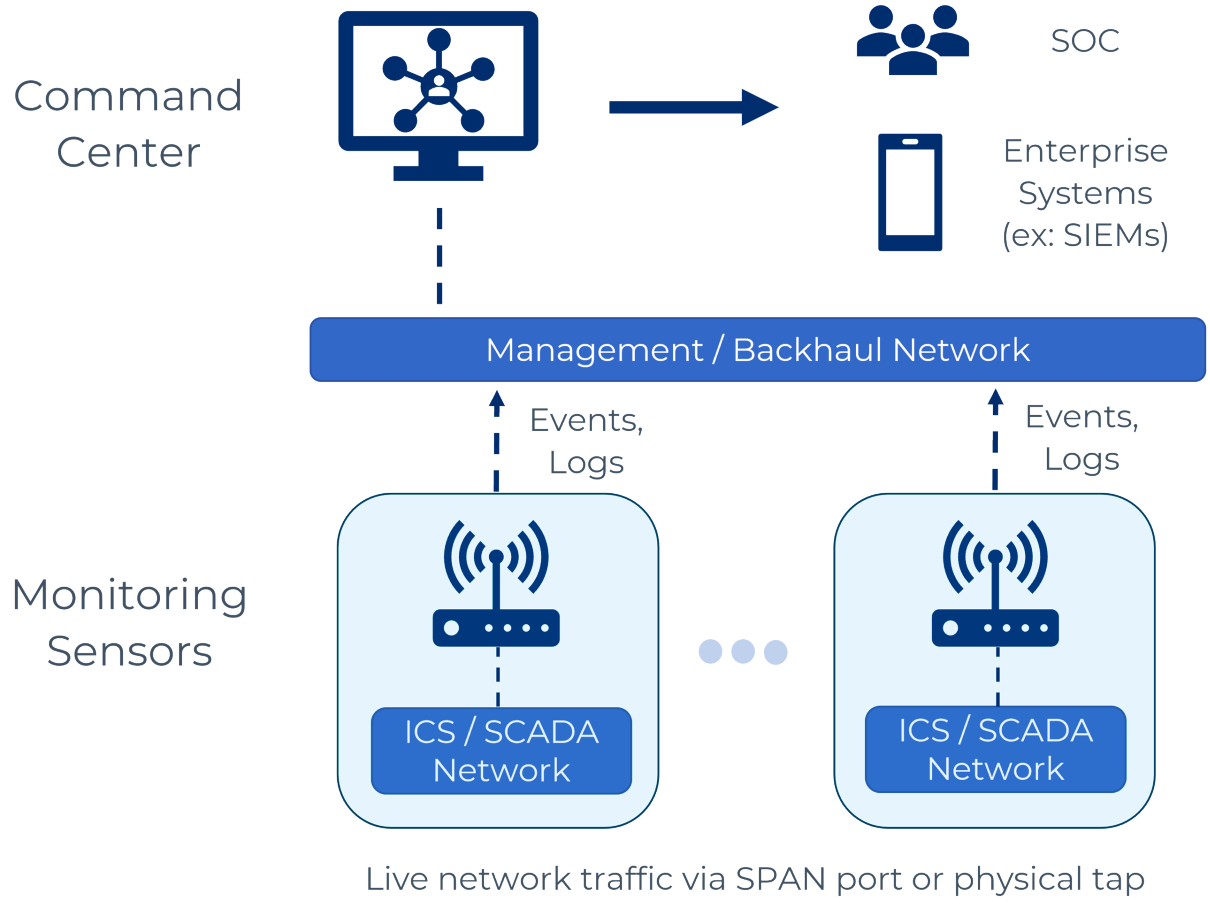
Table of Contents

About eyeInspect

This guide describes how to install eyeInspect. This section introduces the eyeInspect components and the terminology used in this document.

eyeInspect Architecture

An eyeInspect deployment consists of a Command Center and one or more Sensors, as shown in the figure below. Sensors can be Passive Sensors or Active Sensors.



The Command Center is a web-based application used for sensor and event management and provides visual representations and analysis capabilities for logs and events. The Command Center can interface with several third-party enterprise systems (for example, a SIEM system).

A Passive Sensor sends events and logs to the Command Center via the management interface, connected to the ICS / SCADA network via a SPAN / mirroring port to passively listen to the network traffic. Passive Sensors have several self-configuring detection engines and detection levels. Each Passive Sensor has one or more network monitoring ports and a management interface.

An Active Sensor remains inactive unless the eyeInspect operator issues a direct command. When

a command is issued, the Active Sensor sends controlled queries to assets selected by the operator. Information retrieved in this way is then returned to the Command Center. An Active Sensor is connected to the ICS / SCADA network as a regular asset, and to the Command Center via the management interface.

The Command Center, Passive Sensor, and Active Sensor can all be accessed via SSH for server management. For demo and testing setups, the Monitoring Sensor can be installed together with the Command Center in one application.

eyeInspect Glossary

This section explains the terminology used by eyeInspect.

Term	Definition
Bundled installation	An installation of eyeInspect in which the Command Center, Flow Aggregator Forwarder, Passive Sensor and Active Sensor are installed together on one server.
Command Center	The eyeInspect management interface used for sensor and event management. The Command Center is a web based application accessible via HTTPS.
Enterprise Command Center	An optional component for the eyeInspect Suite, offering an enterprise-level management interface to monitor multiple Command Centers.
Active Sensor	An optional component of the eyeInspect Suite. It allows the eyeInspect operator to send requests for information to ICS assets in a controlled way.
Passive Sensor	An essential component of the eyeInspect Suite: a collection of Modules. A Passive Sensor monitors a subnet, i.e., a set of hosts, for malicious activities.
sdconfig	sdconfig is a utility used to configure the eyeInspect system.
eyeInspect operator	Person who uses eyeInspect, e.g. the person responsible for configuring and managing the system.
eyeInspect Physical Appliance	eyeInspect installed on a physical server, e.g. a 19" rack server or an embedded PC.
eyeInspect Virtual Appliance	eyeInspect deployed as virtual machine on a hypervisor, usually VMware ESXi.
WMI	Windows Management Instrumentation, a standard way of interacting with Windows hosts, which is used by Active Sensors.

eyeInspect Installation Prerequisites

Learn about the necessary preparations and prerequisites that must be done prior to installing eyeInspect.

Before you can install eyeInspect, there are several prerequisites that need to be addressed, including:

- Network, authentication, and credential requirements
- Configure firewall and proxy rules
- Download the eyeInspect installation bundle ISO
- Create bootable USB with the ISO
- Upload eyeInspect license files

Network, Authentication and Credential Requirements

To install and configure eyeInspect, establish the following:

- **Network:** The network on which eyeInspect will be included.
- **SPAN Port(s):** The ports for inbound and outbound monitoring for the targeted network segment(s).
- **Hostnames, Static IP Address, Gateway, and Subnet Mask for all desired components:** Command Center, Enterprise Command Center, Passive Sensors, and Active Sensors.
- **NTP Server Address:** The server address used for time synchronization. This is not required for short-term pilot or demonstration deployments.
- **For an existing LDAP/AD authentication database:** Provide the LDAP server address and bind information. LDAP-based authentication can also be implemented after the initial installation.
- **For querying certain assets with an Active Sensor:** Provide access and credentials for the selected assets that you want the Active Sensor to send queries to (for example, WMI or SEL).

Configure Firewall and Proxy Rules for eyeInspect

Before you can install or configure your eyeInspect Command Center or Sensors, you must set your firewall and proxy rules.

eyeInspect Firewall Rules

Source	Destination	Port	Description of Connection
Command Center	Active Sensor	22 (ssh)	System Management
Command Center	Passive Sensor	22 (ssh)	System Management
Enterprise Command Center	Command Center	443	Sends eyeInspect data
Active Sensor	Command Center	9092	Sends Active Sensor data
Active Sensor	Target Hosts	Service-specific	Performs Active Sensor scans (WMI, SEL, etc.)
Passive Sensor	Command Center	29999* 9092	Sends Passive Sensor data
eyeInspect Operators	Command Center	22 (ssh)	Command Center and Enterprise Command center GUI system management
eyeInspect Operators	Enterprise Command Center	443 (https)	Command Center and Enterprise Command center GUI system management
(Optional) Primary Command Center	Secondary Command Center	5432 22 (ssh)	Bi-directional, Command Center High Availability (not enabled by default)

* Port can be customized for your system.

Firewalls and Proxies for Active Sensors

Active Sensors need to be connected to the network of their target assets. Having routers, firewalls, or proxies between the Active Sensor and their target asset diminishes the sensor's ability to retrieve data.

Firewalls and Proxies for Passive Sensors

Starting with eyeInspect v5.1.0 and on, due to the change of the communication direction between the Command Center and Passive Sensor, the default port via which the Command Center and the Passive Sensor communicate has changed to 29999. To change the port to something other than 29999, follow the instructions in **Startup options for enrolling the Passive Sensor to a Command Center** from the eyeInspect 5.5.0 Configuration Guide.

The following traffic must be allowed to reach the Command Center and the Passive Sensor:

- DNS access for Sensor and Command Center
- LDAP access for Command Center and Enterprise Command Center
- NTP access for the Sensor, Command Center and Enterprise Command Center (not required for demo deployments)
- SMTP access for Command Center alert forwarding

- Syslog access for Command Center alert forwarding

Note:
The open port 29999 for communication between the Command Center and Passive Sensor is not needed for bundled configurations where the Command Center and Passive Sensor are on one server.

Download the eyeInspect Installation Bundle ISO

The eyeInspect installation bundle ISO includes all the necessary files to perform a fresh eyeInspect installation, including the Ubuntu operating system.

Download the ISO (***eyeinspect_5.5.1_install_amd64.iso***) from the Forescout Customer Support portal.

Note:
For Forescout OT HW 61 series models, the ISO is ***eyeinspect_5.5.1_install_amd64_61series.iso***.

The ISO contains the following files:

Installer File	Description
ubuntu-22.04.4-live-server-amd64.iso (GNU/Linux 5.15.0-107-generic x86_64)	The Ubuntu Server 22.04.4 LTS operating system for eyeInspect
eyeinspect_u22_1.0.0_configuration_amd64.run **Note:** For Forescout OT HW 61 series models, this file is eyeinspect_u22_1.0.1_configuration_amd64.run	Updates the base operating system with all applicable system updates available at the date of release, configures the OS for eyeInspect, and installs dependencies shared by all eyeInspect components
eyeinspect_command-center_5.5.1_install_amd64.run	Installs the eyeInspect Command Center and required dependencies
eyeinspect_sensor_5.5.1_install_amd64.run	Installs the eyeInspect Passive Sensor and required dependencies
eyeinspect_active-sensor_2.0.0_install_amd64.run	Installs the eyeInspect Active Sensor and required dependencies

Create Bootable USB with the ISO

After downloading the ISO, you need to flash the ISO onto a bootable media such as a flash drive to be able to boot and install eyeInspect.

Upload eyeInspect License Files

This section describes how to upload license files to the eyeInspect Command Center.

eyeInspect requires a valid license file. This file should be uploaded from the eyeInspect Command Center. Once a valid license is uploaded, all applicable functionality will be unlocked in the Command Center GUI.

While the installation and upgrade can be done without the license file, for the final

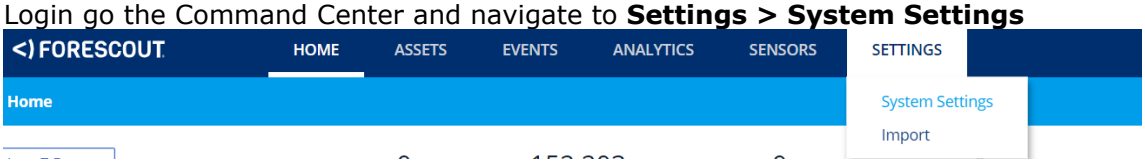
configuration within the Command Center, it is necessary to upload the license file.

Note:

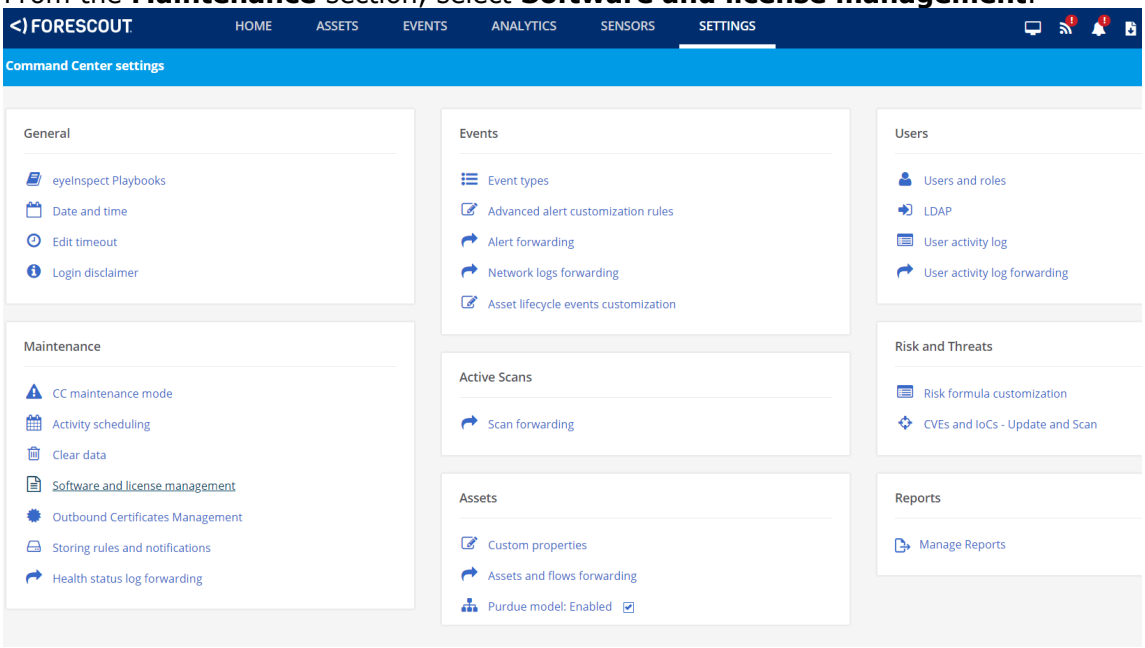
After the eyeInspect license expires, eyeInspect enters a 45-day grace period. During this time, everything works normally and data from sensors continues to be processed by the Command Center. Once the grace period ends, the Command Center stops accepting new data from sensors (similar to maintenance mode). Additionally, if the Command Center is rebooted after the grace period, login will be disabled until a new license is applied. Data processed during and before the grace period remains in the Command Center.

To upload the license file, peform the following steps:

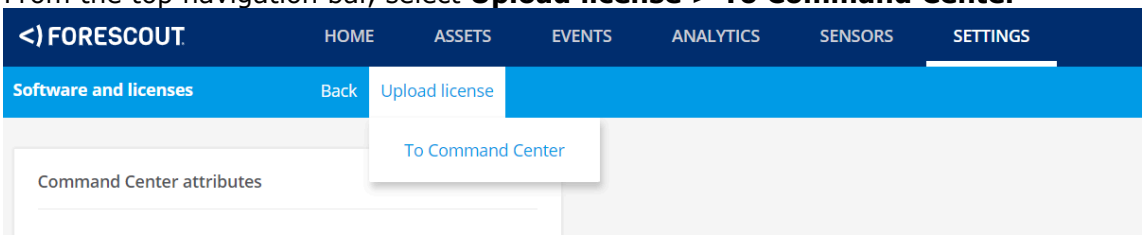
1. Login go the Command Center and navigate to **Settings > System Settings**



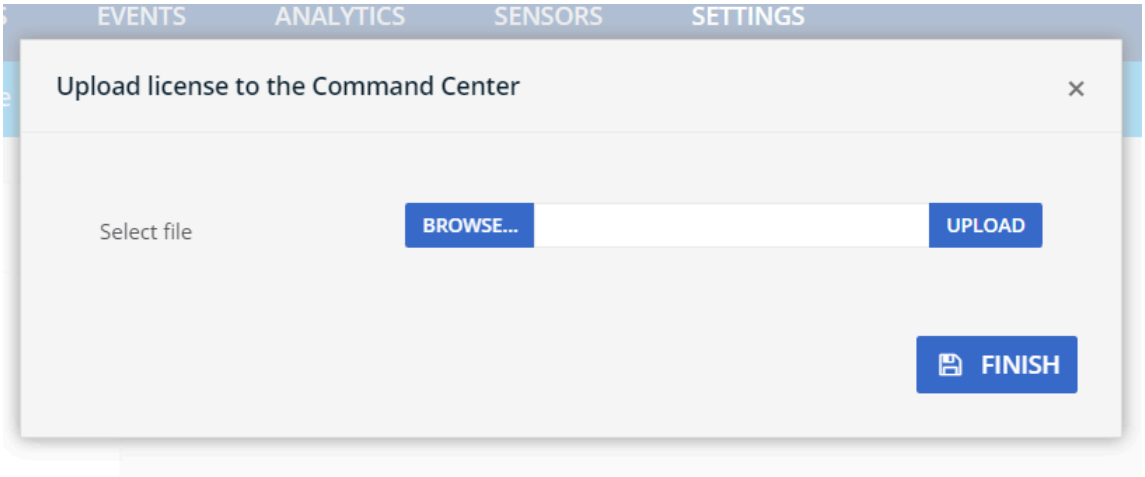
2. From the **Maintenance** section, select **Software and license management**.



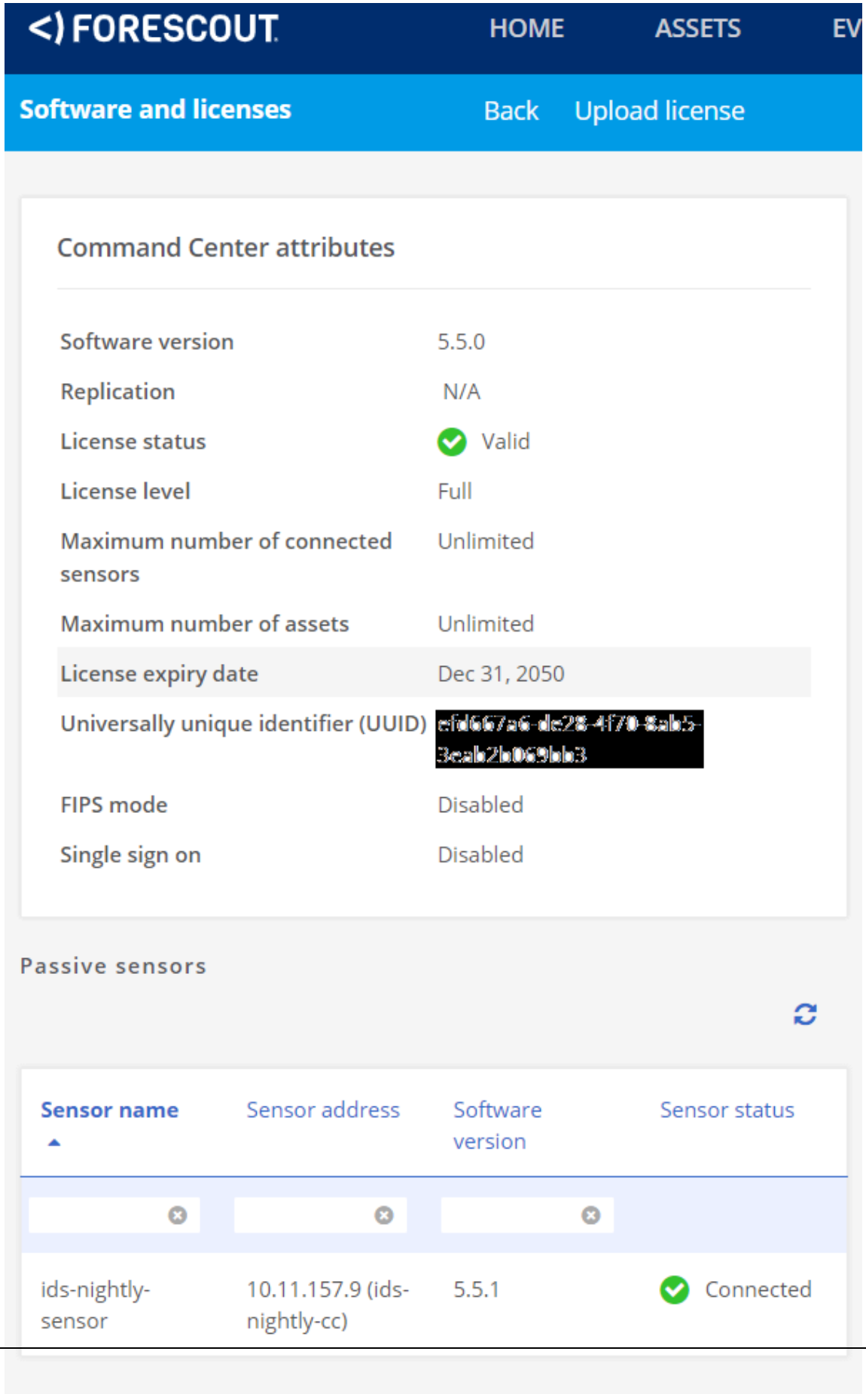
3. From the top navigation bar, select **Upload license > To Command Center**



4. From the **Upload license to the Command Center** dialog, select **BROWSE...** to select the license file on your computer.



5. Select **UPLOAD** to upload the license, and **FINISH** to save. The license details can then be viewed on the Command Center.


FORESCOUT
HOME
ASSETS
EV
Software and licenses
Back
Upload license
Command Center attributes
Software version
5.5.0
Replication
N/A
License status
Valid
License level
Full
Maximum number of connected sensors
Unlimited
Maximum number of assets
Unlimited
License expiry date
Dec 31, 2050
Universally unique identifier (UUID)
efd667a6-de28-4f70-8ab5-3eab2b069bb3
FIPS mode
Disabled
Single sign on
Disabled
Passive sensors
Sensor name
Sensor address
Software version
Sensor status
ids-nightly-sensor
10.11.157.9 (ids-nightly-cc)
5.5.1
Connected

Install eyeInspect

The eyeInspect installation consists of three parts, bundled into one ISO for seamless installation:

A. **Installation of Ubuntu OS 22.04.4 LTS**, which includes:

1. Language
2. Keyboard
3. Ubuntu mirror
4. Disk setup
5. *silentdefense* user
6. Hostname *eyeinspect-iso*
7. OpenSSH server
8. OS configuration

B. **Configuration of eyeInspect system**, which includes:

1. Change of password during initial login
2. Change of the server hostname. The default hostname is ***eyeinspect-iso***. Note that changing server hostname is optional.

C. **Installation of eyeInspect components,** in the following possible options**:**

1. Command Center 5.5.1 and Flow Aggregator Forwarder 1.1.0
2. Passive Sensor 5.5.1 and Active Sensor 2.0.0
3. Bundle installation (both 1 and 2)

Note:
All three parts listed above are bundled together in the installation ISO and the user is guided by the on-screen prompts, as described in the following sections.

Install the Ubuntu OS 22.04.4 LTS

Note:

Before installing the Ubuntu OS, it is necessary to set up the server. Read the next section to know how to do this.

Server Setup

- If the server has UEFI boot capabilities, Secure Boot must be disabled due to required

third-party kernel modules. Please consult your hardware manufacturer's documentation to make sure this feature is disabled before starting the installation of eyeInspect.

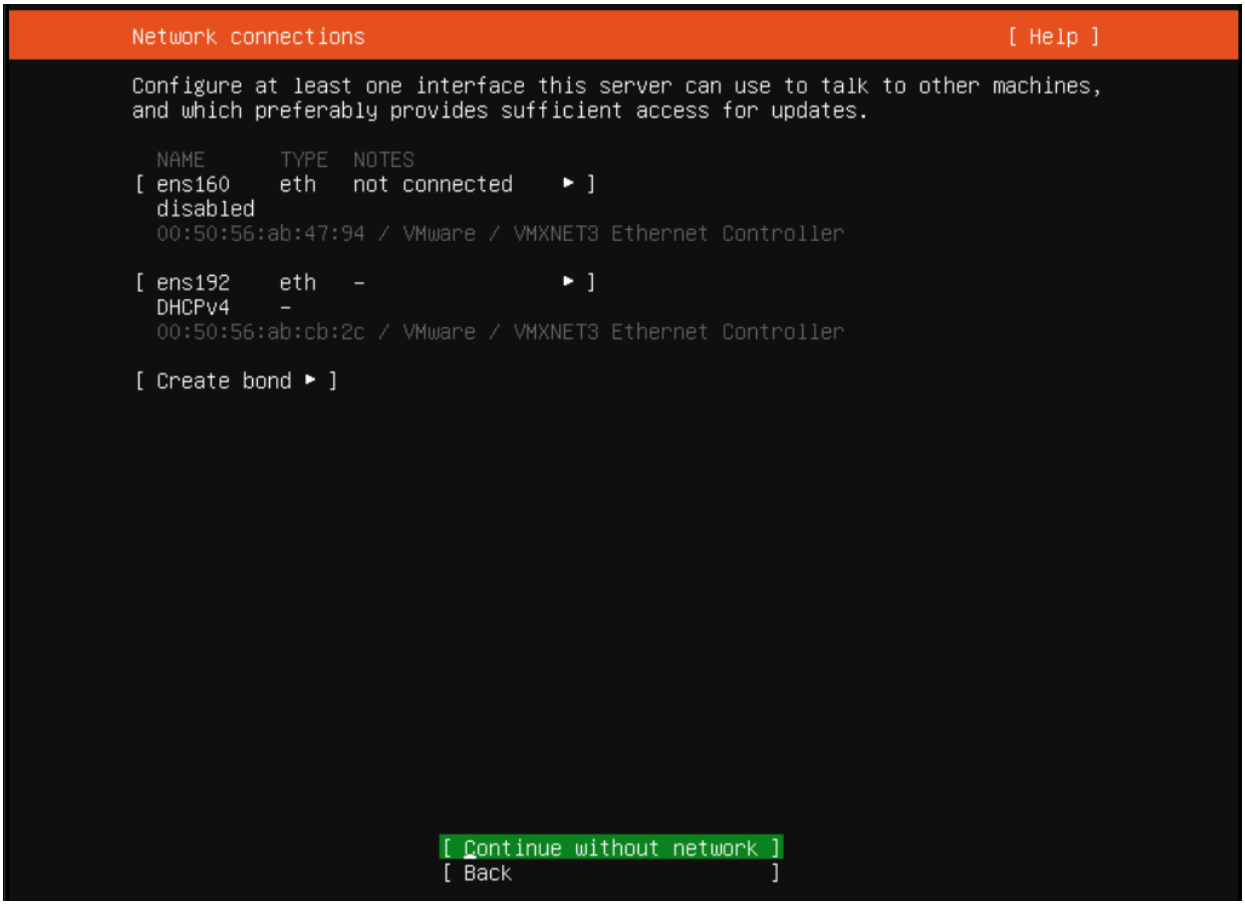
- When installing a server that will only be used as a Passive Sensor, verify the HyperThreading is enabled to improve performance. Please consult your hardware manufacturer's documentation in order to check the status of HyperThreading in the BIOS/UEFI environment.
- During the OS installation, make sure that the Ethernet cable is not connected to the server or that the server cannot reach any DHCP or network discovery service.

Install the Ubuntu OS 22.04.4 LTS

The eyeInspect installation begins by installing the Ubuntu OS 22.04.4 LTS (Long Term Support) Operating System on the server, using either physical media or remotely by using an out-of-band management solution. The installer will require configuring the network on the **Network connections** screen, as described below:

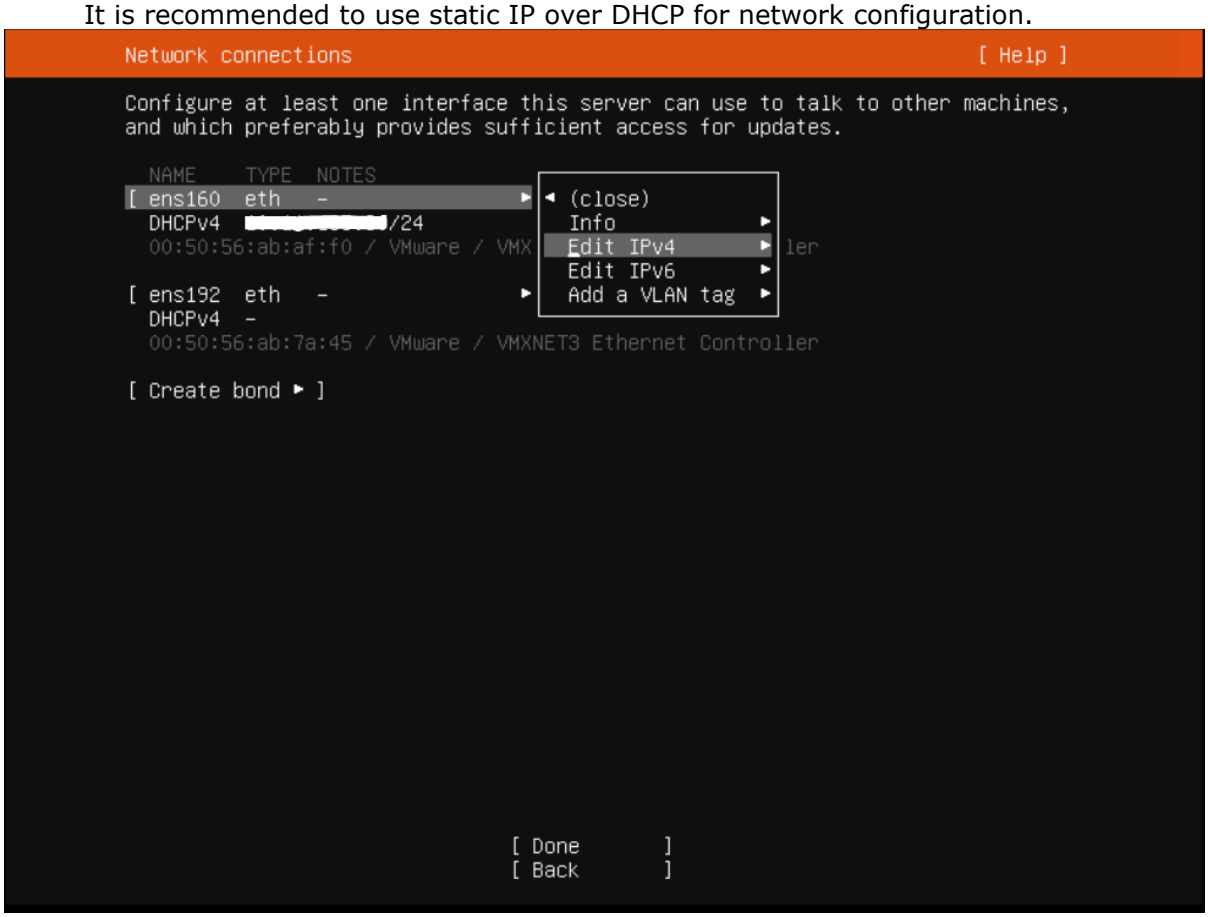
Note:
If DHCP is used, proceed directly to step 6. Navigate to the first interface in the displayed list and press Enter

1. Navigate to the first interface in the displayed list and press **Enter**.

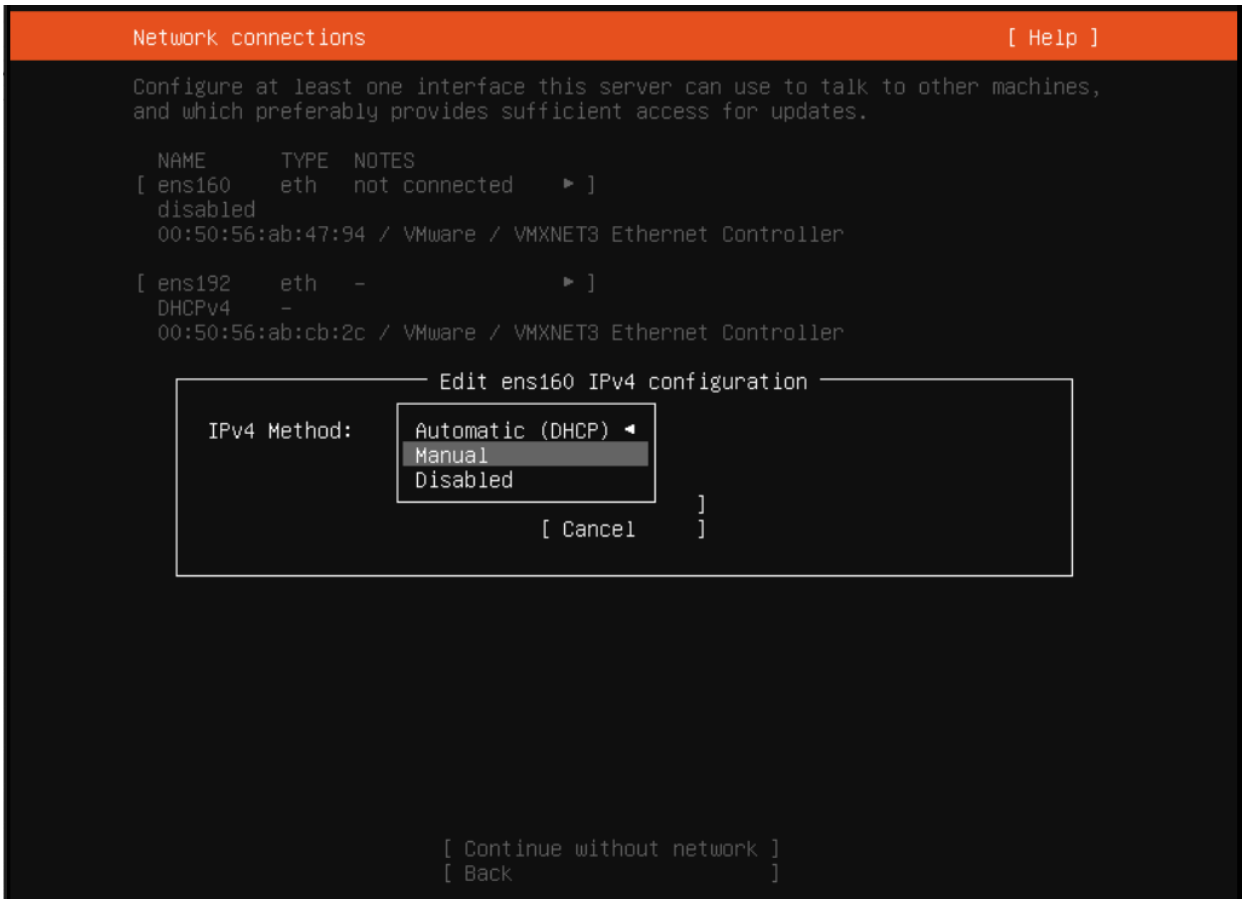


2. Ubuntu defaults to Dynamic Host Configuration Protocol (DHCP). To set a static IP address, select the **Edit IPv4** menu entry, and press **Enter**.

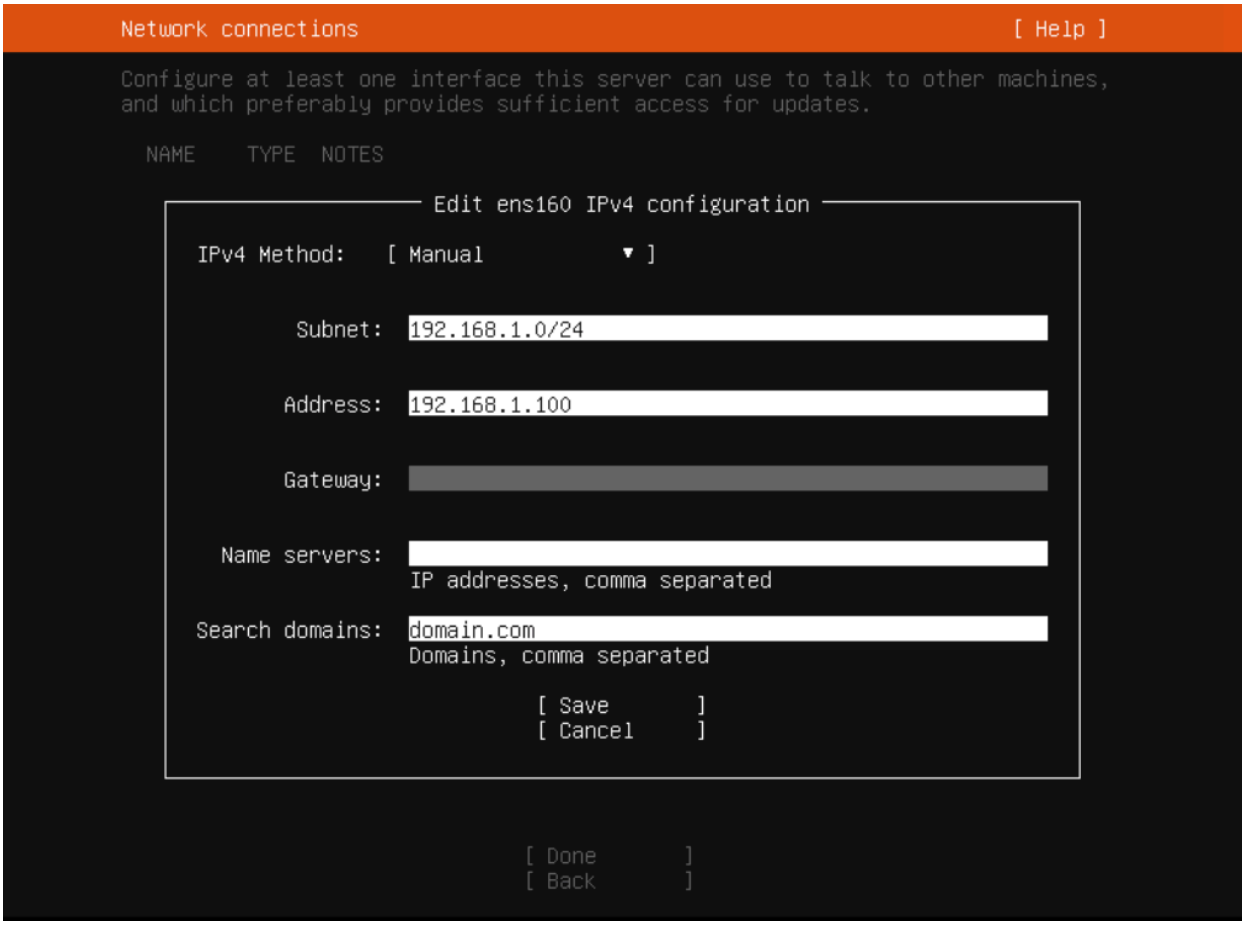
Note:
It is recommended to use static IP over DHCP for network configuration.



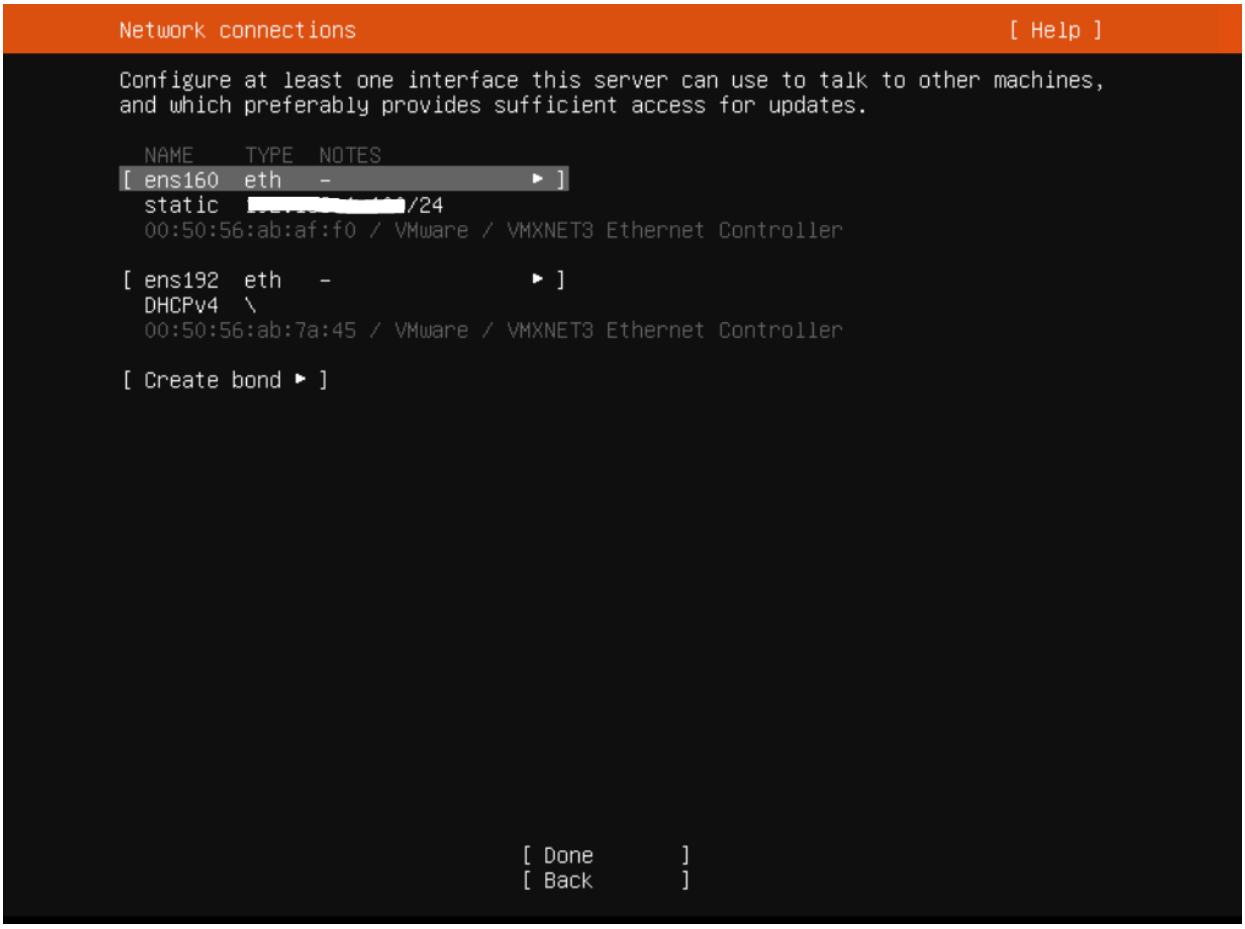
3. Select **Manual** as the IPv4 Method



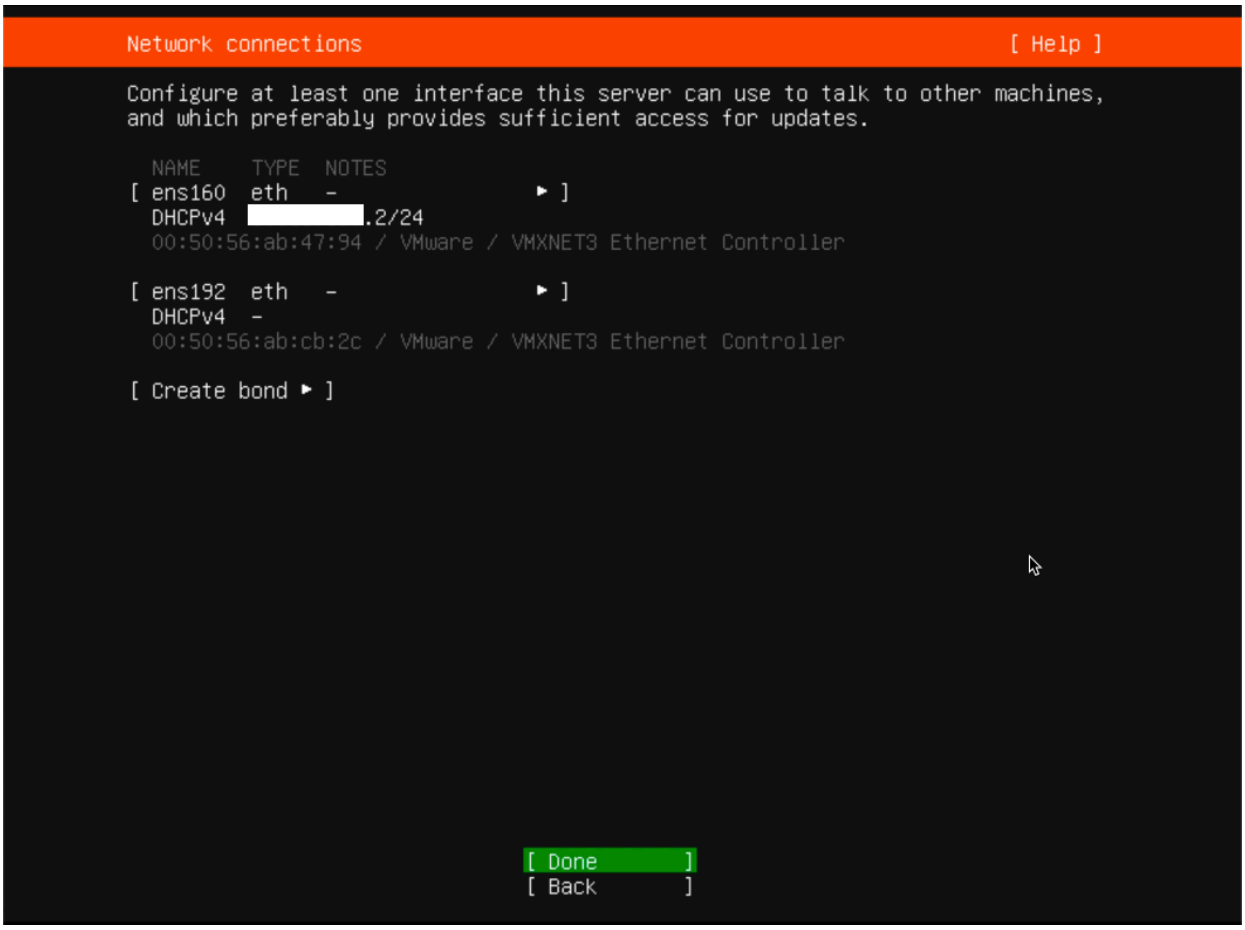
4. Fill in the LAN settings in the provided form, select **Save** and press **Enter**.



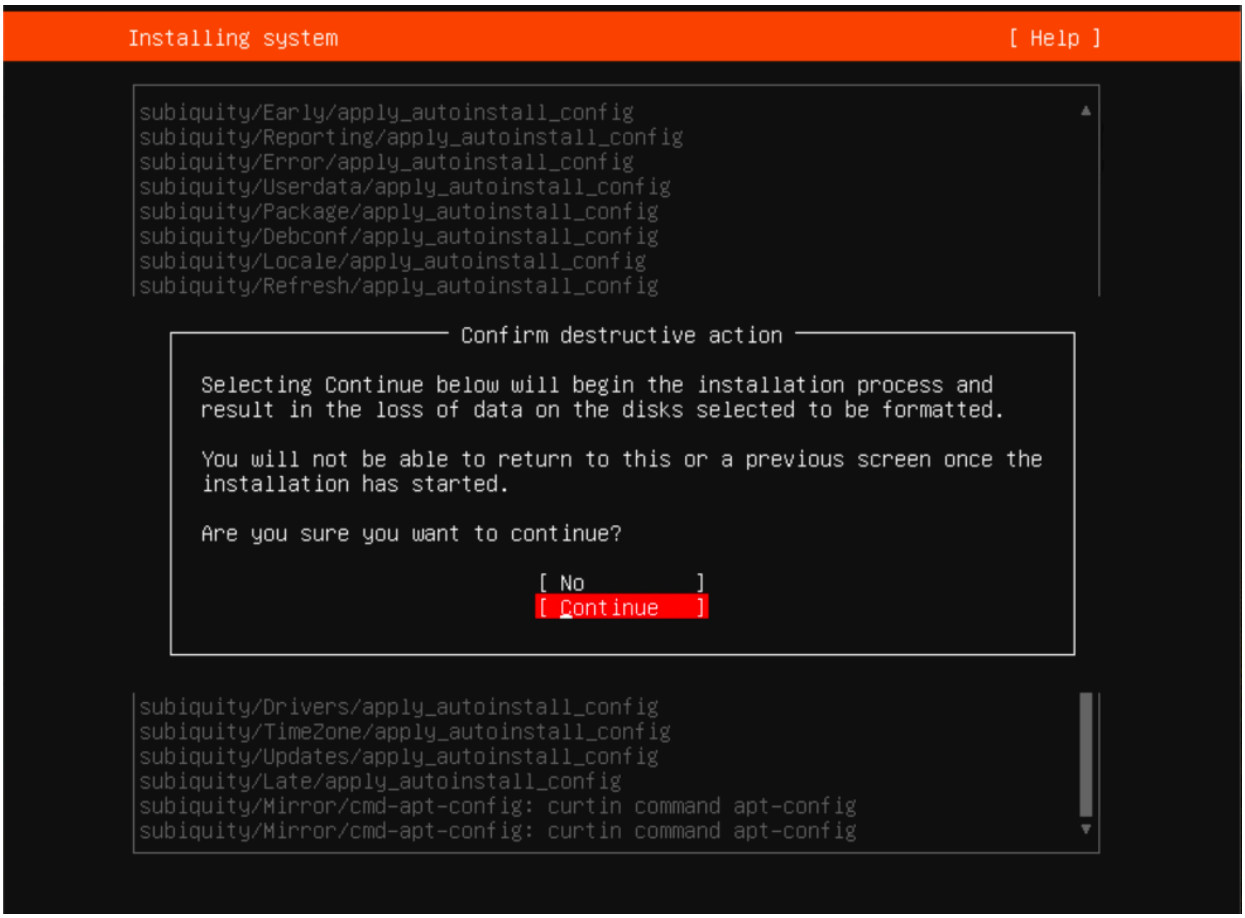
5. Preview the updated network connections, select **Done** and press **Enter**



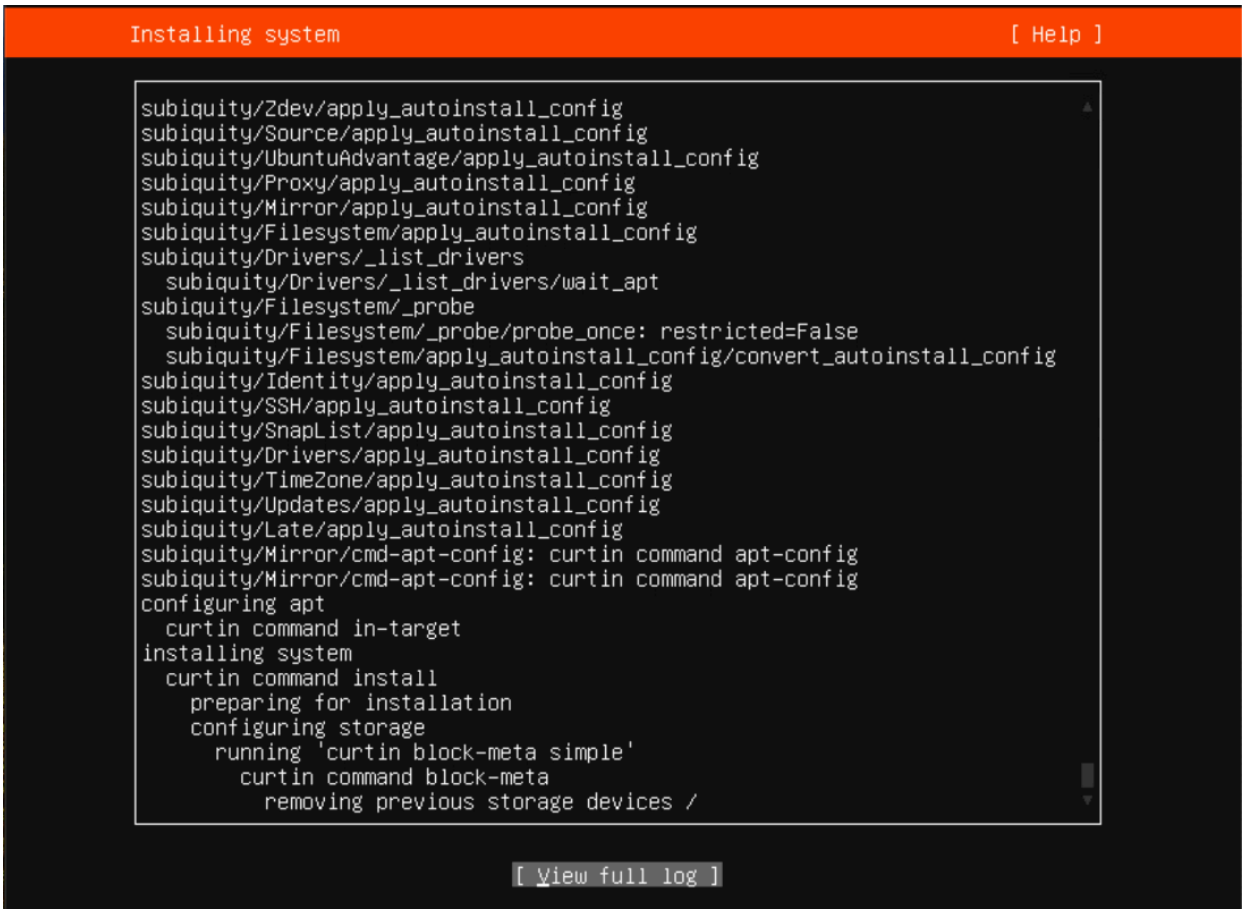
6. The DHCP will automatically provide a new IP address to the first interface. Select **Done** and press **Enter**



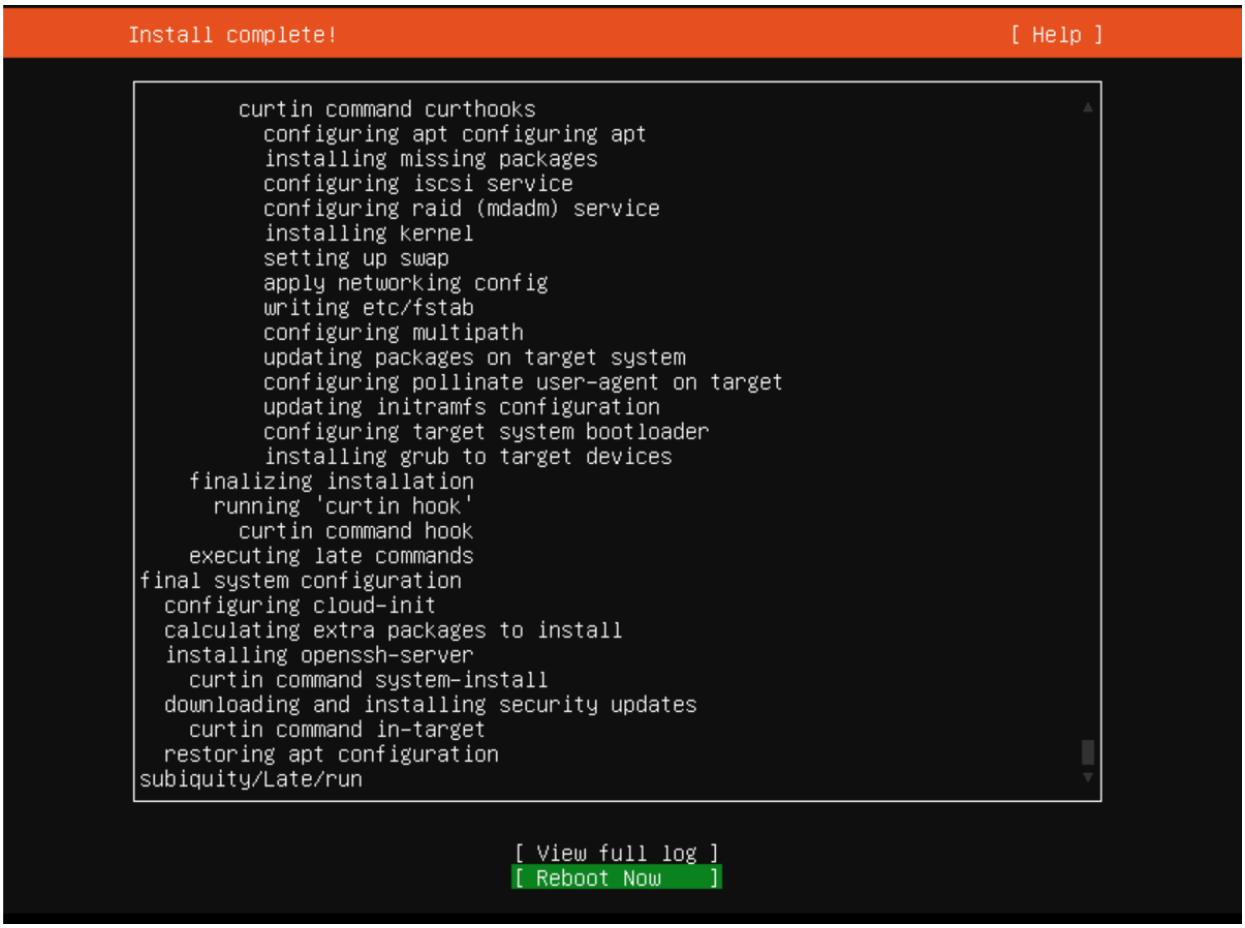
7. On the **Installing system** screen, a dialog appears asking for confirmation to begin installation. Select **Continue** and press **Enter** to proceed.



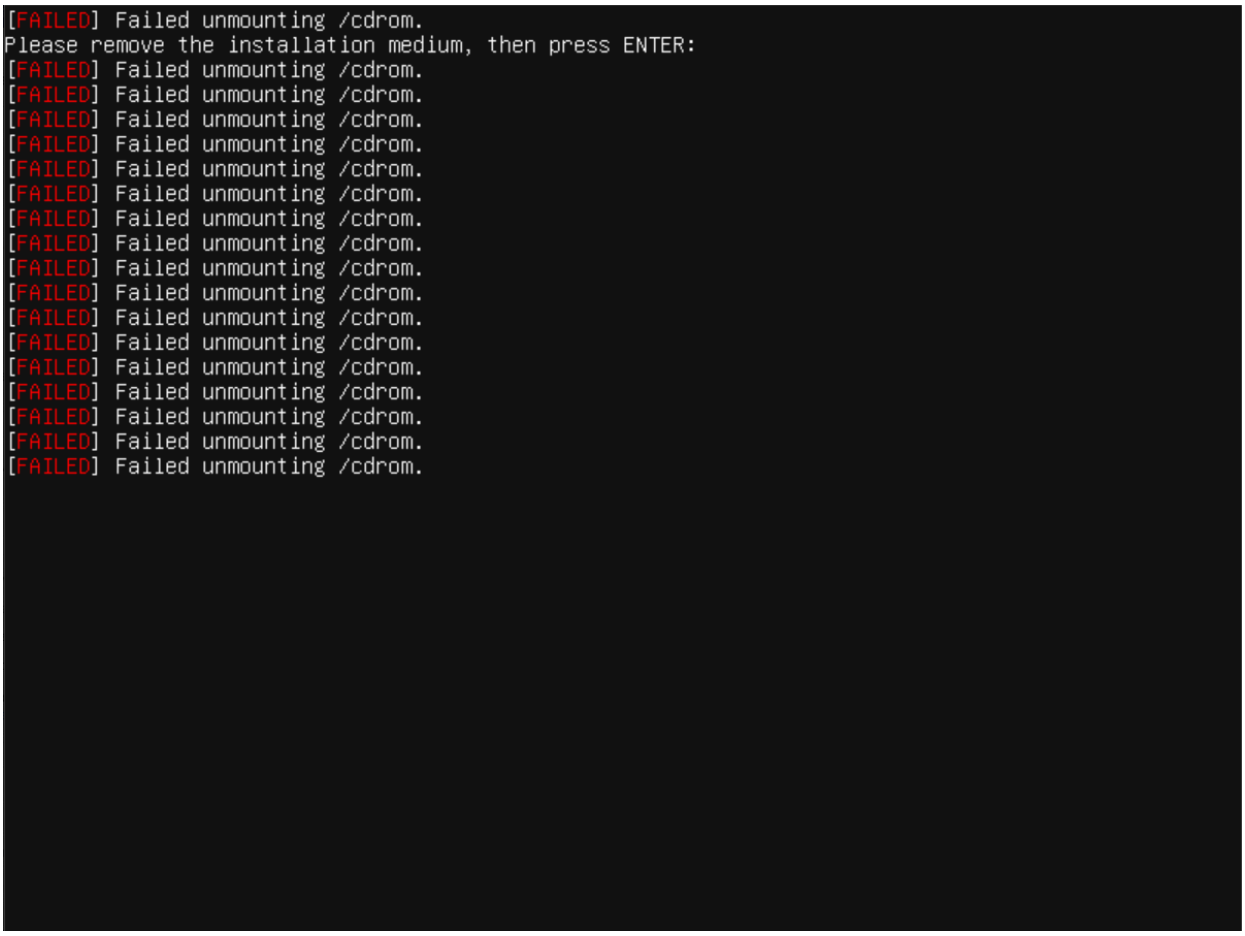
8. On the **Installing system** screen, you can preview the ongoing installation process and, optionally, see the detailed log by selecting **View full log** and pressing **Enter**.



9. When the title of the screen changes to **Install complete!**, continue by selecting **Reboot Now** from the bottom of the screen and press **Enter**.



Note:
If the Ubuntu install media is not removed, you may see the below error. In this case, remove the media as directed and press **Enter.**



The system reboots and proceeds to the eyeInspect system configuration.

(For Forescout OT HW 61 Series Models Only) Troubleshoot Networking Issues

If the management network interface does not work correctly after the OS installation, check whether the network cable for the server management interface is inserted in the correct port. It should be plugged into the first port (**iDRAC**) of the on-board management network interface card, as illustrated below. Other ports should be used for passive sensors.

OT hardware model 6120:

OT hardware model 6140/6160:

Configure the eyeInspect System

The eyeInspect system configuration starts, and the following in-progress screen is shown:

```
------------------------------Forescout eyeInspect------------------------------

   eyeInspect system configuration in progress!

   User silentdefense login will be released once the installation is completed.

--------------------------------------------------------------------------------
```

Upon completion, the user is prompted to change the password after first login.

```
------------------------------Forescout eyeInspect system configuration completed.

   eyeInspect system configuration completed.

   User unblocked, the first login requires a password change.

--------------------------------------------------------------------------------
eyeinspect-iso login:
```

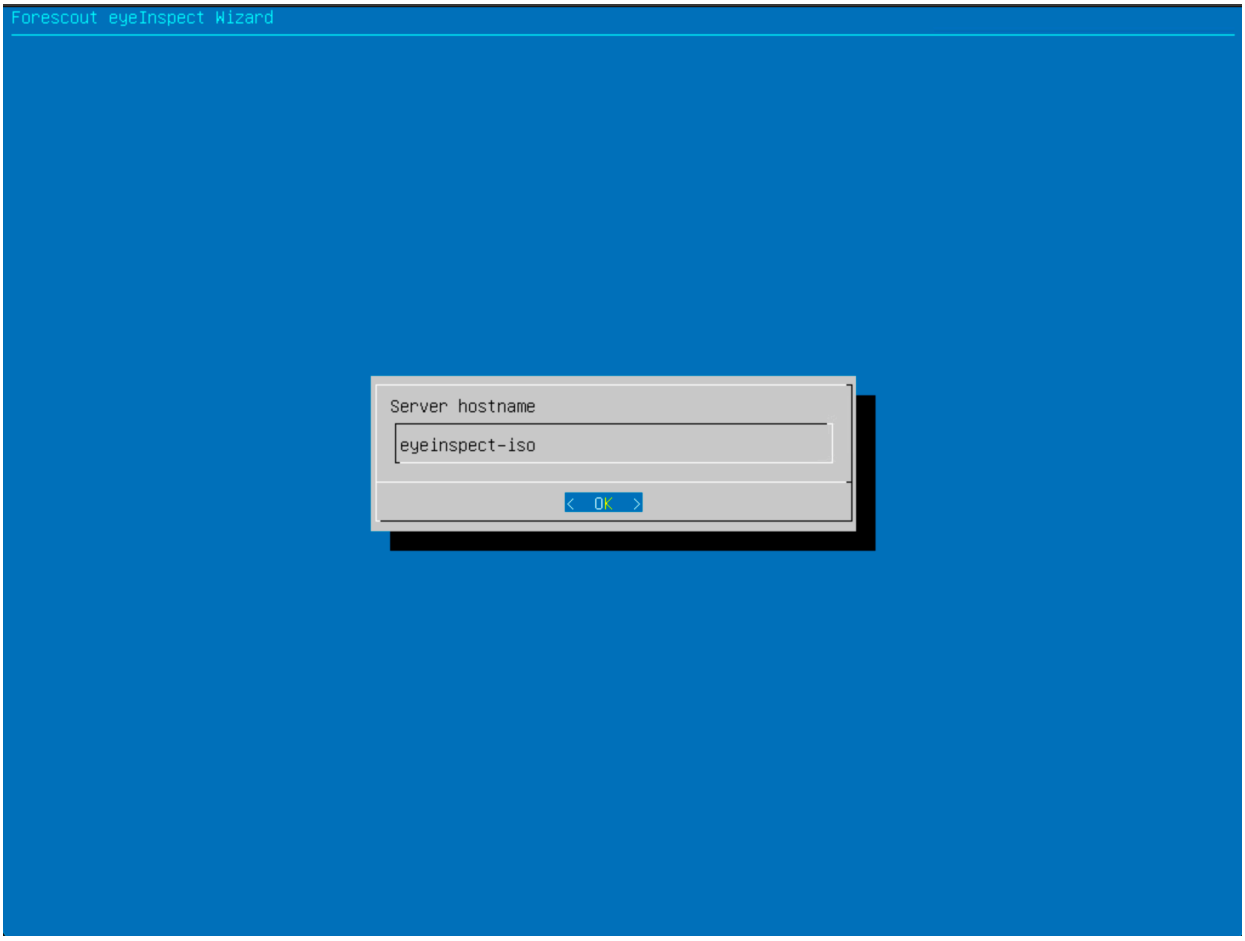
Follow the on-screen instructions to change the password.The initial login credentials are:

- **username: silentdefense**
- **password: silentdefense**

```
------------------------------Forescout eyeInspect system configuration completed.

   eyeInspect system configuration completed.

   User unblocked, the first login requires a password change.

--------------------------------------------------------------------------------
eyeinspect-iso login: silentdefense
Password:
You are required to change your password immediately (administrator enforced).
Changing password for silentdefense.
Current password:
New password:
Retype new password: _
```

After successful password change, the eyeInspect wizard starts.

The **Server hostname** dialog appears and displays the default hostname, ***eyeinspect-iso***..



If desired, change the hostname here, and select **OK**.

Note:

Changing hostname is optional.

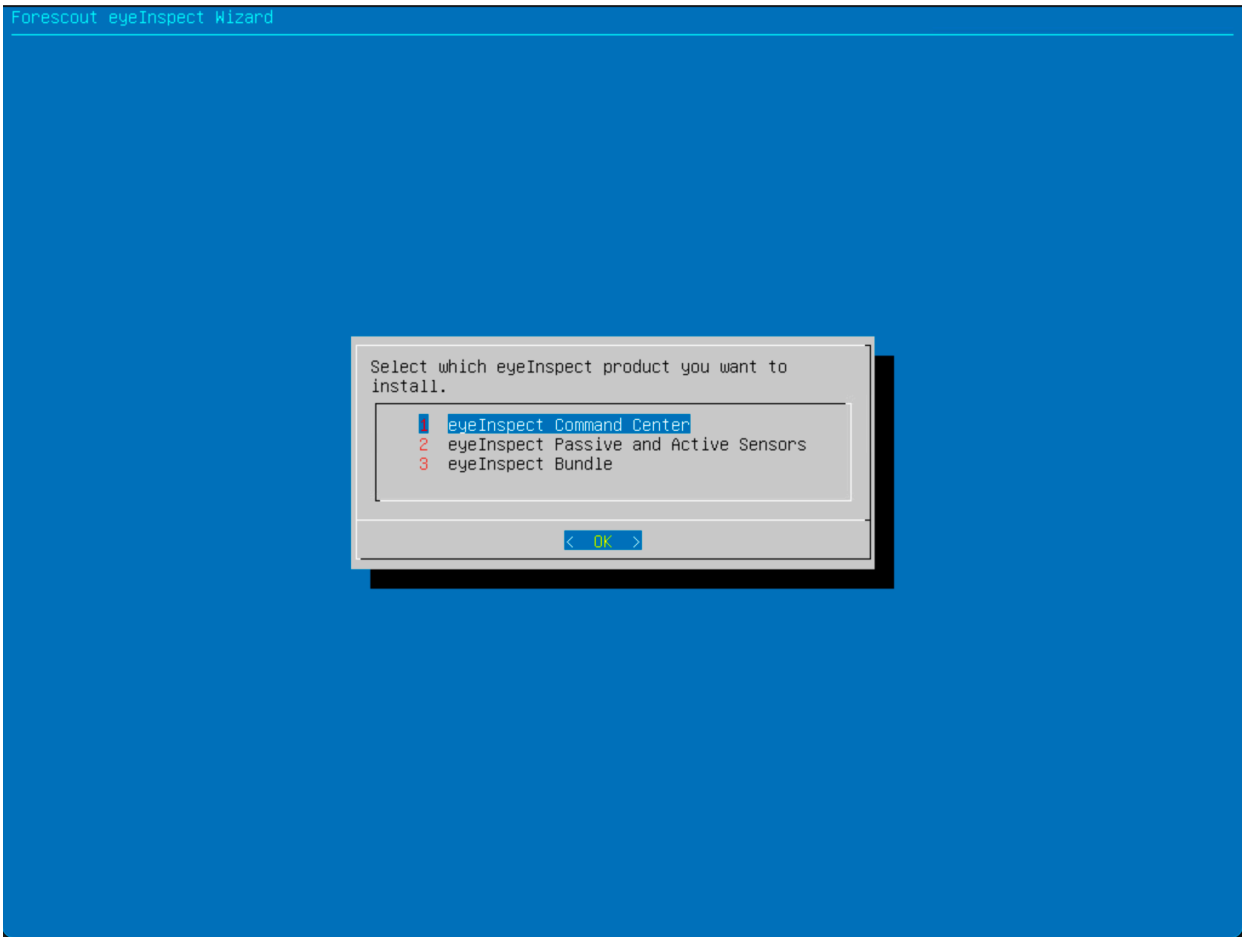
Note:

The hostname should not contain underscores (_).

The Wizard then proceeds to installation of the eyeInspect components.

Install the eyeInspect Components

The eyeInspect Wizard displays the three installation options available.



The installation process is described in detail in the following pages:

- Install the eyeInspect Command Center
- Install the eyeInspect Passive and Active Sensors
- Install the eyeInspect Bundle

Install the eyeInspect Command Center

To install the Command Center and Flow Aggregator Forwarder, do the following:

1. Select the first option eyeInspect Command Center and click OK. The installation begins, and a dialog with the installation in-progress message is displayed.
2. Upon completion, an installation successful message is displayed. Select OK to close the wizard and open the terminal.
3. Check if the system timezone is correct by running the following command:

   ```
   ~$ date
   ```

   If the timezone is wrong, set it to the correct one by running the following command:

   ```
   ~$ sudo dpkg-reconfigure tzdata
   ```

4. Reboot the system by running the following command:

```
~$ sudo reboot
```

5. If you want the Command Center to communicate with the Passive Sensor via a port different than the default 29999, perform the following steps:
   a. Edit the **/etc/iptables/rules.v4** file by issuing the following command:

```
sudo nano /etc/iptables/rules.v4
```

   b. Add the following rule:

```
sudo iptables -I INPUT -p tcp -m tcp --dport <CUSTOM PORT> -j
ACCEPT
```

   c. Restart the firewall service by issuing the following command:

```
sudo systemctl restart netfilter-persistent
```

6. After the installation is complete, it is recommended to check if there is any eyeInspect OS update available, and if yes, to apply the update.

Prevent assets from disappearing

Note:
Perform these steps after you have successfully set up the Command Center by following the Getting Started section of the eyeInspect v5.5.0 User Guide.

To prevent a known issue of **disappearing assets**, caused by the order of updating their information, perform the following steps:

1. Log in to the Command Center.
2. Navigate to Settings > System settings > Activity scheduling.
3. Open the scheduled activity of type Host cleanup.
4. Increase the Retention period (days) to 45.
5. Click Finish.
6. Log in the Command Center via SSH.
7. Open the **/opt/sdconsole/conf/application.properties** file in a command line editor of your choice.
   Note:
   Create this file if it does not already exist.
8. Set the following values:

```
sdcc.cronjob.maxFetchHosts=20000
sdcc.cronjob.maxFetchLinks=100000
```

9. If your network does not support dynamic IP assignment via a DHCP server, set also the following value:

```
sdcc.dhcp.cleanup=false
```

10. Save the changes and close the editor.
11. Restart the Command Center by running the following command:

```
sudo supervisorctl restart silentdefense-cc
```

Install the eyeInspect Passive and Active Sensors

To install the passive and active sensors, do the following:

1. Select the second option eyeInspect Passive and Active Sensors and select OK
2. The Passive Sensor installation begins, and a dialog box with the installation in-progress message is displayed.
3. Once the Passive Sensor installation is complete, the Active Sensor installation begins automatically, and a dialog box with an in-progress message is displayed.
4. Upon completion, you will see an installation successful message. Select OK to close the wizard and open the terminal.
5. Check if the system timezone is correct by running the following command:

   ```
   ~$ date
   ```

   If the timezone is wrong, set it to the correct one by running the following command:

   ```
   ~$ sudo dpkg-reconfigure tzdata
   ```

6. Reboot the system by issuing the following command:

   ```
   sudo reboot
   ```

7. After the installation is complete, Forescout recommends that you check if there is any eyeInspect OS update available, and if yes, to apply the update.

Next Steps for Passive Sensor

After the installation is complete, perform the following steps to finish installing the passive sensor:

1. Log in the Passive Sensor via SSH and export existing sensor configuration via the Nidstool by running the following command:

   ```
   sudo nidstool config export nids_config.yml
   ```

2. Edit the generated `nids_config.yml` file with the required parameters and save the file. The minimum necessary parameters required to start the Passive Sensor container are:
   a. sniff-threads
   b. interfaces
   c. mgmt-address
   d. mgmt-secondary-address (if the Command Center is in High Availability mode)

   For more information, refer to table Startup options for enrolling the Passive Sensor to a Command Center in the section Passive Sensor startup options from the eyeInspect v5.5.0 Configuration Guide.
3. Apply the configuration and start the container by running the following commands:

   ```
   sudo nidstool config apply nids_config.yml --permissive
   ```

```
sudo nidstool up nids-main
```

4. Accept the new Passive Sensor enrollment request. See Adding Passive Sensors (version 5.1.0 or higher) in the eyeInspect v5.5.0 User Guide for more information.

Next Steps for Active Sensor

After the installation is complete, perform the following steps to finish installing the active sensor:

1. Login to the active sensor via SSH and update the /opt/icsp/icsp-sensor/.env file with the following details:
   a. `SENSOR_NAME` - for identification during enrolment (optional)
   b. `ICSP_CC_IP` - IP address of the Command Center (required)
   c. `ICSP_CC_IP_SECONDARY` - if the Command Center is in High Availability mode (optional)
2. Start the container by running the following command:

```
/opt/icsp/icsp-sensor/manage-containers.sh --up
```

3. Accept the new Active Sensor enrollment request. See Adding Active Sensors to the Command Center in the eyeInspect v5.5.0 User Guide for more information.

Note:
When changing the .env file while the container is running, you must restart the container with the manage-containers.sh script using the `--rm` and `--up` options.

Note:
After accepting the enrollment request, the active sensor may still show as disconnected. Allow a few minutes for the connection and health status to be updated.

After installing the Active Sensor, additional configuration may be required for Windows assets on the sensor's network. For all Windows assets that the operator wants to use Active Sensor to send WMI queries to, make sure that there are user credentials with WMI rights on those assets. Refer to Microsoft's Windows Management Instrumentation documentation for more information.

Connectivity

If Active Sensor is not returning the expected results, check that there are no firewalls or proxies separating the Active Sensor from its target assets.

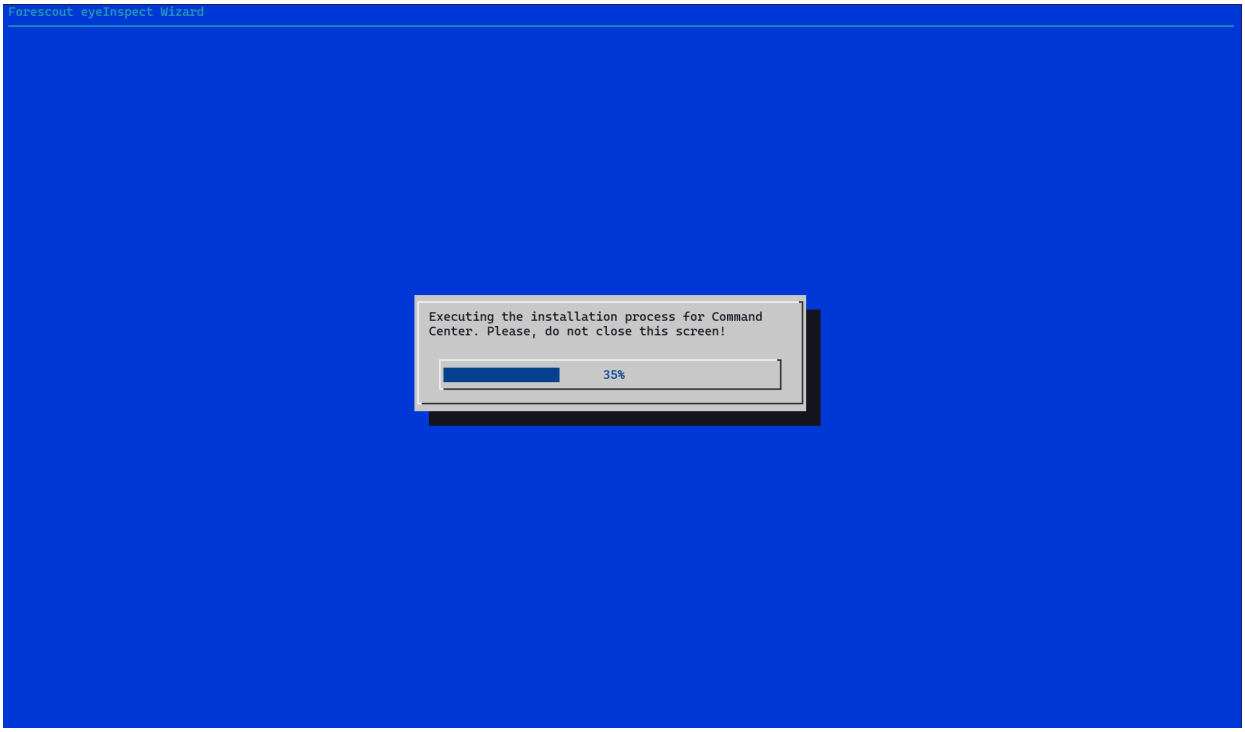
Reserved IP Ranges

The Active Sensor components need access to the target network. As a result, there may be cases where the private IP ranges used for Docker and for the eyeInspect management interface overlap with the target network IP range. In this case, the private IP ranges must be changed. For more information on how to change these private IP ranges, see Adding Active Sensors to the Command Center in the eyeInspect v5.5.0 User Guide.

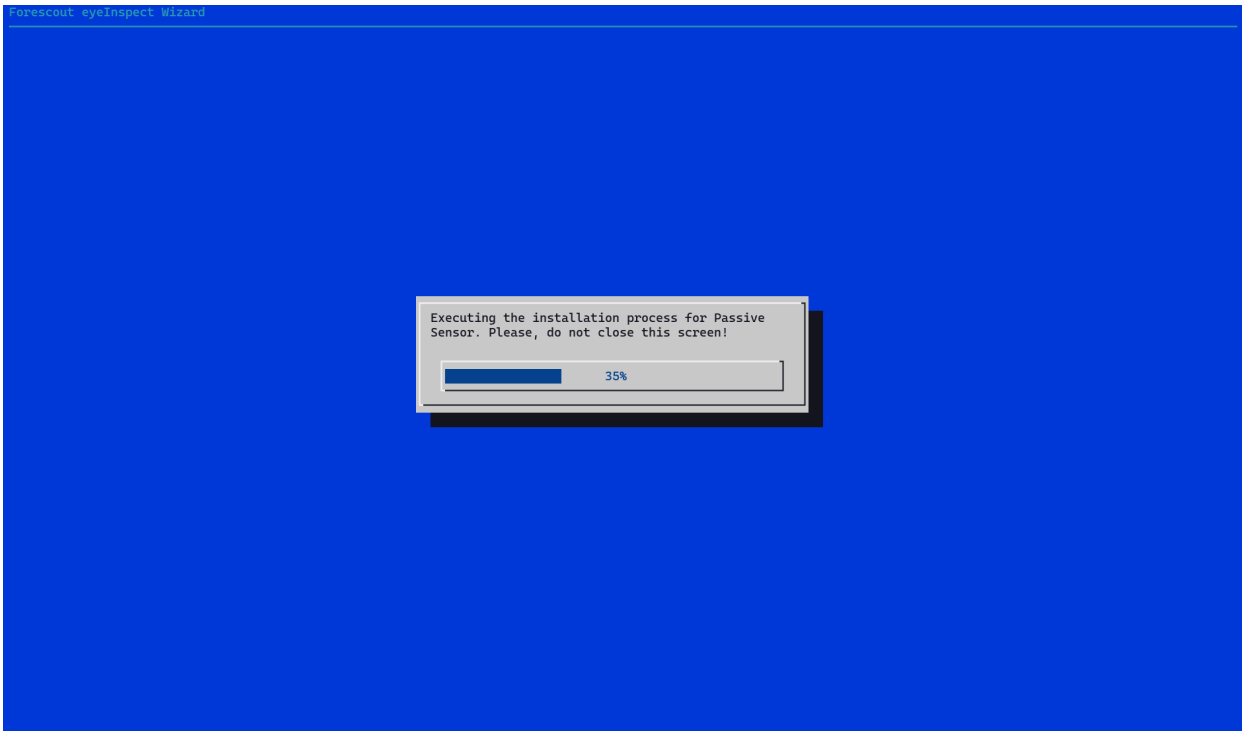
Install the eyeInspect Bundle

To install all the components (Command Center, Flow Aggregator Forwarder, Passive Sensor and Active Sensor) together, select the third option - **eyeInspect Bundle** - and select **OK**.

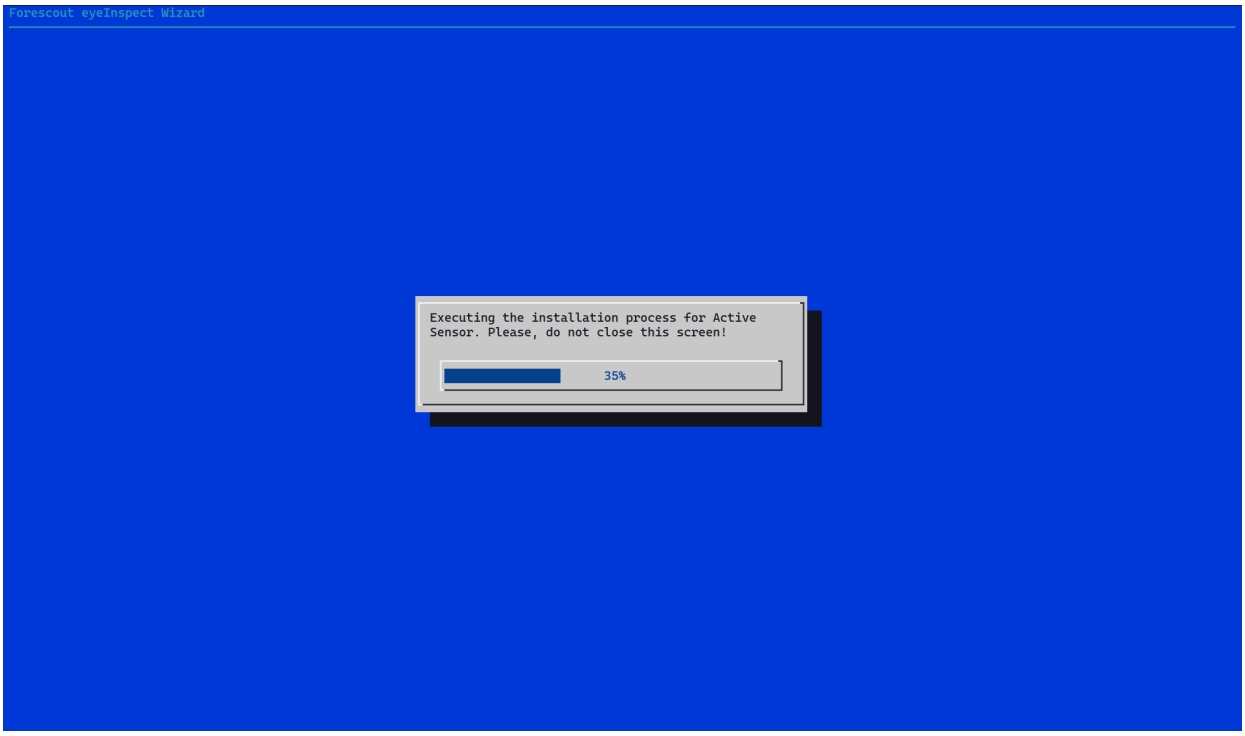
The Command Center installation begins and a dialog with the installation in-progress message is displayed.



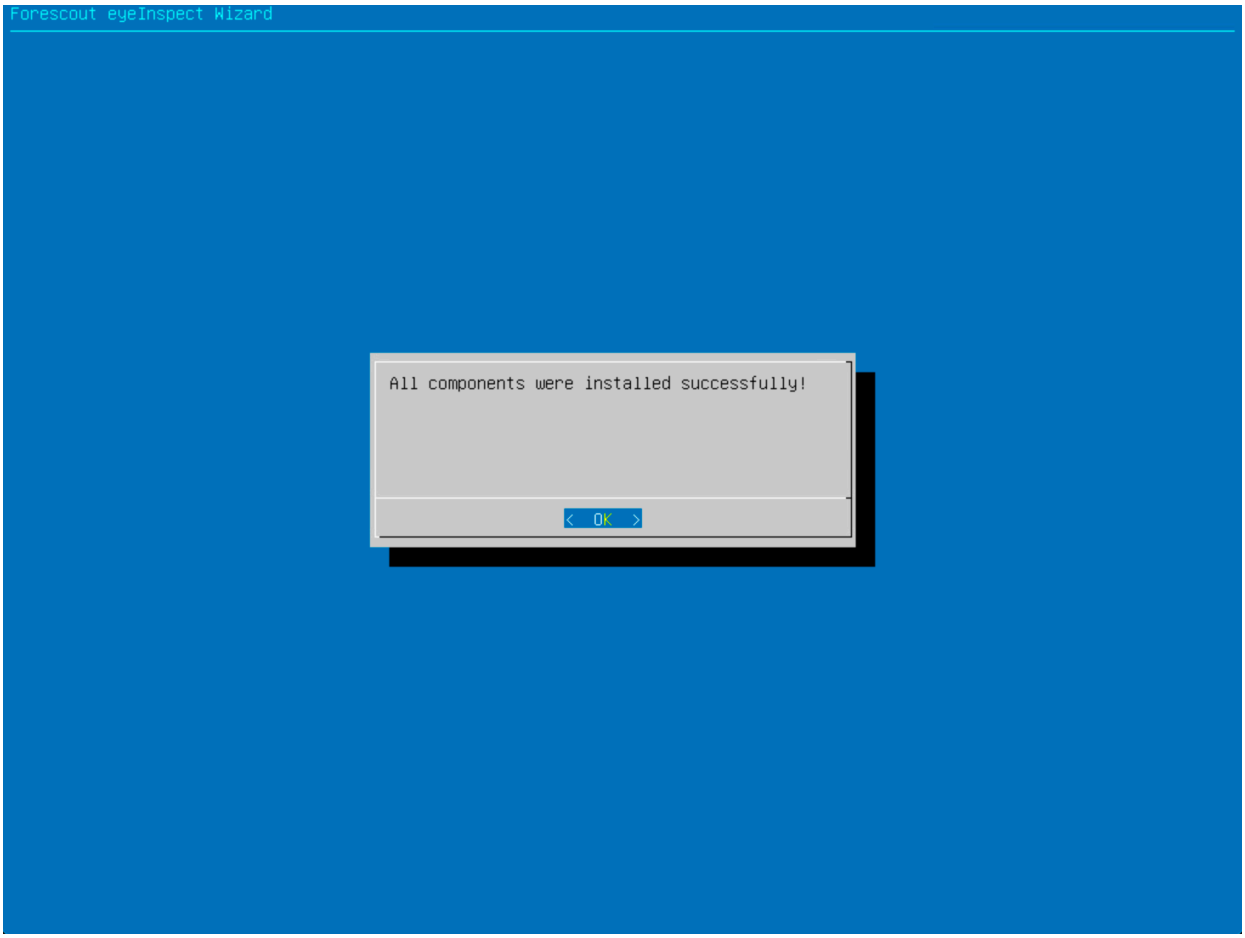
Next, the Passive Sensor installation begins and the appropriate message is displayed.



The last component to be installed is the Active Sensor.



Upon completion, an installation successful message is displayed. Select **OK** to close the wizard and open the terminal.



Next Steps

After the installation is complete, do the following :

- For the Command Center - follow from Step 3
- For the Passive Sensor - go here
- For the Active Sensor - go here

Virtual Appliance Deployments

All eyeInspect deployments as Virtual Appliance are intended for use with VMWare ESXi hypervisors version 5 or above. For labs and demo purposes, eyeInspect may also be provided for use with VirtualBox. For Passive Sensor deployments, the virtual network interface of the Passive Sensor may be attached to:

- A VMDirectPath I/O passthrough: This configuration is required when the traffic to be monitored enters the hypervisor from a physical network interface on the hypervisor server (e.g. traffic mirrored from a physical network); this configuration bypasses the virtual switch and requires a physical NIC to be exclusively dedicated to the virtual machine running the Passive Sensor .

- A virtual-only virtual switch (i.e. not attached to any physical network interface): This configuration is supported only when all monitored traffic originates within the hypervisor network, and no traffic comes from the physical network interfaces. Details for the former configuration can be found on the VMWare website1.