FORESCOUT

Forescout

Traffic Inspection Library

Configuration Guide

Version 20.0.2

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

2020-02-10 11:05

Table of Contents

About the Traffic Inspection Library

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.

Install the latest version of the Traffic Inspection Library to take advantage of the most current scripts.

Install this module only when the Operational Technology module is installed, and Sensors and other SilentDefense components are deployed in the network.

This release of the Traffic Inspection Library enhances detection of these equipment/endpoint types:

Healthcare

The library includes parsers for a number of healthcare specific protocols, and enhances the granularity of Forescout classification of healthcare devices.

Forescout Requirements

This module requires the following Forescout releases and other components:

- Forescout version 8.2
- Operational Technology Module version 1.2.0
- SilentDefense components running release 4.0.1

Installation

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.*

Configuration

No module configuration is required.

Update Scripts on Sensors

When you install a new release of the Traffic Inspection Library, updated inspection scripts are distributed to Sensors that run a different version of the scripts. However, some Sensors may be unavailable during distribution of updates. Use this procedure to manually update scripts on Sensors.

- *Only scripts with filenames identical to the files in the Library are updated. To exclude a customized script file from update, change its file name.*

To distribute updated scripts to Sensors:

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

   - *Current releases of the Operational Technology Module support a single Command Center.*

2. Select **Sensor Scripts**. The *Scripts Status* dialog shows the scripts used by each Sensor of the selected Command Centers.
   - When a Sensor uses the scripts provided by the installed Traffic Inspection Library, its status is *Up to date*.
   - When a Sensor uses another version of Traffic Inspection scripts, its status is *Update required*.
3. Select **Update Scripts** to distribute the most recent Traffic Inspection scripts to all the Sensors that require update. Older scripts are overwritten.

Additional CounterACT 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 Technical Documentation 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 Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:

- Go to https://www.Forescout.com/company/technical-documentation/

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 Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will

only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support 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 quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

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

Documentation Portal

- Select **Documentation Portal** from the **Help** menu to access the Documentation Portal.