FORESCOUT

Operational Technology Module 1.3.1

Release Notes

# Supporting Operational Technology Endpoints in Forescout

As IT (Information Technology) and OT (Operational Technology) networks converge, challenging new operational and safety cyber risks arise.

The solution described in this document improves Forescout's visibility and control of OT and industrial networks, as well as IoT intensive 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, IoT, and OT devices.

## Components

The following components provide enhanced visibility of Operational Technology environments in the Forescout platform:

- Sensors

  Each 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 Sensors are packaged in modules that can be selectively enabled. A dedicated monitoring interface sends events and logs from the 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.

🗎 *In this release, Forescout interacts with only one Command Center instance.*

### 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 Sensors in two ways:

- Multi-CC support are hosted on a Forescout Appliance.
- *Standalone Sensors* are installed on a certified hardware server.

# What's New

This section describes new or enhanced features in this release.

## Operational Technology Module 1.3.1

### eyeSight 8.2.1 compatibility

The OT Module 1.3.1 release contains a compatibility update required to support eyeSight 8.2.1.

### Module Compatibility

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.

## Operational Technology Module 1.3.0

### Multi-CC support

There are many cases where having multiple OT Command Centers is preferable. It is now possible to connect multiple Command Centers to one Operational Technology module Enterprise Manager, allowing for smooth integration between eyeSight and SilentDefense across all Command Centers.

See the *Operational Technology Module Configuration Guide* for more information.

### OT Risk Score

The OT Security and Operational Risk Scores for assets detected by SilentDefense is now made available to eyesight through the Operational Technology Module. It works out of the box when updating to version 1.3.0, without any additional configuration.

## eyeSegment support

Integration between eyeSegment and OT is possible when connecting the Operational Technology module to SilentDefense version 4.1.2. An OT Monitoring Sensor setting is required for the eyeSegment integration to work: Add the following line to *“/opt/nids/conf/nids.conf” and restart the sensor*.

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

See the *Operational Technology Module Configuration Guide for more details.*

## UI Update for Certificate Export

The Add Command Center wizard no longer contains the option to overwrite the OT Command Center certificates. This option is now available on the Edit Command Center page, under the “Certificate Issues” tab.

## Module Compatibility

Operational Technology module version 1.3.0 is compatible with CounterAct 8.2.0 (8.2.0 build 1565 and up, and 8.2.0.2) and SilentDefense version 4.1.1 or 4.1.2.

For CounterAct 8.2.1 versions, please use the Operational Technology module version 1.3.1 instead.

Integration of OT for eyeSegment is optional. To enable eyeSegment support, required versions are counterAct 8.2.0.2 and SilentDefense 4.1.2.

# Deployment Scenarios

The following deployments are supported:

- New/Upgrade Deployment of OT Support in Forescout

  To introduce support for OT endpoints in your Forescout environment, install the components provided in this release as described in the *Operational Technology Module Configuration Guide*. If you already run Forescout OT components in your environment, upgrade to this release as described in Upgrade Procedures.

- Integrated OT Support with an Existing SilentDefense Deployment

  In this scenario, Forescout OT components interact with components of an existing SilentDefense deployment. For example, a SilentDefense Command Center instance can manage Sensors hosted by Forescout, and can report information to the Forescout Operational Technology Module. To upgrade components of an existing SilentDefense deployment, refer to SilentDefense product documentation.

# Upgrade Procedures

This section describes how upgrade Forescout OT components to this release from a previous release. See the *Operational Technology Module Configuration Guide* for detailed first-time installation procedures.

🗎 *To upgrade SilentDefense components, see SilentDefense 4.1.1 documentation and the SilentDefense 4.1.2 release notes.*

## Upgrade the Operational Technology Module

🗎 *When you upgrade the Operational Technology Module, integrated Sensors on Forescout devices are also upgraded.*

🗎 *To ensure connectivity between the OT module and the OT Command Center can be established, please ensure that the OT module runs on the EM, and that the EM is the first to be updated to the new version.*

**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.

1. Download the module `.fpi` file.
2. 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 the Operational Technology Module and select **Stop**. Stop the module on Enterprise Manager and all Appliances.
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 will not proceed if you do not agree to the license agreement.

   🗎 *The installation will begin 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.

## Upgrade Command Center

🗎 *A new license is required for the upgraded Command Center. Existing license files are incompatible with this release. Obtain a new license before you upgrade.*

**To upgrade an Command Center:**

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 upgrade package. Unpack the archive.
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. Enter the following command to run SQL database updates:

   sudo -u postgres psql -d silentdefense -f fix-db-counteract-3131.sql
8. Use a command like **sudo ./** *<filename>* to run the update installer **update_os….run** provided in the update package. The script updates core operating system packages to the versions available at the specified date.

   Reboot the server when prompted.

9. Start the OT Command Center updater **`commandcenter_<version>_update….run`** provided in the update package.
10. Reboot the server.

## Upgrade Standalone Sensors

Use the Update manager hosted by Command Center to update groups of Sensors.

**To upgrade standalone Sensors:**

To update Monitoring Sensors, execute the following steps. Repeat this for every Monitoring Sensor.

1. Log in using SSH as the silentdefense user.
2. Verify the required files are present by issuing the following command to list the contents of the current directory:
   ```
   $ ls -alh
   ```
3. Ensure the installers are marked executable by issuing the following command:
   ```
   $ chmod a+x *.run
   ```
4. Update the server environment by issuing the following command:
   ```
   $ sudo ./os provisioning 4.1.1 update.run
   ```

5. After the OS provisioning has finished, issue a reboot of the system:

   ```
   $ sudo reboot
   ```

6. Run the update installer by issuing the following command:

   ```
   $ sudo ./sensor 4.1.1 update.run
   ```

7. After the Monitoring Sensor is updated, issue a reboot of the system:

   ```
   $ sudo reboot
   ```

8. The update script automatically checks if the Monitoring Sensor is running and stops it if necessary, after which it will install the new version of the Monitoring Sensor.

# Fixed Issues

| | |
|---|---|
| **OTSM 1.3.1** | • Not applicable. This release provides eyeSight 8.2.1 compatibility only. |
| **OTSM 1.3.0** | • Fixed an issue that caused protocols other than L7 protocols to be missing from eyesight. (OT-577) |
| **OTSM 1.2.1** | • Fixed an issue that caused Analytics stop working after applying the update to OTSM 1.2.0.<br>• Fixed an issue that caused Analytics to stop working after deploying new certificates via the OTSM plugin.<br>• Fixed an issue that prevented OTSM to connect to SilentDefense after user credentials were changed on the Command Center. |
| **OTSM 1.2.0** | • There are no fixed issued in this release. |

# Known Issues

The following table lists known issues in this release.

| Issue | Description |
|---|---|
| **OT-333** | When OT endpoints are reassigned between Forescout Appliances, this may change their classification as OT endpoints and delay update of OT endpoint properties. |
| **OT-578** | Hosts Number shown in EM decreasing almost immediately after increasing the number based on the polling of OTSM plugin |
| **PE-934** | Sensors are not displayed in "Update Sensor Scripts" when Traffic Inspection Library was installed in an environment with OT 1.2.1 Plugin |
| **OT-579** | Incorrect information shown by OT Plugin when accessing the FS Console for a FS Appliance |
| **OT-597** | Connectivity between the OT plugin and the Command Center can fail when the following two conditions are not met: The EM must run the OTSM plugin, and the EM must be the first to be upgraded to the latest version. |
| **OT-615** | The Operational Technology Module does not support Appliance Group Fail-over. If the focal appliance disconnects from the EM, it needs to be reconnected manually. |

## 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 Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

## Legal Notice

2020-07-06 18:27