



ForeScout®

Operational Technology Module

Configuration Guide

Version 1.3.1



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-07-06 18:05

Table of Contents

Supporting Operational Technology Endpoints in Forescout.....	5
Components	5
About This Guide	6
What to Do	6
New Deployment of OT Support	7
Integrate OT Support with an Existing SilentDefense Deployment	7
Install and Configure Command Centers	8
Install Command Center on a Hardware Server	8
Requirements	8
Installation	8
Install Command Center on a Virtual Machine	10
Requirements	10
Installation	11
Configure Command Center	12
Apply Security Updates	13
Initial Configuration in the Command Center Console	14
Install and Configure the Operational Technology Module	18
Requirements	18
Install the Module	18
Configure the Module	19
Configure OT Module Connections to Command Center	20
Initial Certificates Setup	22
Map IP Reuse Domains to Command Center	23
Manage Traffic Inspection Scripts	24
Install and Configure OT Sensors	25
OT Sensor Requirements	25
Activate Integrated OT Sensors	26
Install and Configure Standalone OT Sensors	28
Install a Standalone OT Sensor	28
Configure a Standalone OT Sensor	29
eyeSegment Support	30
Update the OT Vulnerability Database	31
Managing Operational Technology Endpoints in Forescout	33
Passive Management of Sensitive Endpoints	33
Overlapping IP Addresses	33
Nested Devices	34
Work with Endpoint Information	35

Appendix 1: Install the Ubuntu OS on Standalone OT Sensors	38
Additional ForeScout Documentation	54
Documentation Downloads	54
Documentation Portal	55
ForeScout Help Tools.....	55

Supporting Operational Technology Endpoints in Forescout

As IT (Information Technology) and OT (Operational Technology) networks converge, a new range of challenging operational cyber risks emerges.

The solution described in this document extends Forescout's visibility and control solution to include OT networks and industrial environments. Passive network monitoring and protocol analysis components combine with the Forescout visibility platform to enable device discovery, classification, and assessment for the full spectrum of IT and OT devices.

Components

Forescout's support for Operational Technology endpoints in Forescout consists of the following components:

- OT Monitoring Sensors

Each OT Monitoring Sensor is connected to the ICS/SCADA network via one or more SPAN/mirroring ports to passively audit the network traffic and detect malicious activities. The detection methods used by OT Sensors are packaged in modules that can be selectively enabled. A dedicated monitoring interface sends events and logs from the OT Sensor to the Command Center.

- Command Centers

Each Command Center collects and processes data reported by one or more Sensors, and supports a web interface for OT endpoint event management.

- Command Centers provided with your eyeSight license simplifies Sensor management and reports Sensor information to Forescout.
- When you install the SilentDefense license, additional Command Center functionality is available such as dashboards and analytical tools.

- Operation Technology Module

The Operational Technology Module connects to Command Center instances to integrate events and information gathered from monitored OT endpoints. This information is made available for use in Forescout policies and by endpoint management tools.

- Content Modules provide regularly updated information to enhance detection and handling of Operational Technology endpoints:

- The Operational Technology Vulnerability Database provides periodic updates of the vulnerabilities that Command Center can detect on endpoints, based on published CVEs and advisories.
- The Traffic Inspection Library adds protocol parsing capabilities to the Forescout platform. The library provides scripts that enhance traffic inspection by the Operational Technology module and associated SilentDefense components. The library is updated periodically to improve the breadth and precision of inspection.

Implementation Options for Operational Technology Components

A **Command Center** can be deployed in two ways:

- On a physical server, usually a 19" rack server or an embedded PC.
- As a virtual machine on a VMware ESXi hypervisor.

You can deploy an **OT Monitoring Sensor** in two ways:

- As an *Integrated OT Sensor*, hosted on a Forescout Appliance.
- As a *Standalone OT Sensor*, installed on another server or virtual server in the network. This is the preferred method.

About This Guide

This guide tells you how to install and configure components of Forescout's Operational Technology solution.

What to Do

This section provides deployment overviews for the following scenarios:

- [New Deployment of OT Support](#)
- [Integrate OT Support with an Existing SilentDefense Deployment](#)

This guide describes procedures for initial deployment and configuration of Forescout Operational Technology components. To upgrade the Operational Technology Module or existing Command Centers and Sensors after initial deployment, see the Release Notes for detailed procedures and release compatibility information.

Certificate Options for Integration with SilentDefense Deployments

Because SilentDefense can be deployed as a standalone product, it has its own Certificates. When integrating SilentDefense with the Forescout platform, a choice must be made which certificates to use: the Forescout signed certificates, or the SilentDefense certificates. The preferred choice is to use the Forescout signed certificates. The installation procedures in this document will provide information on how this is done.

If there are reasons why the SilentDefense certificates must not be overwritten, it is possible to import SilentDefense certificates into the Operational Technology module instead. For information on importing certificates, please refer to the Forescout Administration Guide, Appendix B: "Configuring the Certificate Interface".

New Deployment of OT Support

[Install and Configure Command Center](#)

Overwrite the SilentDefense internal certificates with the Forescout Signed certificates generated by the Operational Technology module.

[Install and Configure the Operational Technology Module](#)

During configuration, you define a focal Appliance that connects with Command Center.

To work with standalone OT Sensors:

[Install and Configure Standalone OT Sensors](#)

[Install and Configure Standalone OT Sensors](#)

[Initial Certificates Setup](#)

To work with integrated OT Sensors:

[Activate Integrated OT Sensors](#)

[Configure Management Connections to OT Sensors](#)

[Work with Endpoint Information](#)

[Update the OT Vulnerability Database](#)

To use advanced Command Center features:

[Install or Upgrade Your License](#)

Integrate OT Support with an Existing SilentDefense Deployment

In this scenario, Forescout connects to a Command Center instance that is part of an existing SilentDefense deployment.

Upgrade existing SilentDefense deployment to a version supported by the Operational Technology module. Refer to the SilentDefense documentation for the update procedure.

[Install and Configure the Operational Technology Module](#)

During configuration, you define a focal Appliance that connects with Command Center.

Important: For deployments where the existing certificates must not be overwritten, please refer to Appendix B of the Forescout Administration Guide for information on how to import SilentDefense certificates into the Operational Technology Module.

[Work with Endpoint Information](#)

[Update the OT Vulnerability Database](#)

To use advanced Command Center features:

[Install or Upgrade Your License](#)

Install and Configure Command Centers

This section describes how to install a Command Center instance and define the Sensors that it manages. The Operational Technology Module can be connected to multiple Command Center instances. As such, this procedure may be repeated to install multiple Command Center instances.

To support assignment to a managing Appliance, each Command Center server must use an IP address within the scope of ForeScout's *internal network* definitions. See the *Forescout Administration Guide* for more information about the internal network.

Install Command Center on a Hardware Server

Requirements

This section lists required components to install Command Center.

Server Requirements

Refer to the following page for OT component server hardware requirements:

<https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/>

The machine on which the Command Center is installed must be running Ubuntu Server 16.04.6 LTS 64-bit (AMD64 or EM64T architecture). Refer to [Appendix 1: Install the Ubuntu OS](#).

Forescout Requirements

CounterAct 8.2.1 including Operational Technology Module version 1.3.1, and SilentDefense version 4.1.1 or 4.1.2.

For CounterAct 8.2.0 versions, please use the Operational Technology module version 1.3.0 instead.

eyeSegment Requirements

Integration of OT for eyeSegment is optional. To enable eyeSegment support, required versions are CounterAct 8.2.1 and SilentDefense 4.1.2.

Installation

- 📄 *In addition to the files in the installer package, you will need a new license file for this product release.*
- 📄 *Run script files in the order specified in this procedure.*
- 📄 *To submit sudo commands, provide your root password when prompted.*

To install OT Command Sensor on a Hardware Server:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**To identify your licensing mode, select **Help > About ForeScout** from the Console.
2. Download and unpack the installation package.
3. Copy unpacked files to the server using suitable protocols such as scp/sftp for Linux machines, or pscp/winscp for Windows machines.
 - On Linux machines, use a command similar to the following:
`scp <file_name> silentdefense@<server_IP>:~/`
 - On Windows machines, use an SSH tool with a command such as the following:
`pscp.exe <file_name> silentdefense@<server_IP>:`where `<file_name>` specifies one or more of the installation files, and `<server_IP>` is the hostname or IP address of the management interface of the server.
4. Open an SSH session to the machine and log in as the silentdefense root user you defined in Ubuntu.
5. Verify the files are all on the server by issuing the following command to list the contents of the current directory:
`ls -alh`
6. Mark the executable files by running the following command:
`chmod a+x *.run`
7. Use a command like `sudo ./ <filename>` to run the update installer `update_os....run` provided in the installation package. The script updates core operating system packages to the versions available at the specified date.
8. Run the main configuration installer `main_configuration....run` provided in the installation package.
9. After the main configuration installer finishes successfully, reboot the system:
`sudo reboot`
Log in as the silentdefense root user you defined in Ubuntu.
10. Start the Command Center installer
`commandcenter_<version>_install_withdeps....run` provided in the installation package.
 - The installer prompts you to choose which product to install. Select Command Center.
 - If more than 4GB memory is available, the installer prompts you to configure memory. Press Enter to accept default settings.

After installation, [Configure Command Center](#).

Install Command Center on a Virtual Machine

Requirements

This section lists required components to install Command Center.

Forescout Requirements

CounterAct 8.2.1 including Operational Technology Module version 1.3.1, and SilentDefense version 4.1.1 or 4.1.2.

For CounterAct 8.2.0 versions, please use the Operational Technology module version 1.3.0 instead.

Integration of OT for eyeSegment is optional. To enable eyeSegment support, required versions are CounterAct 8.2.1 and SilentDefense 4.1.2.

VMware Requirements and Support

The Command Center is distributed as an OVA machine image for installation on a virtual server. Forescout virtual systems are supported on the following VMware versions:

- VMware ESXi v6.5
- VMware ESXi v6.0
- VMware ESXi v5.5
- VMware ESXi v5.1

The guest OS is defined as *Other Linux-2.6 64bit kernel*.

Virtual Machine Network Requirements

NTP traffic must reach the Command Center.

Command Center can use the following protocols if desired. See SilentDefense documentation for details.

- DNS access
- LDAP access
- SMTP access (for alert forwarding)
- Syslog access (for alert forwarding)

Configure the firewall rules listed in the following table.

Source	Destination	Destination Port	Description
Command Center	Sensor(s)	TCP 22 (ssh) TCP 9092 (Kafka) TCP 9999 (*)	System management. EyeSegment and CC Analytics. Event communication.
Forescout Connecting Appliance	Command Center	TCP 9092 (Kafka) TCP 8444 TCP 443 (https) TCP 22 (ssh)	EyeSegment support. SilentDefense updates. Data communication. System management.

📄 (*) *configurable, see SilentDefense documentation*

Installation

Follow this procedure to install Command Center on a virtual machine. To configure this Command Center, the default user `silentdefense` is provided. Obtain the password for this user account from your Forescout representative.

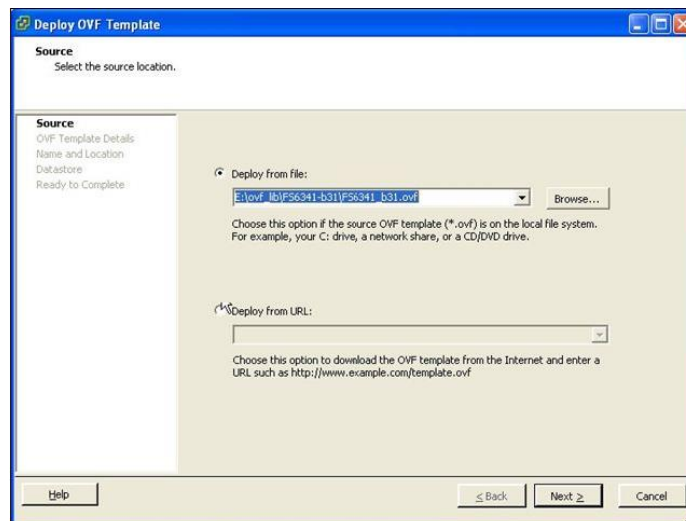
To install a Command Center virtual device:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the Command Center (Virtual) .OVA file.
3. Access the vSphere Console.
4. Select **File>Deploy from file (OVF template)**.

The Deploy OVF Template wizard opens at the Source page.




5. Select the Command Center .OVA virtual system package and then select **Next**. The OVF Template Details page opens.
6. Select **Next**. The Name and Location page opens.
7. Specify a name and then select **Next**. The Datastore page opens.
8. Define the location where you want to store the virtual machine file (you need at least 1.5 GB free space) and then select **Next**. The Network Mapping page opens.
9. Map the virtual interface and then select **Next**. The Ready to Complete page opens.

10. Select **Finish** to deploy the virtual device.

After installation, [Configure Command Center](#).

Configure Command Center

After installation, follow the procedures in this chapter to configure the Command Center instance.

 *To configure Command Center on a virtual machine, the default user **silentdefense** is provided. Obtain the password for this user account from your Forescout representative.*

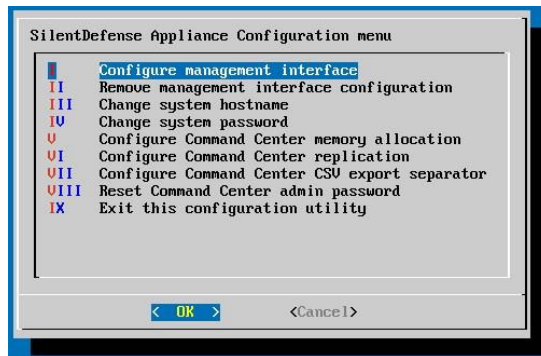
To configure a Command Center instance:

1. Power on the Command Center server or virtual machine.
2. Log in to the Command Center using SSH, or through a hypervisor client.
 - For a hardware server, use the silentdefense root user you defined in Ubuntu.
 - For a virtual machine, use the default username: **silentdefense** and its password.
3. Enter the following command:

```
sudo sdconfig
```

When prompted, re-enter the default password.

The SilentDefense Appliance Configuration main menu appears.



The following table describes the configuration options that are available.

Feature	Description	Required
Configure management interface	Configure the IP address, gateway, and DNS server of this Command Center that is used for communication with Forescout and with Sensors.	Required
Remove management interface configuration	Remove the configured management network interface from the network interface configuration file in the Linux Operating System.	Optional

Feature	Description	Required
Change system hostname	Change the hostname used to identify the server. This is also the username used to access the Sensor operating system. To complete this action, reboot the system (<code>sudo reboot</code>) and log in as the silentdefense root user.	Optional
Change system password	Change the password used to log in to the Command Center operating system.	Recommended
Configure Command Center memory allocation	Modify default memory allocation for Command Center processes on the server. For details, refer to the SilentDefense documentation suite.	Optional
Configure Command Center replication	Configure warm mirroring between two Command Center instances. For details, refer to the SilentDefense documentation suite.	Optional
Configure Command Center CSV export separator	Define the character used as a value separator in CSV files.	Optional
Reset Command Center admin password	Reset the admin password of the Command Center to the default value.	Optional

4. Select **Configure management interface** and define address and gateway settings for Command Center. Record the values you enter in this interaction. You must enter these values when you define this Command Center instance in Forescout.
5. Next steps:
 - [Initial Configuration in the Command Center Console](#)
 - Define the connection between a Forescout device and this Command Center instance. Refer to [Configure the Module](#).
 - [Update the OT Vulnerability Database](#)

Apply Security Updates

OTSEC security updates for SilentDefense are made available when vulnerabilities are found that affect the Ubuntu operating system and packages on standalone SilentDefense servers. If security updates are available for the SilentDefense version that has been installed, apply them on all OT Command Center and standalone OT Sensor servers. For integrated OT Sensors, this step can be skipped.

1. OTSEC updates follow the naming convention OTSEC-YEAR_NUMBER, for example "OTSEC-2020-002".
2. Copy the .run file to the SilentDefense server.

3. Ensure the file is executable, for example:
`sudo chmod u+x OTSEC-2020-002.run`
4. Execute the .run file:
`./OTSEC-2020-002.run`
5. Reboot the server.

Initial Configuration in the Command Center Console

This section describes initial configuration procedures that you perform after you log in to the Command Center console for the first time.

To log in to the Command Center Console:

1. Enter the following command to navigate to the Command Center console:

```
https://<CC_IP>/login
```

where <CC_IP> is the IP address of the virtual machine that hosts the Command Center.

2. The Login screen appears. Log in using the following default credentials:

Username: **admin**

Password: **admin**



Upon log in you are prompted to change the password. Record the new credentials and use them when you define this Command Center in the Operational Technology Module.

Continue with the following configuration procedures:

- [Install or Upgrade Your License](#)
- [Define Date and Time Settings](#)
- [Configure Management Connections to OT Sensors](#)

Install or Upgrade Your License

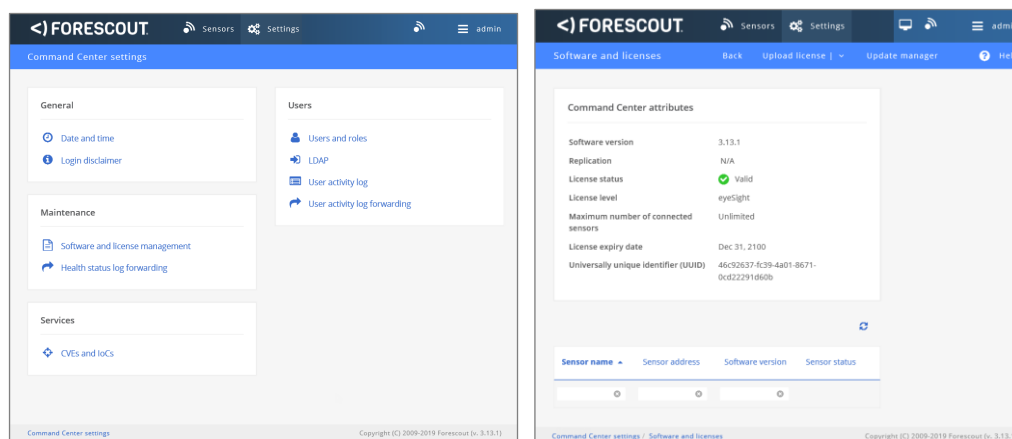
Use this procedure to install a license on Command Center.

-  *When you deploy Command Center on a virtual machine, skip this procedure. The .OVA installer file includes an eyeSight license.*
-  *Upgrade from a standard eyeSight license to a SilentDefense license to access additional Command Center dashboards and other functionality. Obtain a SilentDefense license from your Forescout representative.*

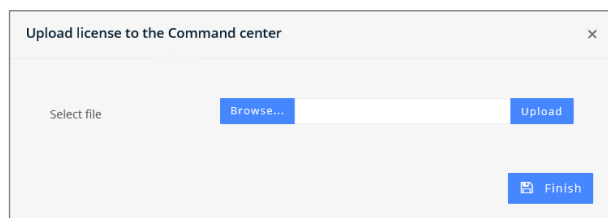
To install a license on Command Center:

1. Open a browser and navigate to the server that hosts the Command Center you want to update.
2. The Login screen appears. Log in using admin-level credentials.

The Command Center settings page appears. In the Maintenance area, select **Software and license management**. The Software and licenses page appears.



3. In the toolbar, select **Upload license > To Command Center**. The Upload license to the Command Center dialog appears.



- a. Browse to the license file.
- b. Select **Upload**.

The license is installed.

4. Select **Finish**.

Define Date and Time Settings

The Command Center must use the same NTP server as Forescout. In addition, the date and time of the Command Center should be keyed to the Connecting CounterACT device.

To define date and time settings:

1. In the Forescout Console:
 - a. Select **Options** in the toolbar.
 - b. In the CounterACT Devices pane, select the Connecting CounterACT device and note NTP and time zone information. Also note NTP server and time zone information in these locations:
General > Time
Console Preferences > Time Zone
2. Log in to the Command Center console. In the top-level menu bar, select **Settings**.
3. In the General area, select **Date and Time**.

The screenshot shows the Forescout Settings interface. At the top, there's a navigation bar with 'Sensors' and 'Settings' tabs. Below it, a blue header bar contains 'Date and time', 'Back', 'Finish', and 'Set manually' buttons. The main content area is divided into sections. The first section, 'Current date and time', includes a 'Time zone' dropdown menu set to 'America/New_York', and input fields for 'Date' (Thu 06 Jun 2019) and 'Time' (06:18:13). The second section has a checkbox labeled 'Enable NTP synchronization' which is checked. The third section, 'NTP servers', shows '0 servers selected' with a plus icon to add more. Below this is a table with the header 'Server name' and two entries: '192.168.1.1' and '192.168.1.2'. At the bottom of the table, it says '2 servers'.

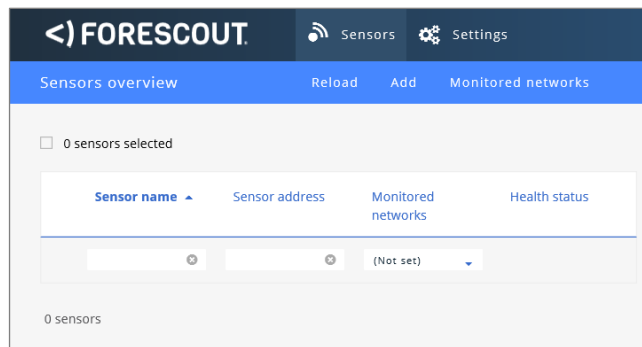
4. Select **Enable NTP synchronization**.
5. In the NTP servers area, select the plus **+** icon. Enter the address of the NTP server used by Forescout. Select **Apply**. The server appears in the list.
6. In the Current date and time area, define values that coordinate with the Connecting CounterACT device.

Configure Management Connections to OT Sensors

This section describes how to define management interfaces between the Command Center and the Sensors it controls. The Sensors must already be installed and running before you perform this procedure. Refer to [Install and Configure OT Sensors](#) for details of OT Sensor installation.

To define a monitoring interface to an OT Sensor:

1. Log in to the Command Center console. In the top-level menu bar, select **Sensors**.
2. The Sensors overview page appears.



3. Select **Add > SilentDefense sensor**. The Add new sensor dialog appears.

4. In the **Policy** field, select *import sensor configuration*. Complete the following fields to identify a Sensor:

Sensor name	A label that identifies the Sensor
Sensor Address	The IP address of the machine hosting the Sensor
Port	The port configured for monitoring on this Sensor

5. Select **Finish**. The Command Center connects to the Sensor and establishes a monitoring interface. This Sensor now reports data to this Command Center.
6. Repeat this procedure to assign other Sensors to the Command Center.

Install and Configure the Operational Technology Module

This section describes how to install the Operational Technology Module in Forescout, and how to configure Sensors and Command Center instances that report OT endpoint information to Forescout.

Requirements

CounterAct 8.2.1 including Operational Technology Module version 1.3.1, and SilentDefense version 4.1.1 or 4.1.2.

For CounterAct 8.2.0 versions, please use the Operational Technology module version 1.3.0 instead.

Integration of OT for eyeSegment is optional. To enable eyeSegment support, required versions are CounterAct 8.2.1 and SilentDefense 4.1.2.


Install the Module


To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**


To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module `.fpi` file. Save the file to the machine where the Console is installed.
3. Log into the Console and select **Options** from the **Tools** menu.
4. Select **Modules**. The Modules pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved module `.fpi` file.
7. Select **Install**. The Installation screen opens.
8. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

 *The installation begins immediately after selecting Install and cannot be interrupted or canceled.*

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

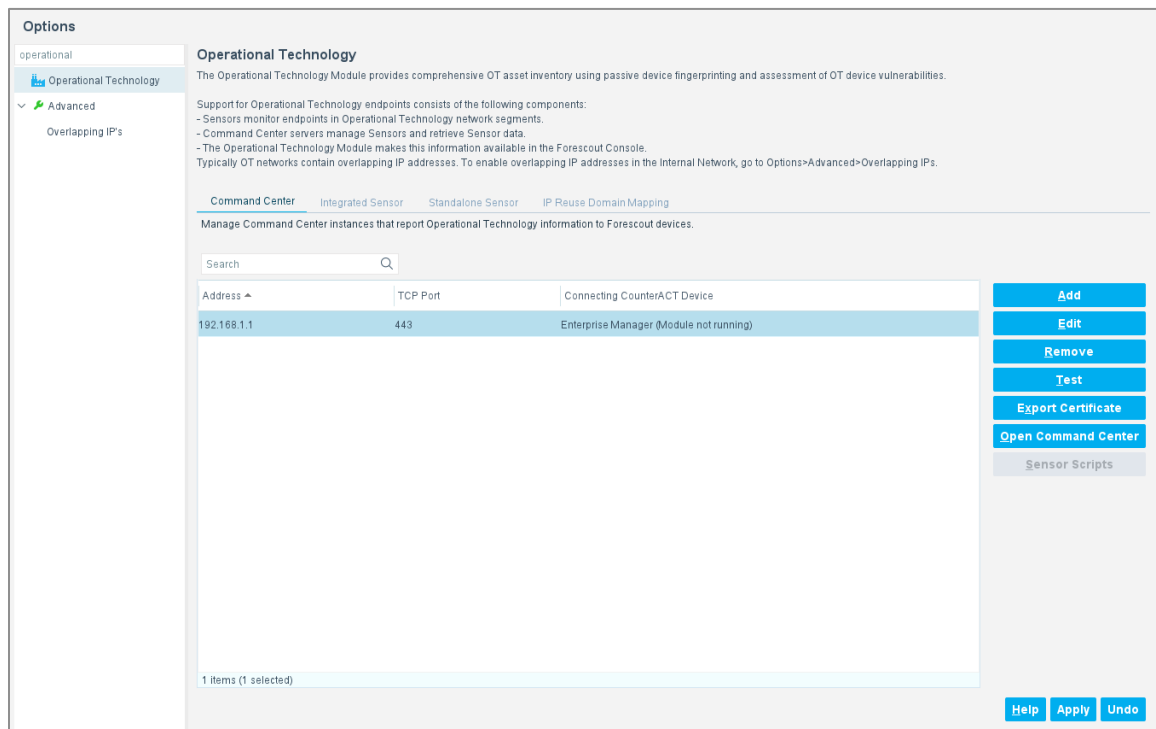
9. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

 *Some components are not automatically started following installation.*

Configure the Module

In the Console, select **Options > Operational Technology** to go to the module configuration pane. Use this pane to perform the following configuration and maintenance tasks:

- Select the Command Center tab to [Configure OT Module Connections to Command Center](#) and to [Manage Traffic Inspection Scripts](#)
- Select the IP Reuse Domain Mapping tab to [Configure OT Module Connections to Command Center](#)
- [Map IP Reuse Domains to Command Center](#)
- Select the Integrated Sensor tab to [Activate Integrated OT Sensors](#)
- Select the Standalone Sensor tab to export certificates used when you [Install and Configure Standalone OT Sensors](#)



Options

- operational
- Operational Technology**
- Advanced
 - Overlapping IP's

Operational Technology

The Operational Technology Module provides comprehensive OT asset inventory using passive device fingerprinting and assessment of OT device vulnerabilities.

Support for Operational Technology endpoints consists of the following components:

- Sensors monitor endpoints in Operational Technology network segments.
- Command Center servers manage Sensors and retrieve Sensor data.
- The Operational Technology Module makes this information available in the Forescout Console.

Typically OT networks contain overlapping IP addresses. To enable overlapping IP addresses in the Internal Network, go to Options>Advanced>Overlapping IP's.

Command Center | Integrated Sensor | Standalone Sensor | IP Reuse Domain Mapping

Manage Command Center instances that report Operational Technology information to Forescout devices.

Search

Address	TCP Port	Connecting CounterACT Device
192.168.1.1	443	Enterprise Manager (Module not running)

1 items (1 selected)

Add
Edit
Remove
Test
Export Certificate
Open Command Center
Sensor Scripts

Help **Apply** **Undo**


Configure OT Module Connections to Command Center

Use this procedure to define connections between ForeScout Appliances and Command Center instances in the environment.

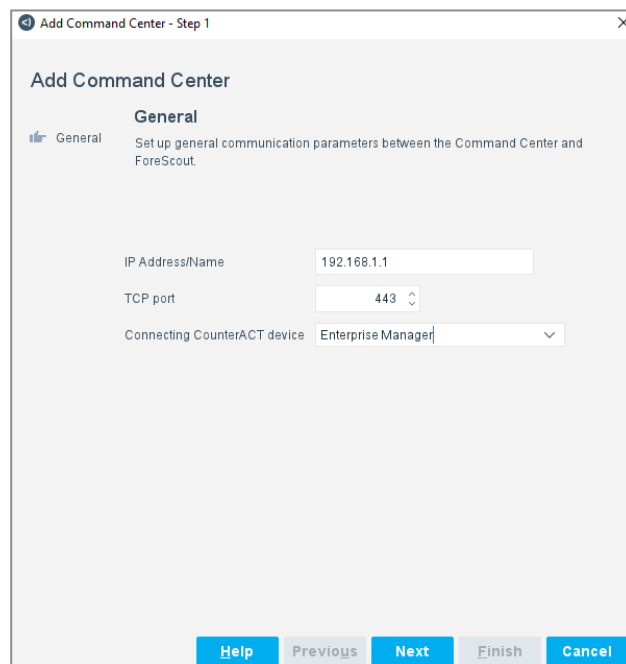
 *In this release, you can only define a single Command Center instance.*

To configure the module:

1. Verify that a user account and SSH credentials for use by the Operational Technology Module are defined on the Command Center. Note this information for use during installation.

 *If you are integrating Forescout with an existing SilentDefense deployment, import public certificate information from an existing Command Center into Forescout:*
-Access the Command Center, and copy the public certificate shown in the browser.
-Import the certificate into Forescout with the Operational Technology Module in the scope of the certificate. For details, see Appendix B, "Configuring the Certificate Interface" in the Forescout Administration Guide.

2. In the ForeScout Console, select **Options > Operational Technology**.
3. In the Command Center tab, do one of the following:
 - To define a new connection select **Add**
 - To modify an existing connection, select it from the list. Double-click or select **Edit**.
4. In the General tab of the Add/Edit dialog, specify the following information.



Add Command Center - Step 1

Add Command Center

General
Set up general communication parameters between the Command Center and ForeScout.

IP Address/Name: 192.168.1.1

TCP port: 443

Connecting CounterACT device: Enterprise Manager

Buttons: Help, Previous, Next, Finish, Cancel

IP/Name	The hostname or IP address of the Command Center instance
TCP Port	The port that Forescout connects to on the Command Center machine
Connecting CounterACT device	The hostname or IP of the Connecting CounterACT device <ul style="list-style-type: none"> Do not select a device that runs an integrated OT Sensor.

5. In the Command Center Credentials tab, specify the following information.

Add Command Center - Step 2 of 2

Add Command Center

☒ General
☐ Command Center Credentials

Command Center Credentials
Enter access credentials to the Command Center.

Credentials

User name: admin

Password: [masked]

Confirm password: [masked]

User Name	Specify the account Forescout uses to query the Command Center and retrieve endpoint data. You defined this user when you first logged in to the Command Center web service.
Password	
Confirm Password	

6. Select **Finish**. The Command Center instance appears in the table.
7. Set up the Command Center Certificates. See the section [Initial Certificates Setup](#) below.

Initial Certificates Setup

Before the Operational Technology Module, OT Command Center, and the OT Monitoring Sensor can communicate, the certificates used by these systems must be updated. The advised way of doing so is by using the certificates generated by the Operational Technology Module for this purpose.

Important: The following procedure overwrites the existing SilentDefense certificates with Forescout signed licenses from the Operational Technology module. For cases where the existing SilentDefense licenses must not be overwritten, skip these steps and import the SilentDefense license into the Operational Technology module instead. For information on how to import certificates, please refer to the Forescout Administration Guide, Appendix B: "Configuring the Certificate Interface".

1. For each Command Center instance, open the Command Center options by selecting that Command Center and pressing Edit.
 - a. Open the tab "Certificates Issues".

The screenshot shows a dialog box titled "Edit Command Center" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "General", "Command Center Credentials", and "Certificates Issue". The "Certificates Issue" tab is selected and active. The content of the tab includes a "Please note" section stating that the configuration is optional and could cause an outage. It also states that completing this configuration will cause sensors in the Command Center to disconnect, and that this option is not recommended for integration with an existing SilentDefense deployment. A warning icon (yellow triangle) is shown next to the text "Your certificates on the Command Center will be overwritten". Below this, there is a section titled "Overwrite Certificates" with a checked checkbox labeled "Overwrite certificates and restart Command Center". Underneath, there are three input fields: "SSH User name" (containing "silentdefense"), "SSH Password" (masked with asterisks), and "Confirm password" (masked with asterisks). At the bottom right of the dialog, there are three buttons: "Help", "OK", and "Cancel".

- b. Because certificates have not yet been set up, warnings will be shown. This is normal.
 - c. Check the "Overwrite certificates and restart Command Center" checkbox.
 - d. Enter the Command Center server credentials for SSH and press OK.
 - e. In the Options pane, select **Modules**. Select the Operational Technology module, and then select **Start**.

2. For each Standalone Sensor, the certificates must be applied on the server manually.
 - a. Retrieve the certificates files by exporting them from the Operational Technology module options. Open the "Standalone Sensor" tab and click "Export Certificate" to download the certificate files.
 - b. Extract the certificate files from the downloaded ZIP files, and copy them to the OT Monitoring Sensor server, for example through SCP.
 - c. Connect to the OT Monitoring Sensor server as the silentdefense user through SSH.
 - d. Copy the files to the following location on the Sensor:
`/opt/nids/cert/`
 - e. Restart the Sensor service with the following command:
`sudo supervisorctl restart nids`

Map IP Reuse Domains to Command Center

Networks in plant/production, building automation, and other Operational Technology environments often contain duplicate sites and network structures. IP addresses repeat, or *overlap*, across the network.

To support these networks, the Forescout platform and the SilentDefense solution use *IP Reuse Domains* to distinguish several instances of an overlapping IP address. You define a unique IP Reuse Domain for each repeated segment or network branch. IP addresses are unique in each IP Reuse Domain.

- In the Forescout platform, IP Reuse Domains are assigned to Appliances. Identical segments are distinguished from each other by the IP Reuse Domain of the Appliance that manages each segment.
- In SilentDefense, IP Reuse Domains are defined in the Command Center Console and assigned to selected Sensors.

After you [Configure OT Module Connections to Command Center](#), you must correlate the IP Reuse Domains defined in the two platforms.

- For information about support for overlapping IPs in the Forescout platform, see the *Working with Overlapping IPs How-to Guide*.
- For details of IP Reuse Domains in SilentDefense, see the *SilentDefense Installation and Configuration Guide*.

Use this procedure to map the IP Reuse Domains defined in the Forescout platform to the IP Reuse Domains defined in SilentDefense. Repeat this procedure when you change IP Reuse Domain definitions in either platform.

To map IP Reuse Domains to Command Center:

1. To review IP Reuse Domains defined in the Forescout platform, go to **Options > CounterACT Devices > Overlapping IPs Management** in the Console. The table shows segments in each IP Reuse Domain. Select **Export** to export IP Reuse Domain information.
2. Go to **Options>Operational Technology** and select the *IP Reuse Domain Mapping* tab.


3. To define mapping between an IP Reuse Domain defined in the Forescout Internal Network and IP Reuse Domains defined in the SilentDefense Command Center:
 - a. Select **Add** or select an existing rule and select **Edit**.
 - b. In the **Internal Network IP Reuse Domain** drop-down, select an IP Reuse Domain.
 - c. In the **Command Center IP Reuse Domains** drop-down, select an IP Reuse Domain. Domains are shown for all connected Command Centers.
 - d. Select **OK**.
4. Repeat 1-3 for all mappings you wish to establish. All non-mapped Command Center IP Reuse Domains will default to the Global IP Reuse Domain of Counteract
5. Select **Apply** to save the definitions.

Manage Traffic Inspection Scripts

The Traffic Inspection Library is a content module that adds protocol parsing capabilities to the Forescout platform. The library provides scripts that enhance traffic inspection by the Operational Technology module and associated SilentDefense components. The library is updated periodically to improve the breadth and precision of inspection. It is recommended to install the latest version of the Traffic Inspection Library to take advantage of the most current scripts.

Install or update the Traffic Inspection Library after you [Configure OT Module Connections to Command Center](#).

When you install a new release of the Traffic Inspection Library, updated inspection scripts are distributed to Sensors that run other versions of the scripts. However, some Sensors may be offline during distribution. Use this procedure to update Sensors that were not automatically updated.

 *Only scripts with filenames identical to the files in the Library are updated. If you used the Command Center console to modify a script file, change its file name to protect changes.*

To distribute updated scripts to Sensors:

1. In the Console, open the *Options* window and select **Operational Technology**.
2. In the **Command Center** tab, select one or more Command Centers. You will update scripts on the Sensors controlled by the selected Command Centers.

 *In this release, you can only define a single Command Center instance.*

3. Select **Sensor Scripts**. The *Scripts Status* dialog shows the scripts used by each Sensor of the selected Command Centers.
 - When a Sensor already uses the scripts provided by the installed Traffic Inspection Library, its status is *Up to date*.
 - When a Sensor still uses older Traffic Inspection scripts, its status is *Update required*.

4. Select **Update Scripts** to distribute the most recent Traffic Inspection scripts to all the Sensors that require update. Older scripts are overwritten.

 *Distribution of updated scripts may cause Sensors to restart.*

Install and Configure OT Sensors

OT Sensors monitor Operational Technology endpoints. Each OT Sensor is managed by a Command Center instance.

To support OT monitoring in Forescout, you can deploy OT Sensors in two ways:

- **Integrated OT Sensors** are hosted on a Forescout Appliance. Note that:
 - Integrated OT Sensors must still be managed by a Command Center instance on another server.
 - Integrated OT Sensors do not report PCAP information.
- **Standalone OT Sensors** are installed on a Linux server.

OT Sensor Requirements

This section lists requirements to deploy an OT Sensor.

Hardware Requirements

Refer to the following page for OT component server hardware requirements:

<https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/>

Networking Requirements

Each OT Sensor uses the following network connections:

- SPAN port(s) to monitor the target network segment(s). Define them when you [Configure a Standalone OT Sensor](#) or [Activate Integrated OT Sensors](#).
- Network access to the Command Center that manages this OT Sensor. Typically, the Command Center is in the *Internal Network* seen by Forescout Appliances, and can be accessed by integrated OT Sensors. You define this connection when you [Configure a Standalone OT Sensor](#).

If necessary, configure the following firewall rule to support this connection.

Source	Destination	Dest. Port	Description
Command Center	OT Sensor(s)	22 (ssh) 9999 9092 (Kafka)	System management SilentDefense event communication eyeSegment Support and CC Analytics

Integrated OT Sensor Host Requirements

Integrated OT Sensors are deployed on Forescout Appliances. Refer to the following page for capacity and sizing details of Appliances:

<https://www.forescout.com/company/resources/forescout-licensing-and-sizing-guide/>

Verify that the target Appliance has the resources to support OT Sensor functionality.

Standalone OT Sensor Host Requirements

The machine on which the OT Sensor is installed must be running Ubuntu Server 16.04.6 LTS 64-bit (AMD64 or EM64T architecture). Refer to [Appendix 1: Install the Ubuntu OS](#).

Certificate requirements

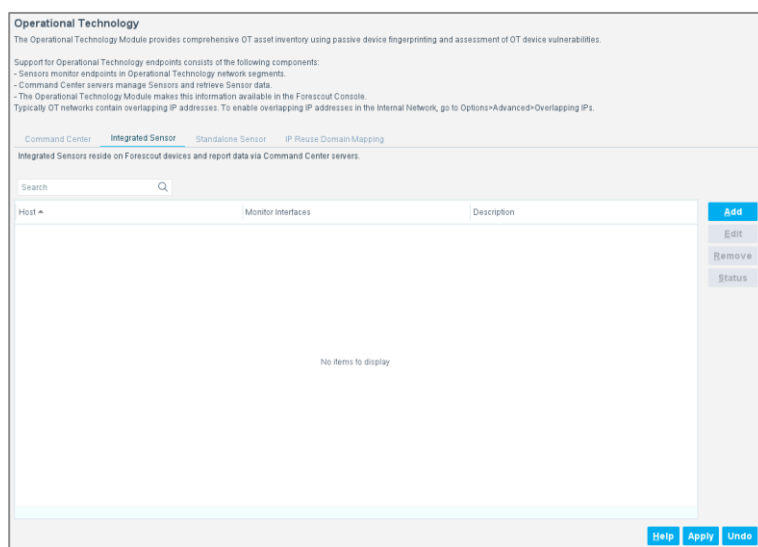
Forescout signed certificates are uploaded to the OT Monitoring Sensor server. For cases where the existing certificates must not be overwritten, the SilentDefense Command Center certificate must be imported into the Operational Technology module. Please refer to the Forescout Administration Guide, Appendix B: "Configuring the Certificate Interface" for more information.

Activate Integrated OT Sensors

Use this procedure to activate an integrated OT Sensor on a Forescout device. Before you begin, review [OT Sensor Requirements](#).

To activate an integrated OT Sensor:

1. In the ForeScout Console, select **Options > Operational Technology**.
2. In the Operational Technology pane, select the Integrated Sensor tab.



3. Select **Add**. The Add Sensor wizard appears.

4. Specify the following information:

Host	The Forescout Appliance that hosts the OT Sensor. <ul style="list-style-type: none"> It is not recommended to activate an OT Sensor on the Forescout device that communicates with Command Center.
Description	A text label that identifies the OT Sensor.

5. Select **Next**. From the interfaces available on the Appliance, select the interfaces that the OT Sensor uses to monitor OT devices. Typically this is a NIC connected to a SPAN or TAP port.



6. Select **Finish**. The OT Sensor appears in the Integrated Sensors table.

Install and Configure Standalone OT Sensors

This section describes how to install and configure OT Sensor instances that are not hosted by Forescout devices.

Install a Standalone OT Sensor

Before you begin, review [OT Sensor Requirements](#).

-  *Run script files in the order specified in this procedure.*
-  *To submit sudo commands, provide your root password when prompted.*

To install a standalone OT Sensor:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download and unpack the installation package.
3. Copy installation files to the server using suitable protocols such as scp/sftp for Linux machines, or pscp/winscp for Windows machines.

- On Linux machines, use a command like the following:

```
scp <file_name> silentdefense@<Sensor_IP>:~/
```
- On Windows machines, use an SSH tool with a command like the following:

```
pscp.exe <file_name> silentdefense@<Sensor_IP>:
```

where <file_name> specifies one or more of the installation files, and <Sensor_IP> is the hostname or IP address of the management interface of the server.

4. Open an SSH session to the OT Sensor machine and log in as the silentdefense root user you defined in Ubuntu.
5. Verify the installation files are all on the server by issuing the following command to list the contents of the current directory:

```
ls -alh
```
6. Mark the installers as executable files by running the following command:

```
chmod a+x *.run
```
7. Use a command like `sudo ./ <filename>` to run the update installer `update_os...run` provided in the installation package. The script updates core operating system packages to the versions available at the specified date.
8. Run the main configuration installer `main_configuration...run` provided in the installation package.

9. After the main configuration installer finishes successfully, reboot the system:

```
sudo reboot
```

Log in as the silentdefense root user you defined in Ubuntu.

10. Start the OT Sensor installer `sensor_<version>_install_withdeps...run` provided in the installation package.

The installation script prompts you for the number of working CPU threads for the OT Sensor. Use caution when changing the default value.

11. Install any OTSEC security updates if available. See [Apply Security Updates](#).
12. Copy certificate files to `"/opt/nids/cert/"`. See [Initial Certificates Setup](#).

Configure a Standalone OT Sensor

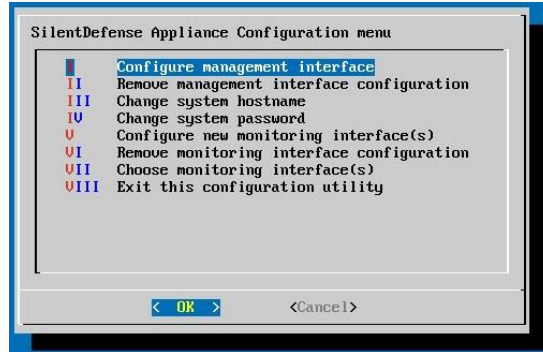
To configure a standalone OT Sensor:

1. Open an SSH session to the machine and log in as the silentdefense user you defined in Ubuntu.
2. Enter the following command:

```
sudo sdconfig
```

When prompted, enter the default password `Ghancot3`.

The Appliance Configuration main menu appears.



The following table describes the configuration options that are available.

Feature	Description	Required
Configure management interface	Configure the IP address, gateway, and DNS server of the OT Sensor that is used for communication with Command Center.	Required
Remove management interface configuration	Remove a configured management network interface from the network interface configuration file in Linux.	Optional

Feature	Description	Required
Change system hostname	Change the hostname used to identify the server. This is also the username used to access the OT Sensor operating system. To complete this action, reboot the system (<code>sudo reboot</code>) and log in as the silensecurity root user.	Optional
Change system password	Change the password used to log in to the OT Sensor operating system.	Recommended
Configure new monitoring interface(s)	Prepare and activate network interfaces defined on the server for use by the OT Sensor. The OT Sensor uses these interfaces to monitor endpoints.	Required
Remove monitoring interface configuration	Remove a configured monitoring interface from the network interface configuration file in the Linux Operating System.	Optional
Choose monitoring interface(s)	Select networks interfaces that the OT Sensor uses to monitor endpoints. This option disables configured monitoring interfaces without removing them.	Optional

Select **Configure management interface** and define address and gateway settings for the OT Sensor. Record the values you enter in this interaction. You must enter these values when you define this OT Sensor instance in Command Center, as described in [Configure Management Connections to OT Sensors](#).

eyeSegment Support

To support eyeSegment integration, the OT Monitoring Sensor must be version 4.1.2. Additional configuration must be applied on the OT Monitoring Sensor server. This can be done persistently by adding the configuration setting to the configuration file `/opt/nids/conf/nids.conf`. Edit this file and add a new line to it with following setting:

```
af-enable-netflow=true
```

After editing the configuration, if the Monitoring Server is running, restart it. On a standalone OT Sensor, use `sudo supervisorctl restart nids`. On an integrated sensor, reboot the server.

For more information about OT Monitoring Sensor settings, see the *SilentDefense Installation and Configuration guide, appendix B.2*.

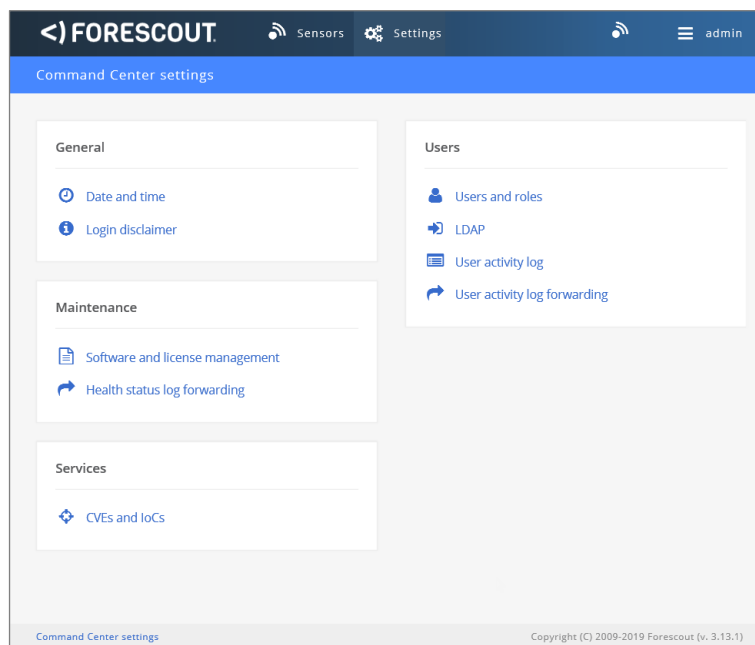
Please ensure that the OT Monitoring Sensor and the connecting Forescout Appliance can both connect to the OT Command Center on port 9092. This port is used to transport data for eyeSegment. If there is a firewall between the Appliance and the Command Center, or between the Monitoring Sensor and the Command Center, please ensure that firewall rules are set to allow communications over 9092 through those respective firewalls.

Update the OT Vulnerability Database

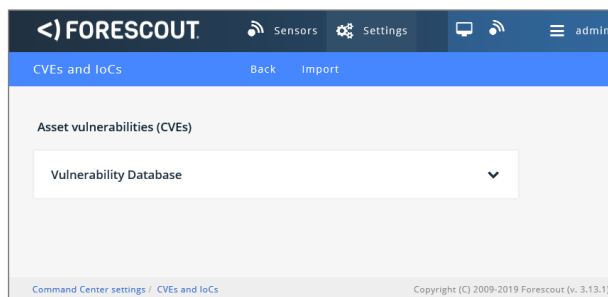
Use this procedure to install periodic updates of the OT Vulnerability Database used by OT Sensors to monitor Operational Technology endpoints. Updating the OT Vulnerability Database also updates parameter values for the OT Vulnerability host property.

To update the OT Vulnerability Database:

1. Open a browser and navigate to the server that hosts the Command Center you want to update.
2. The Login screen appears. Log in using admin-level credentials.
3. The Command Center settings page appears.



4. In the Services area, select **CVEs and IoCs**. The CVEs and IoCs page opens.



- e. Select **Import**.
 - f. Specify the file that contains database updates.
 - g. Select **Upload**.
- Database updates are imported into the Command Center.
5. Select **Finish**.

Managing Operational Technology Endpoints in Forescout

Endpoints in OT/automation environments have unique functional requirements. This section describes configuration settings, tools, and methods to manage these endpoints using the Forescout/SilentDefense solution.

Passive Management of Sensitive Endpoints

Mission-critical Operational Technology endpoints cannot tolerate active management contact from the Forescout platform. To manage these endpoints passively:

- Use Segment Manager to organize sensitive endpoints in dedicated segments.
- Use the *Properties – Passive Learning* group. Endpoints and address ranges in this group are not actively inspected as part of policy evaluation.
 - Add all known network ranges for sensitive endpoints to the group.
 - To ensure passive handling of endpoints, it is recommended to use IP addresses to define group members, rather than MAC addresses.
- Configure switches belonging to sensitive segments with read-only permissions in Forescout.
- When you construct Forescout policies that apply control actions, define the scope to exclude sensitive endpoints unless required.

Refer to the *Forescout Administration Guide* for details of segment, group, and switch configuration in Forescout, and for Forescout policy options.

Overlapping IP Addresses

Networks in plant/production, building automation, and other Operational Technology environments often contain duplicate sites and network structures. IP addresses repeat, or *overlap*, across the network.

To support networks with overlapping IP addresses, you must enable configuration options and tools in the Forescout platform. SilentDefense components support overlapping network segments by default.

The Forescout platform and SilentDefense components use **IP Reuse Domains** to distinguish several instances of an overlapping IP address. You define a unique IP Reuse Domain for each repeated segment or network branch. IP addresses are unique in each IP Reuse Domain.

- In the Forescout platform, IP Reuse Domains are assigned to Appliances. Identical segments are distinguished from each other by the IP Reuse Domain of the Appliance that manages each segment. For information about support for overlapping IPs in the Forescout platform, see the *Working with Overlapping IPs How-to Guide*.

- In SilentDefense, IP Reuse Domains are defined in the Command Center Console and assigned to selected Sensors. For details of IP Reuse Domains in SilentDefense, see the *SilentDefense Installation and Configuration Guide*.

The IP Reuse Domains defined in the Forescout platform must correspond to the IP Reuse Domains defined in Command Center. See [Configure OT Module Connections to Command Center](#).

When support for overlapping IPs is enabled in the Forescout platform, the IP Reuse Domain is added to IP addresses or segments in NAC view and other views. IP addresses are presented in the following format:

<IPv4>@IP_Reuse_Domain

For example:

192.168.0.1@Site_A

In the following example, the Console lists [nested devices](#) within a controller that is assigned to an IP Reuse Domain. The IP of the parent controller endpoint is 1.4.28.1 and the IP Reuse Domain is Site2.

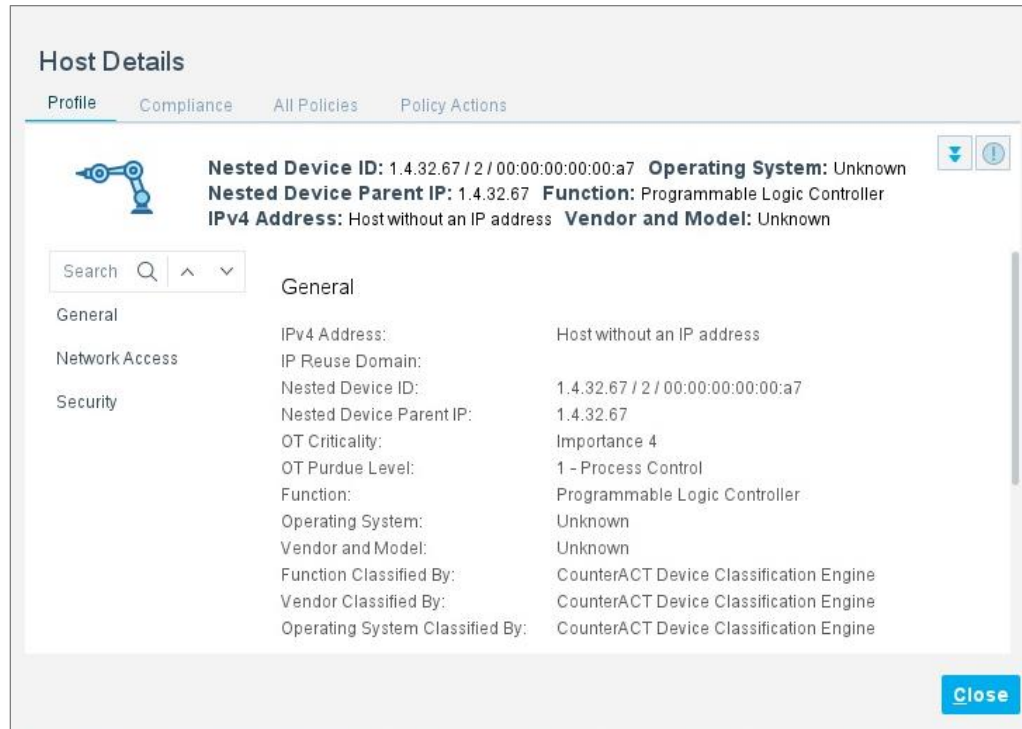


Use the **IP Reuse Domain** host property to create policies and Inventory views to manage endpoints in overlapping sites.

Nested Devices

In Operational Technology and automation environments a controller or other endpoint may integrate sub-modules or PLCs. High level management systems or DCS/SCADA servers communicate only with the main controller, which then mediates the communication to the secondary nested controllers.

SilentDefense components identify these child devices based on deep analysis of traffic from the parent. In the Console screen shown below, the IP address exposed by the parent device is 1.4.32.67. Sub-modules are identified by strings appended to the parent IP address. The format of these strings varies with the configuration and internal protocol of the nested device.



Use the following host properties to work with this information in Forescout.

Nested Device ID	The full string used to identify a sub-module or nested device, including the parent IP address.
Nested Device Parent IP	The IP address of an endpoint that contains sub-modules or nested devices.

The Operational Technology module provides an Inventory view that lists nested devices.


Work with Endpoint Information

The Operational Technology Module periodically retrieves information about OT endpoints from Command Center, and applies an aging filter to identify active endpoints with recently reported data. By default, this filter matches the three-day limit used in Forescout to filter inactive endpoints.

The module provides reported information as endpoint properties.

- Use these properties to create conditions in Forescout policies.
- The module provides predefined Inventory views based on key properties.

In addition, information about OT endpoint function, vendor, and model is used to resolve general Forescout endpoint classification properties.

 *Some properties are only relevant to certain endpoint types such as embedded devices or PLCs.*


The following properties are available in the Policy editor under **Properties>Operational Technology**.

Client Protocols	The application-level communications protocols used by an OT endpoint to initiate a communications stream. From the Command Center API field: Host>client_protos
OT Communication First Seen	The ISO-formatted timestamp of when an OT endpoint was first seen by a Sensor. For example: 2017-07-26T15:07:37.000+01:00 From the Command Center API field: Host>first_seen
OT Communication Last Seen	The ISO-formatted timestamp of when an OT endpoint was last seen by a Sensor, as calculated by the Command Center. For example: 2017-07-26T15:07:37.000+01:00 From the Command Center API field: Host>last_seen
OT Criticality	A measure of how critical (important) an OT endpoint is, based on its role. There is a parallel Track Changes property. From the Command Center API field: Host>criticality
OT Firmware Version	The firmware version running on an OT endpoint. From the Command Center API field: Host>firmware_version There is a parallel Track Changes property.
OT Hardware Version	The hardware version of an OT endpoint. From the Command Center API field: Host>hardware_version
OT Host Name	The name of an OT endpoint. From the Command Center API field: Host>main_name
OT Modules	Information about modules detected in an OT endpoint, by rack slot. From the Command Center API field: Host>module_identities Refer to SilentDefense API documentation for details of the ModuleIdentity data structure used to report this value.
OT NERC CIP Classification	NERC CIP classifications assigned to an endpoint. A parallel Inventory view is provided. From the Command Center API field: Host>nerc_cip_classifications Refer to SilentDefense API documentation for details of the NERCCIPClassification data structure used to report this value.
OT Project Name	The project of a PLC endpoint. From the Command Center API field: Host>project

OT Purdue Level	<p>The Purdue level of an OT endpoint. Valid values include:</p> <ul style="list-style-type: none">▪ LEVEL0▪ LEVEL1▪ LEVEL2▪ LEVEL3▪ LEVEL35▪ LEVEL4▪ LEVEL5▪ UNDEFINED <p>There is a parallel Track Changes property. From the Command Center API field: Host>purdue_level</p>
OT Serial Number	<p>The serial number of an OT endpoint. From the Command Center API field: Host>serial_number</p>
OT Vulnerabilities	<p>Vulnerabilities that were detected on an OT endpoint. The database includes known CVEs and detailed CVSS information. From the Command Center API field: Host>cves There is a parallel Track Changes property. Refer to SilentDefense API documentation for details of the HostCVEInfo data structure used to report this value.</p>
Server Protocols	<p>The application-level communications protocols accepted by an OT endpoint to establish a communications stream. From the Command Center API field: Host>server_protos</p>

Appendix 1: Install the Ubuntu OS on Standalone OT Sensors

This section describes how to install the Ubuntu Server Operating System on the server, using either physical media or remotely by using an Out-of-band management solution.

 *These instructions are generally applicable to Ubuntu Server 16.04.x releases. Refer to Ubuntu product documentation for more details, including release-specific changes.*

The installer will ask a number of questions:

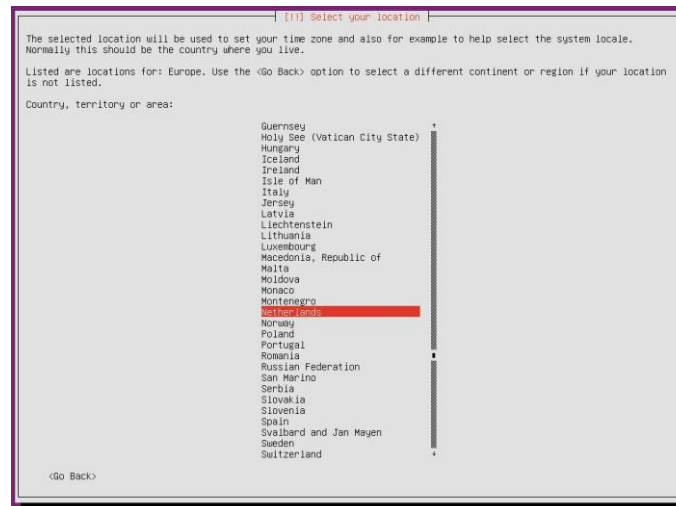
1. **Linux kernel** This will determine the type of the installed Linux kernel. The Linux HWE kernel is used (HardWare Enablement helps catching up with the newest hardware technologies). Choose *Install Ubuntu Server with the HWE kernel* to install it.



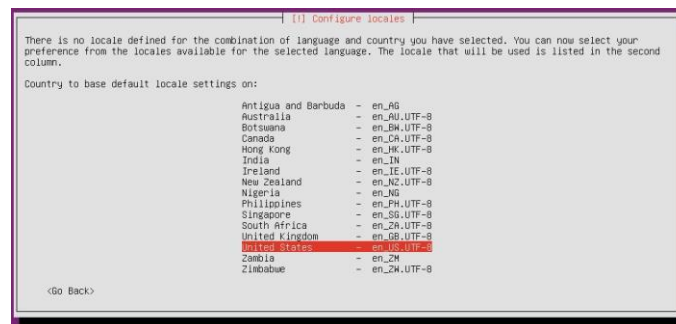
2. **Language** This will determine the language of the Operating System. Choose *English* here to be able to receive proper support.



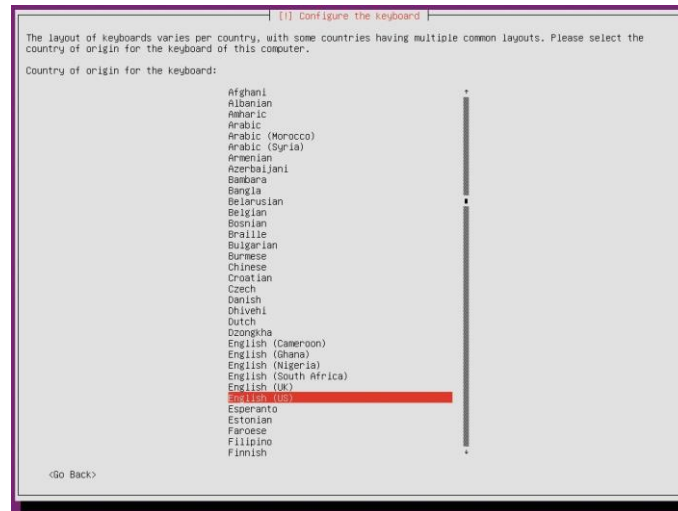
- 3. Location** Choose your geographical location here, in order to determine your timezone and locale settings.



- 4. Locale** The installer will determine a default locale based on your location settings. Usually the default settings can be accepted here.



- 5. Keyboard layout** If you know your keyboard layout, you can choose not to have it detected and select it from a list. Usually the defaults can be accepted here.

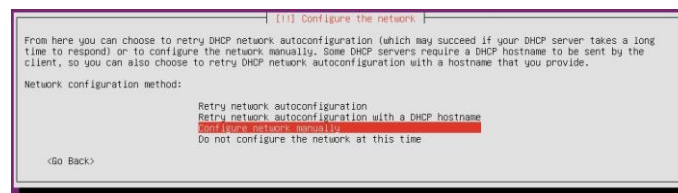


- 6. Network hardware** The installer will now look for available network interfaces. Ubuntu uses predictable network interface names, using a cascading logic for assigning predictable names to interfaces, according to the following information:

- Names incorporating Firmware/BIOS provided index numbers for on-board devices (example: eno1)
- Names incorporating Firmware/BIOS provided PCI Express hotplug slot index numbers (example: ens1)
- Names incorporating physical/geographical location of the connector of the hardware (example: enp2s0)
- Names incorporating the interfaces's MAC address (example: enx78e7d1ea46da)
- Classic, unpredictable kernel-native ethX naming (example: eth0)

For the management network interface the first interface of the on-board network adapter should be used, so select that one to be the primary interface (usually eno1).

- 7. Network configuration** The installer will attempt to configure the interface using DHCP. Since the server is not connected to the Internet and we do not want it to download operating system updates, cancel the automatic configuration. Instead, we will configure a static IP address. Choose the option *Configure network manually*.



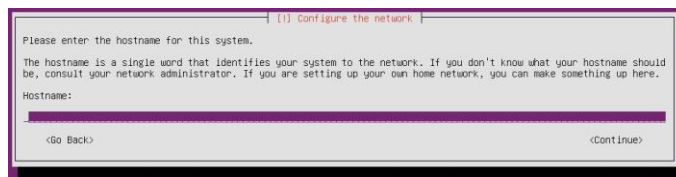
The installer will ask several questions to configure the network:

- IP address
- Netmask
- Gateway address

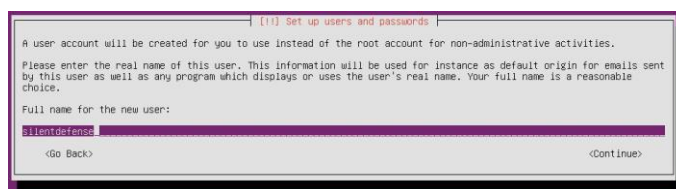
- Name server (DNS) address (Not required)

After entering these values, the installer will validate the configuration by trying to ARP-ping the gateway. After that, the installer continues with the next question.

8. Hostname Enter the hostname for the server.

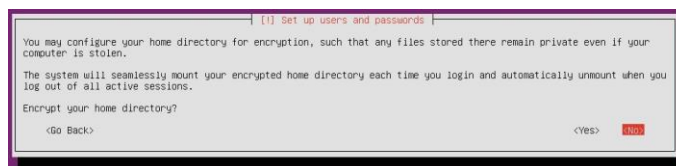


9. User configuration Enter silentdefense for both the *Full name* and *Username* of the new user (silentdefense as user is required by SilentDefense™ software. Please, DO NOT change it !). Enter a password for the silentdefense user.

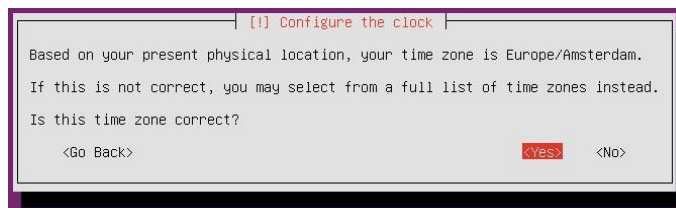


Recommended password length is at least 10 characters, with mixed lower- and uppercase, numbers and symbols. Remember this password well, as it might be required during support activities.

10. Encryption of home directory Choose *No* when asked whether or not to encrypt the silentdefense user's home directory. That is not necessary because no sensitive information will be stored in this directory.

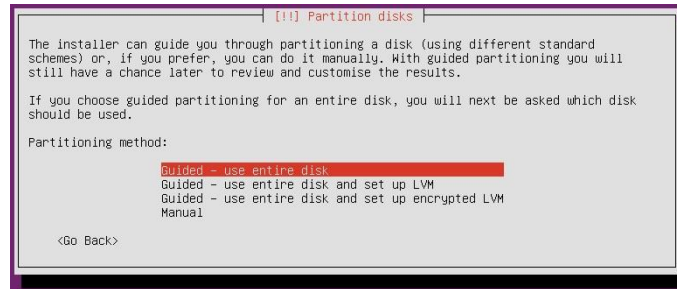


11. Timezone The installer will suggest a timezone based on your location. If that is correct, accept it. Otherwise, select the desired timezone from the list.



12. Partition disks The installer will ask the user to determine how the hard disk(s) should be partitioned. *Manual* disk partitioning is the recommended choice (the installer might define an unnecessarily large *swap* partition, based on the amount of RAM detected).

If the size of the storage isn't a problem the "Guided – use entire disk" option also can be used.



- Do not select either "Guided - use entire disk and set up LVM" or "Guided - use entire disk and set up encrypted LVM" option.

Storage can be:

- mounted and partitioned
- new or wiped

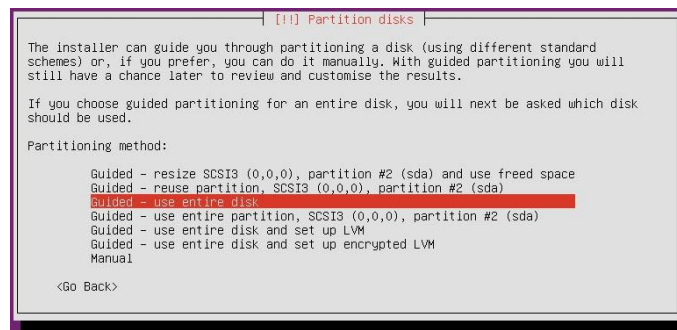
Storage having mounted partitions

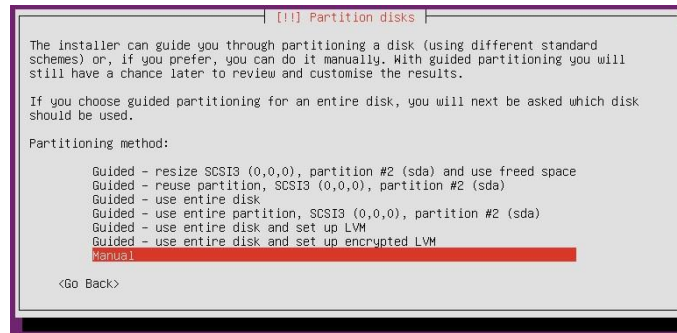
In certain configurations, the installer might detect a disk having mounted partitions. In this case follow the below procedure (these steps will explain the partitioning procedure on a BIOS system):

- a. Choose Yes to unmount the partition.

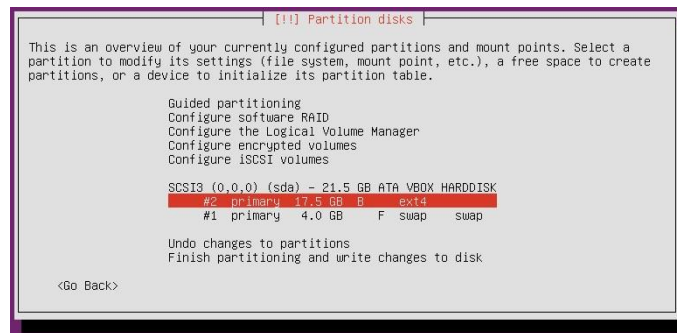


- b. Select "Guided – use entire disk" or "Manual" (in this procedure the "Manual" method will be followed)

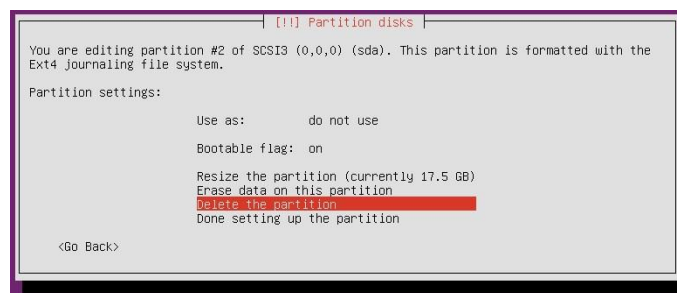




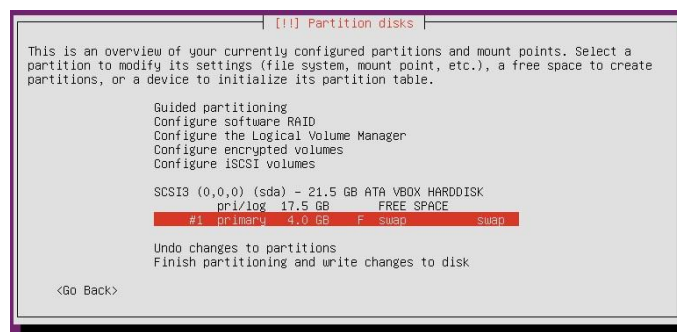
c. Select the "ext4" partition to be removed



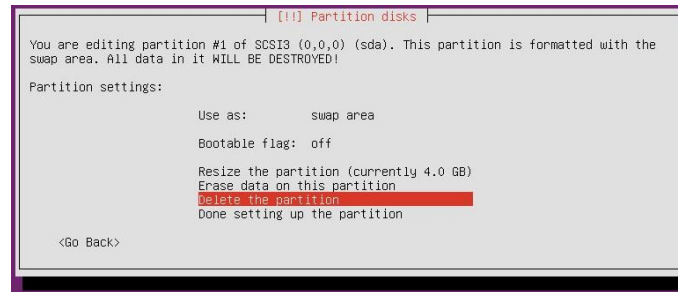
d. Delete the previously selected ext4 partition



e. Select the "swap" partition to be removed



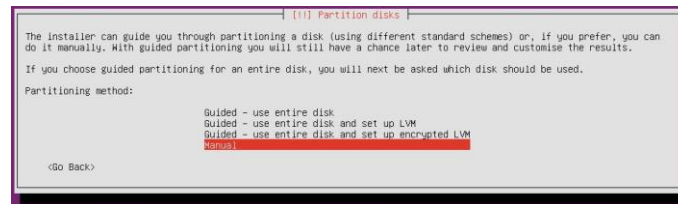
f. Delete the previously selected swap partition



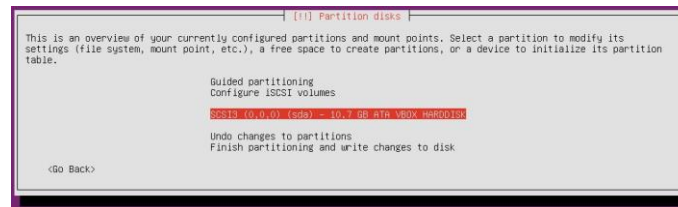
New or wiped storage

If the storage wasn't partitioned, because it is new or it has already been wiped, follow the below procedure:

- Choose "Manual" configuration of partitions.



- Choose the disk to use. At the "Partition disks" prompt, select the device using *up/down arrows* keys and *Enter* to confirm and go to the following prompt: select the device and press *Enter*.



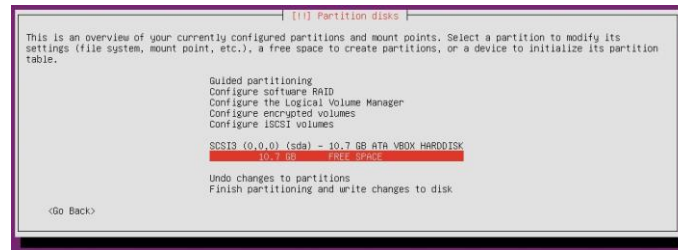
- Choose "Yes" when asked to create a new empty partition table on the device.

Follow the instructions below according to the hardware configuration (BIOS or UEFI)

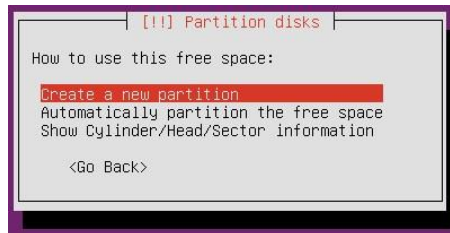


Partitioning a (U)EFI system

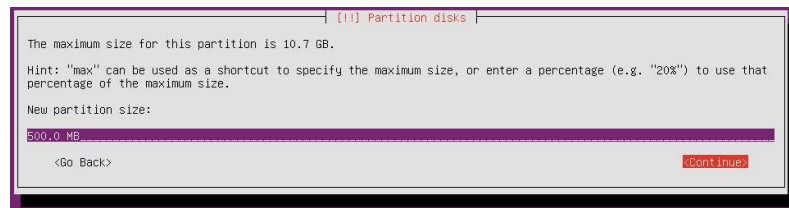
- Create the EFI partition (select *FREE SPACE* and press *Enter*):



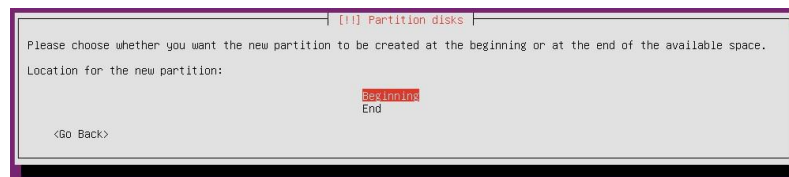
- b. Choose "Create a new partition" function



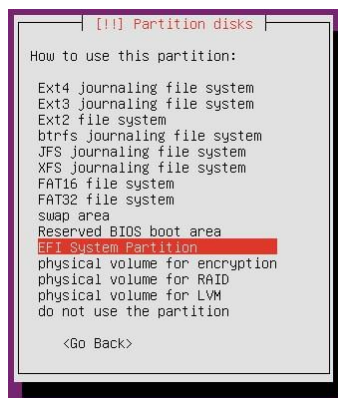
- c. Enter 500 MB for the partition size for the EFI system partition



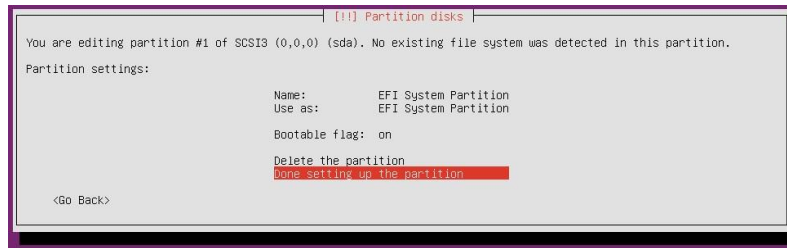
- d. Choose "Beginning" as the location



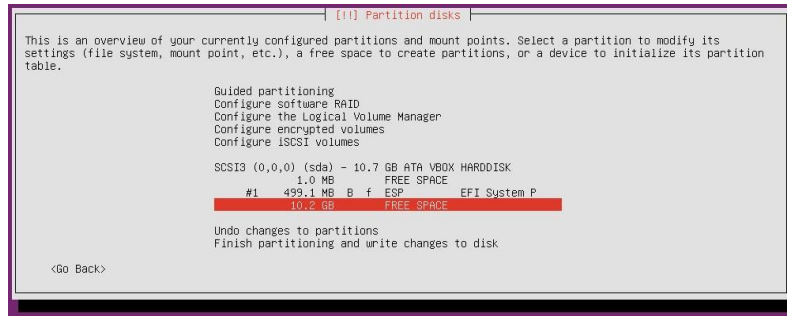
- e. Select "EFI System Partition" from the "Use as:" drop-down list (this selection should cause the *bootable* flag to be enabled)



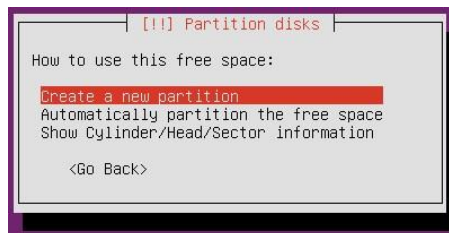
- f. Choose "Done setting up the partition"



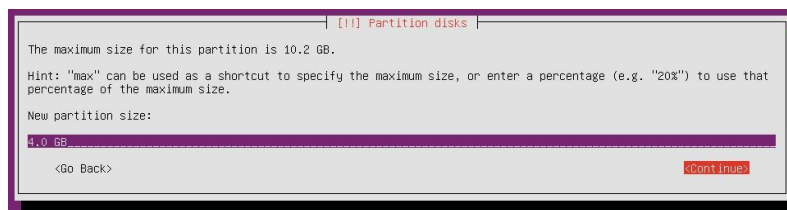
- g.** Create the swap partition (select *FREE SPACE* - with the biggest size - and press *Enter*):



- h.** Choose "Create a new partition"



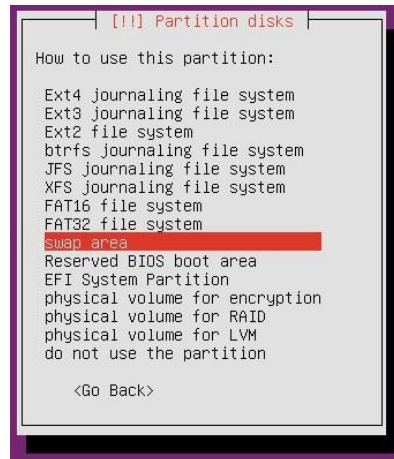
- i.** Enter 4.0 GB for the partition size



- j.** Choose "End" as the location for the new partition



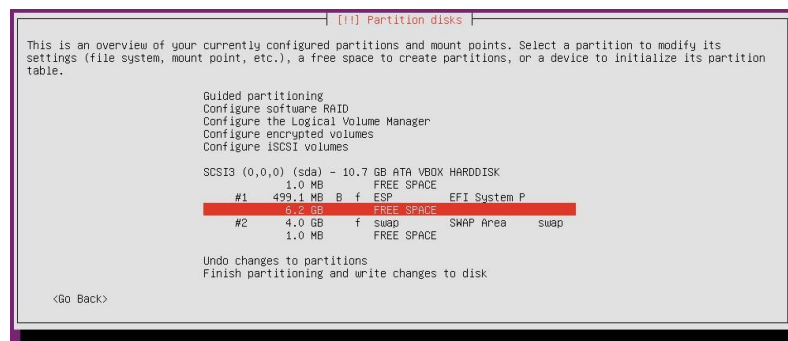
- k.** Select "Swap area" from the "Use as:" drop-down list



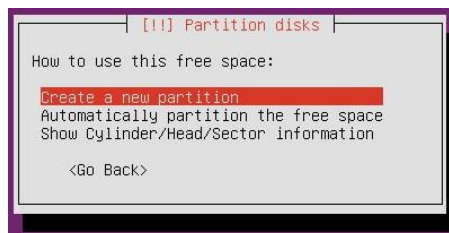
l. Choose "Done setting up the partition"



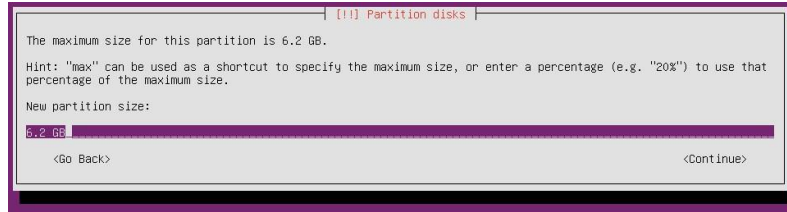
Create the root partition (select *FREE SPACE* – with the biggest size - and press *Enter*):



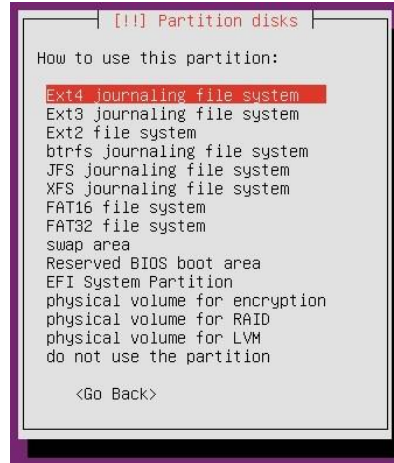
m. Choose "Create a new partition" function



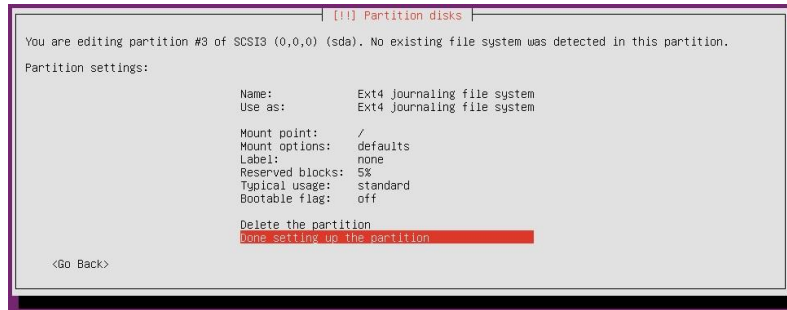
n. Use the remaining space, the amount should be filled in by default



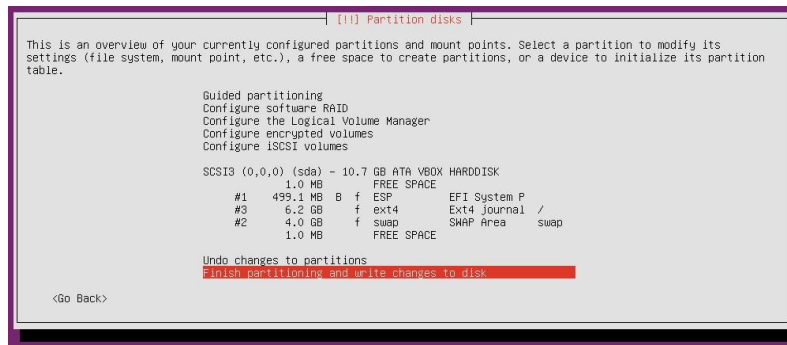
- o. Verify that the "Use as:" option shows "Ext4 journaling file system" as the chosen file system



- p. Choose "Done setting up the partition"

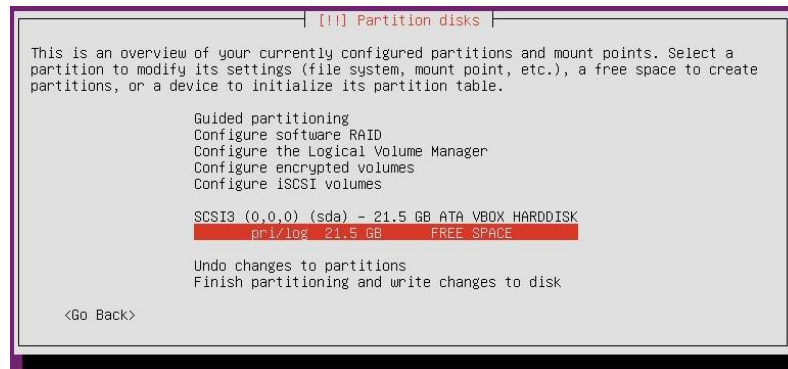


- q. Choose "Finish partitioning and write changes to disk" and "Yes" when asked to "Write the changes to disks?".



Partitioning a BIOS system

Create the swap partition (select *FREE SPACE* -with the biggest size - and press *Enter*):



a. Choose "Create new partition" function



b. Enter 4.0 GB for the partition size



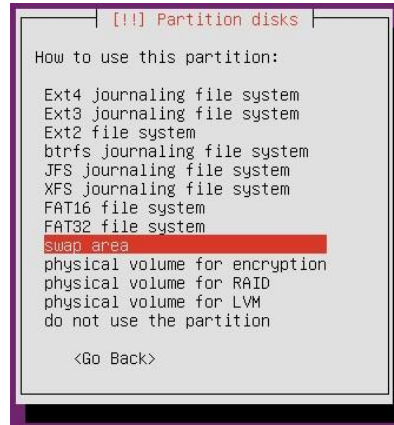
c. Choose "Primary" for the partition type



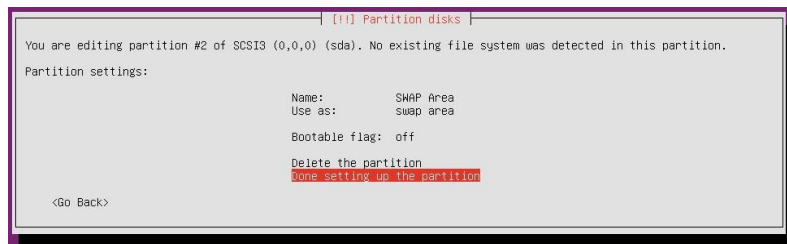
d. Choose "End" as the location



- e. Select "Swap area" from the "Use as:" drop-down list



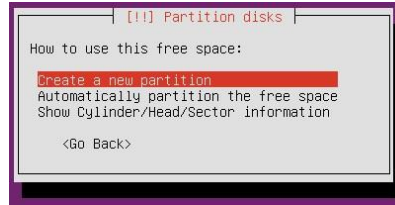
- f. Choose "Done setting up the partition"



Create the root partition (select *FREE SPACE* - with the biggest size - and press *Enter*):



- g. Choose "Create new partition" function



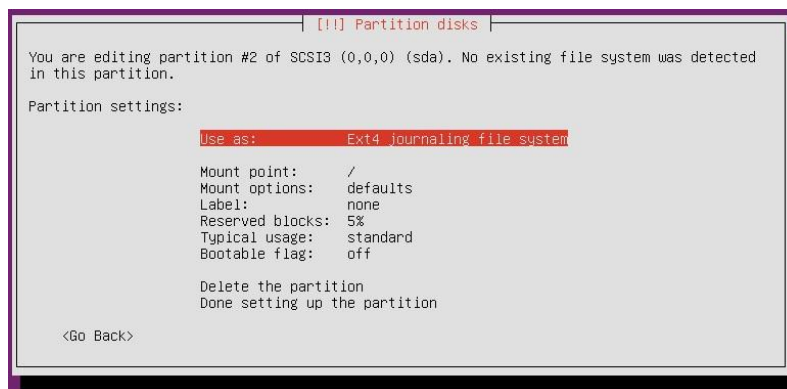
- h. Use the remaining space, the amount should be filled in by default



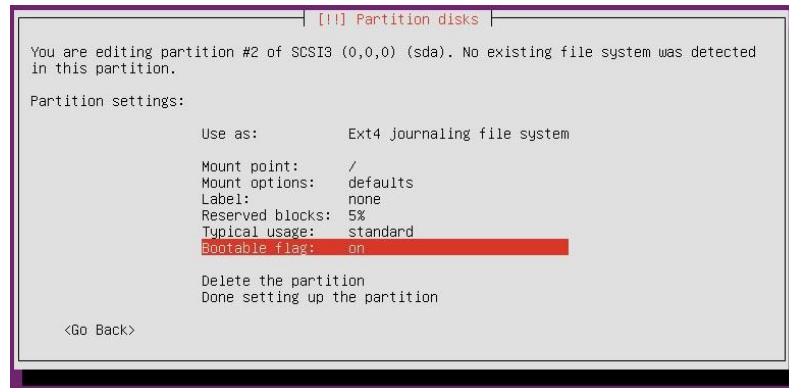
- i. Choose "Primary" for the partition type



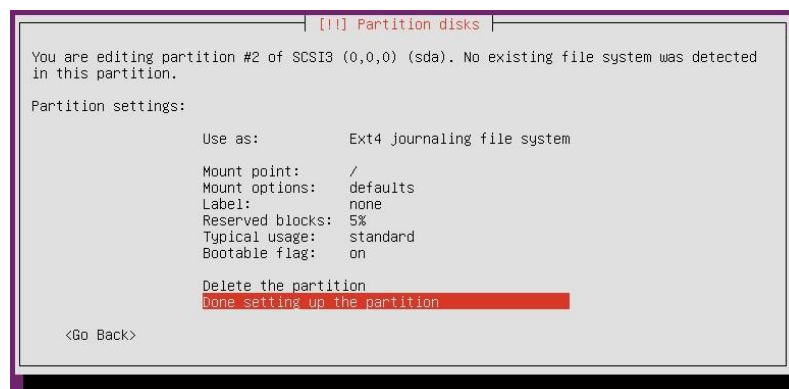
- j. Verify that the "Use as:" option shows "Ext4 journaling file system" as the chosen file system



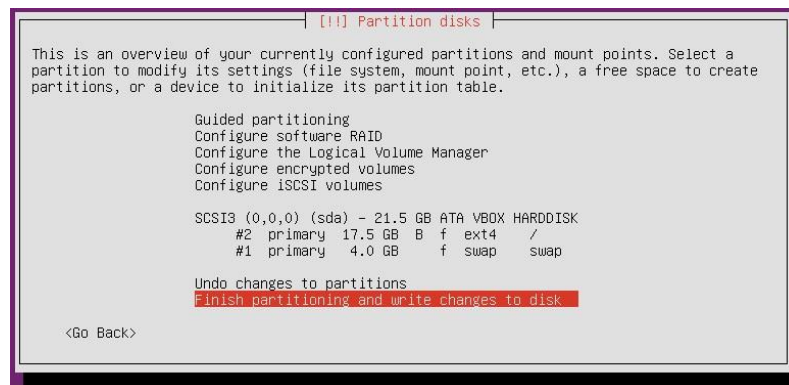
- k. Set the *bootable* flag to "on"



l. Choose "Done setting up the partition"



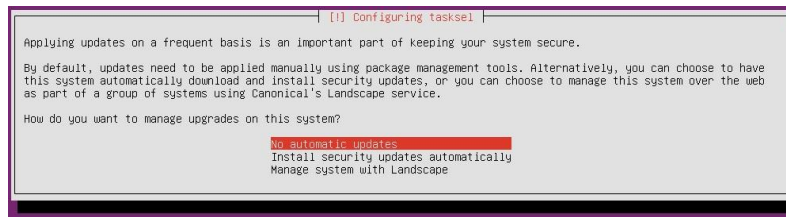
m. (d) Choose "Finish partitioning and write changes to disk" and "Yes" when asked to "Write the changes to disk?"



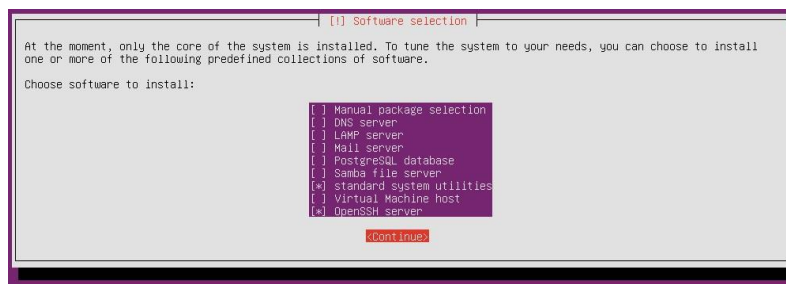
13. Package manager Do not fill in a proxy address for the package manager, just choose *Continue*.



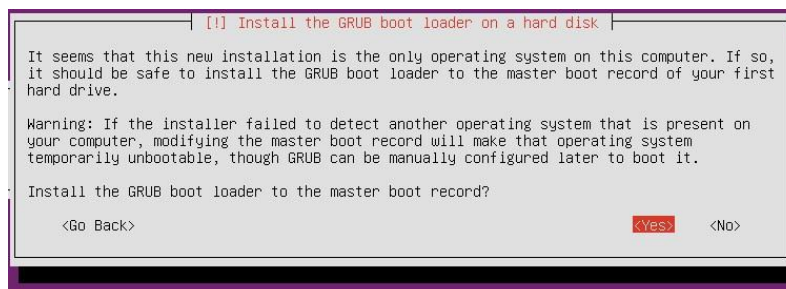
- 14. Automatic updates** The installer will ask if updates should be automatically installed. Since necessary updates will be provided by *SecurityMatters*, choose *No automatic updates*.



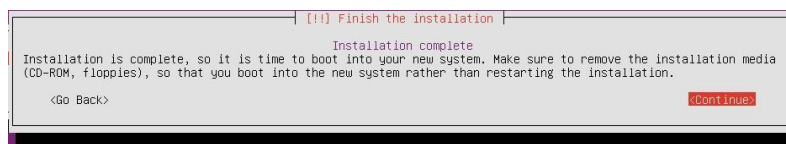
- 15. Software selection** Most of the software will be installed by SilentDefense but the *OpenSSH Server* package should be selected during the OS installation. This allows remote management of the Operating System through a SSH session. Furthermore, the "Standard system utilities" should stay selected (it is by default). Use the arrow keys to move through the packages list and press the spacebar to select the "OpenSSH server" package.



- 16. Bootloader installation** The installer will ask if the bootloader can be installed on the hard disk. Since this will be the only Operating System that is going to be installed, choose *Yes*.



- 17. Finishing installation** The installation is now almost finished. Choose *Continue* to reboot the system into the new Operating System.



Additional ForeScout Documentation

For information about other Forescout features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Forescout Resources Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Portal](#)

 Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources page provides links to the full range of technical documentation.

To access the Forescout Resources page:

- Go to <https://www.Forescout.com/company/resources/>, select **Technical Documentation**, and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After installing the plugin, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the [Forescout Resources Page](#) (Flexx licensing) or the [Documentation Portal](#) (Per-Appliance licensing).