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.

2020-02-12 14:49
# 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 ........................................................................... 6
    - Integrate OT Support with an Existing SilentDefense Deployment .................... 7
- **Install and Configure Command Center** ......................................................... 8
  - Install Command Center on a Hardware Server ................................................. 8
    - Requirements ...................................................................................................... 8
    - Installation .......................................................................................................... 8
  - Install Command Center on a Virtual Machine .................................................. 9
    - Requirements ...................................................................................................... 9
    - Installation .......................................................................................................... 10
  - Configure Command Center ............................................................................... 11
    - Initial Configuration in the Command Center Console ..................................... 13
- **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 ................................... 19
    - Map IP Reuse Domains to Command Center ..................................................... 21
    - Manage Traffic Inspection Scripts .................................................................... 23
- **Install and Configure OT Sensors** ................................................................. 23
  - OT Sensor Requirements ..................................................................................... 24
  - Activate Integrated OT Sensors .......................................................................... 24
  - Install and Configure Standalone OT Sensors .................................................... 26
    - Install a Standalone OT Sensor ........................................................................ 26
    - Configure a Standalone OT Sensor .................................................................... 27
- **Working with Certificates** ............................................................................ 28
  - Export and Install Certificate Files for Standalone Sensors .................................. 29
  - Install a Custom Certificate for the Command Center Web Service ................... 29
- **Update the OT Vulnerability Database** ......................................................... 30
- **Managing Operational Technology Endpoints in Forescout** ....................... 32
  - Passive Management of Sensitive Endpoints ..................................................... 32
  - Overlapping IP Addresses ................................................................................... 32
  - Nested Devices ................................................................................................... 33
  - Work with Endpoint Information ....................................................................... 34
- **Appendix 1: Install the Ubuntu OS on Standalone OT Sensors** .................... 37
Additional ForeScout Documentation ......................................................... 53
  Documentation Downloads ........................................................................ 53
  Documentation Portal ........................................................................... 54
  ForeScout Help Tools .......................................................................... 54
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 Sensors**
  Each OT 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 Center**
  The Command Center collects and processes data reported by Sensors, and supports a web interface for OT endpoint event management.
  - The Command Center 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. Use this information in Forescout policies and 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

The 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 OT Sensors in two ways:

- **Integrated OT Sensors** are hosted on a Forescout Appliance.
- **Standalone OT Sensors** are installed on another server or virtual server in the network.

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.

New Deployment of OT Support

**Install and Configure Command Center**

**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**

**Export and Install Certificate Files for Standalone Sensors**

To work with integrated OT Sensors:

**Activate Integrated OT Sensors**

**Configure Management Connections to OT Sensors**

**Work with OT Endpoint Information in Forescout**

**Update the OT Vulnerability Database**

To use advanced Command Center features:

**Install or Upgrade Your License**
Certificate Options for New Deployments

The installation procedures described in this document use default certificates provided with the Operational Technology Module. These certificates are self-signed.

To enable secured web connection to the Command Center, it is possible to distribute a custom certificate after installation. This certificate must also be imported into Forescout.

- For details of installing a certificate in Forescout, refer to Appendix B, "Configuring the Certificate Interface" in the Forescout Administration Guide
- Refer to Working with Certificates for details of installing certificates on Command Center and standalone Sensors.

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 this release, or to a compatible release. Refer to SilentDefense documentation.
- Export the public certificate from the existing Command Center. Typically, this certificate is available from the browser window.
- Import this certificate into Forescout. Refer to Appendix B, "Configuring the Certificate Interface" in the Forescout Administration Guide

Install and Configure the Operational Technology Module

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

Work with OT Endpoint Information in Forescout

Update the OT Vulnerability Database

To use advanced Command Center features:

Install or Upgrade Your License

Certificate Options for Integration with SilentDefense Deployments

In the installation procedures described in this document, the certificate used in the existing Command Center is copied to Forescout. If you want to add Forescout standalone or integrated OT Sensors to this existing deployment, you must copy this certificate to OT Sensors to allow them to connect to the Command Center.

It is also possible to work with Forescout default certificates. In this case, you must export the Forescout certificate and install it on existing Sensors and Command Center instances.

Refer to Working with Certificates for details of installing certificates on Command Center and standalone OT Sensors.
Install and Configure Command Center

This section describes how to install an Command Center instance, and define the Sensors that it manages.

To support assignment to a managing Appliance, the 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:


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

Forescout 8.2 including Operational Technology Module version 1.2.0

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

Forescout 8.2 including Operational Technology Module version 1.2.0
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.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Center</td>
<td>Sensor(s)</td>
<td>TCP 22 (ssh) TCP 9999 (configurable: see SilentDefense documentation)</td>
<td>System management and event communication.</td>
</tr>
<tr>
<td>Forescout Connecting Appliance</td>
<td>Command Center</td>
<td>TCP 8444 TCP 443 (https) TCP 22 (ssh)</td>
<td>Software updates.</td>
</tr>
</tbody>
</table>

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 an 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 an 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure management interface</td>
<td>Configure the IP address, gateway, and DNS server of this Command Center that is used for communication with Forescout and with Sensors.</td>
<td>Required</td>
</tr>
<tr>
<td>Remove management interface configuration</td>
<td>Remove the configured management network interface from the network interface configuration file in the Linux Operating System.</td>
<td>Optional</td>
</tr>
<tr>
<td>Change system hostname</td>
<td>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 (sudo reboot) and log in as the silentdefense root user.</td>
<td>Optional</td>
</tr>
<tr>
<td>Change system password</td>
<td>Change the password used to log in to the Command Center operating system.</td>
<td>Recommended</td>
</tr>
<tr>
<td>Configure Command Center memory allocation</td>
<td>Modify default memory allocation for Command Center processes on the server. For details, refer to the SilentDefense documentation suite.</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure Command Center replication</td>
<td>Configure warm mirroring between two Command Center instances. For details, refer to the SilentDefense documentation suite.</td>
<td>Optional</td>
</tr>
</tbody>
</table>
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**

**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**

---

**Feature** | **Description** | **Required**
--- | --- | ---
**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

---
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.
3. The Command Center settings page appears.

In the Maintenance area, select Software and license management. The Software and licenses page appears.
4. In the toolbar, select **Upload license > To Command Center**. The Upload license to the Command Center dialog appears.

   ![Upload license to the Command Center dialog](image)

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

   The license is installed.

5. 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**.

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.

![Sensors overview page](image)


![Add new sensor dialog](image)

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor name</td>
<td>A label that identifies the Sensor</td>
</tr>
<tr>
<td>Sensor Address</td>
<td>The IP address of the machine hosting the Sensor</td>
</tr>
<tr>
<td>Port</td>
<td>The port configured for monitoring on this Sensor</td>
</tr>
</tbody>
</table>

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
The following components are required to install the Operational Technology Module:
Forescout 8.2

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.

3. Save the file to the machine where the Console is installed.

4. Log into the Console and select Options from the Tools menu.

5. Select Modules. The Modules pane opens.

6. Select Install. The Open dialog box opens.

7. Browse to and select the saved module .fpi file.

8. Select Install. The Installation screen opens.

9. 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.

10. 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 **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**

Configure OT Module Connections to Command Center

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

ℹ️ 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.

ℹ️ 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.

```
<table>
<thead>
<tr>
<th>IP/Name</th>
<th>The hostname or IP address of the Command Center instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>The port that Forescout connects to on the Command Center machine</td>
</tr>
<tr>
<td>Connecting CounterACT device</td>
<td>The hostname or IP of the Connecting CounterACT device</td>
</tr>
<tr>
<td></td>
<td>Do not select a device that runs an integrated OT Sensor.</td>
</tr>
</tbody>
</table>
```

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

Command Center Credentials
Enter access credentials to the Command Center.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>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.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>
| Overwrite certificates and restart Command Center | Select this option to automatically configure certificates and distribute them to Command Center. When you select this option, specify SSH credentials. When you finish the configuration dialog and apply changes, Forescout restarts the Command Center instance. A backup file of existing certificates is created.  
  • **Note:** Do not select this option when you integrate an existing SilentDefense Command Center with Forescout. |
| SSH User name          | Specify the SSH credentials Forescout uses to distribute certificates to Command Center. |
| SSH Password           |                                                                                           |
| Confirm password       |                                                                                           |

6. Select **Finish**. The Command Center instance appears in the table.
7. In the Options pane, select **Modules**. Select the Operational Technology module, and then select **Start**.

**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. Repeat this procedure when you change IP Reuse Domain definitions in either platform.

- *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.

**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* field, enter a comma-separated list of IP Reuse Domains defined in the SilentDefense Command Center.
   d. Select *OK*.

4. Repeat this procedure to define a mapping rule for each IP Reuse Domain defined in the Forescout platform.

5. Select *Test* to test the mapping rules. The SilentDefense IP Reuse Domains listed in mapping rules must be present in the Command Center defined in the Command Center tab.

6. 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:


**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.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Center</td>
<td>OT Sensor(s)</td>
<td>22 (ssh)</td>
<td>System management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9999</td>
<td>SilentDefense event communication</td>
</tr>
</tbody>
</table>

**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:


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.

**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.


4. Specify the following information:

   **Host** | The Forescout Appliance that hosts the OT Sensor.  
   - 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.

### 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.

Install certificate files as described in Export and Install Certificate Files for Standalone Sensors

### 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure management interface</strong></td>
<td>Configure the IP address, gateway, and DNS server of the OT Sensor that is used for communication with Command Center.</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Remove management interface configuration</strong></td>
<td>Remove a configured management network interface from the network interface configuration file in Linux.</td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Change system hostname</strong></td>
<td>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 (sudo reboot) and log in as the silendefense root user.</td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Change system password</strong></td>
<td>Change the password used to log in to the OT Sensor operating system.</td>
<td>Recommended</td>
</tr>
<tr>
<td><strong>Configure new monitoring interface(s)</strong></td>
<td>Prepare and activate network interfaces defined on the server for use by the OT Sensor. The OT Sensor uses these interfaces to monitor endpoints.</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Remove monitoring interface configuration</strong></td>
<td>Remove a configured monitoring interface from the network interface configuration file in the Linux Operating System.</td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Choose monitoring interface(s)</strong></td>
<td>Select networks interfaces that the OT Sensor uses to monitor endpoints. This option disables configured monitoring interfaces without removing them.</td>
<td>Optional</td>
</tr>
</tbody>
</table>

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](#).

## Working with Certificates

Use the procedures in this section to ensure that solution components can communicate with each other using the correct certificate files.

For example, in deployments that combine Forescout OT components with existing SilentDefense components, you may need to use the procedures described here to install Forescout certificates on existing SilentDefense components. You may also need to import existing signed certificates into the Certificates area of the Forescout Console.
Export and Install Certificate Files for Standalone Sensors

Use this procedure to export certificate files from Forescout and install them on a Sensor. This lets standalone OT Sensors and SD Sensors communicate with an Command Center that uses the certificate provided by Forescout.

Integrated OT sensors always use the certificate defined in Forescout for OT Communication.

To export certificates from Forescout:

1. In the ForeScout Console, select Options > Operational Technology.
2. In the Operational Technology pane, select the Standalone Sensor tab.
3. Select Export Certificate. Save the archived certificate files.

To install certificate files on a standalone sensor:

1. Open an SSH session to the Sensor machine and log in as the silentdefense root user you defined in Ubuntu.
2. Unzip the archived certificate files you exported from Forescout. Copy the files to the following location on the Sensor:
   /opt/nids/cert/
3. Restart the Sensor service with the following command:
   sudo supervisorctl restart nids
   When prompted, provide your root password.

Install a Custom Certificate for the Command Center Web Service

When Command Center is installed and defined in Forescout, self-signed default certificates are installed. This allows unsecured access to the Command Center web interface. Use the following procedure to install a signed certificate.
To install a custom certificate on Command Center:

1. Prepare a Java keystore that includes a private key and the signed public certificate issued to the domain name used by the Command Center server.
2. Copy the keystore to the location `/home/silentdefense/`.
3. Submit the following command to put the keystore file in the SSL directory:
   ```sh
   sudo mv /home/silentdefense/<keystore>.jks /opt/sdconsole/ssl/
   ```
   Where `<keystore>` is the name of the keystore file.
4. Back up the existing configuration file using a command like the following:
   ```sh
   sudo cp /opt/sdconsole/tomcat/conf/server.xml
   /opt/sdconsole/tomcat/conf/server.xml_defaultssl
   ```
5. Submit the following command to edit the configuration file:
   ```sh
   sudo nano /opt/sdconsole/tomcat/conf/server.xml
   ```
6. Search for the following line:
   ```xml
   <Connector port="443" protocol="HTTP/1.1" SSLEnabled="true" ...
   ```
7. In this XML element, edit the following attributes:
   - Change `KeystoreFile` to the pathname of the new file.
   - Change `KeystorePass` to the password needed to unlock the keystore.
8. Save changes to the configuration file.
9. Submit the following command to restart the Command Center:
   ```sh
   sudo supervisorctl restart silentdefense-cc
   ```

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.

![Command Center settings](image)

**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 Map IP Reuse Domains 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.

![Console screen showing nested devices](image)

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.

<table>
<thead>
<tr>
<th><strong>Nested Device ID</strong></th>
<th>The full string used to identify a sub-module or nested device, including the parent IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nested Device Parent IP</strong></td>
<td>The IP address of an endpoint that contains sub-modules or nested devices.</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>API Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Protocols</td>
<td>The application-level communications protocols used by an OT endpoint to initiate a communications stream.</td>
<td>Host&gt;client_protos</td>
</tr>
<tr>
<td>OT Communication First Seen</td>
<td>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</td>
<td>Host&gt;first_seen</td>
</tr>
<tr>
<td>OT Communication Last Seen</td>
<td>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</td>
<td>Host&gt;last_seen</td>
</tr>
<tr>
<td>OT Criticality</td>
<td>A measure of how critical (important) an OT endpoint is, based on its role.</td>
<td>Host&gt;criticality</td>
</tr>
<tr>
<td>OT Firmware Version</td>
<td>The firmware version running on an OT endpoint.</td>
<td>Host&gt;firmware_version</td>
</tr>
<tr>
<td>OT Hardware Version</td>
<td>The hardware version of an OT endpoint.</td>
<td>Host&gt;hardware_version</td>
</tr>
<tr>
<td>OT Host Name</td>
<td>The name of an OT endpoint.</td>
<td>Host&gt;main_name</td>
</tr>
<tr>
<td>OT Modules</td>
<td>Information about modules detected in an OT endpoint, by rack slot.</td>
<td>Host&gt;module_identities</td>
</tr>
<tr>
<td>OT NERC CIP Classification</td>
<td>NERC CIP classifications assigned to an endpoint. A parallel Inventory view is provided.</td>
<td>Host&gt;nerc_cip_classifications</td>
</tr>
<tr>
<td>OT Project Name</td>
<td>The project of a PLC endpoint.</td>
<td>Host&gt;project</td>
</tr>
</tbody>
</table>

Refer to SilentDefense API documentation for details of the ModuleIdentity data structure used to report this value.
<table>
<thead>
<tr>
<th><strong>OT Purdue Level</strong></th>
<th>The Purdue level of an OT endpoint. Valid values include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>▪ LEVEL0</td>
</tr>
<tr>
<td></td>
<td>▪ LEVEL1</td>
</tr>
<tr>
<td></td>
<td>▪ LEVEL2</td>
</tr>
<tr>
<td></td>
<td>▪ LEVEL3</td>
</tr>
<tr>
<td></td>
<td>▪ LEVEL35</td>
</tr>
<tr>
<td></td>
<td>▪ LEVEL4</td>
</tr>
<tr>
<td></td>
<td>▪ LEVEL5</td>
</tr>
<tr>
<td></td>
<td>▪ UNDEFINED</td>
</tr>
<tr>
<td></td>
<td>There is a parallel Track Changes property.</td>
</tr>
<tr>
<td></td>
<td>From the Command Center API field: Host&gt;purdue_level</td>
</tr>
<tr>
<td><strong>OT Serial Number</strong></td>
<td>The serial number of an OT endpoint.</td>
</tr>
<tr>
<td></td>
<td>From the Command Center API field: Host&gt;serial_number</td>
</tr>
<tr>
<td><strong>OT Vulnerabilities</strong></td>
<td>Vulnerabilities that were detected on an OT endpoint. The database includes known CVEs and detailed CVSS information.</td>
</tr>
<tr>
<td></td>
<td>From the Command Center API field: Host&gt;cves</td>
</tr>
<tr>
<td></td>
<td>There is a parallel Track Changes property.</td>
</tr>
<tr>
<td></td>
<td>Refer to SilentDefense API documentation for details of the HostCVEInfo data structure used to report this value.</td>
</tr>
<tr>
<td><strong>Server Protocols</strong></td>
<td>The application-level communications protocols accepted by an OT endpoint to establish a communications stream.</td>
</tr>
<tr>
<td></td>
<td>From the Command Center API field: Host&gt;server_protos</td>
</tr>
</tbody>
</table>
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.

![Hostname](image)

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.

![User configuration](image)

Recommended password length is at least 10 characters, with mixed lowercase 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.

![Encryption of home directory](image)

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.

![Timezone](image)

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:


b. 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.

c. 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

a. 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
I. 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”
I. 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:


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).