



Fore Scout

Core Extensions Module: Flow Analyzer Plugin

Configuration Guide

Version 1.4.1



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 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

© 2019 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.

2019-02-27 18:40

Table of Contents

- About the Flow Analyzer 4**
 - How It Works.....4
- Forescout Software Requirements 5**
- Configure the Sharing of Anonymized Flow Data Statistics 5**
 - Enable Flow Analyzer Data Sharing5
 - Configure the Flow Analyzer6
 - Verify That the Plugin Is Running8
- Test the Configuration..... 8**
- Core Extensions Module Information 8**
- Additional Forescout Documentation..... 9**
 - Documentation Downloads **Error! Bookmark not defined.**
 - Documentation Portal **Error! Bookmark not defined.**
 - Forescout Help Tools..... **Error! Bookmark not defined.**

About the Flow Analyzer

The Flow Analyzer Plugin is a component of the Forescout® Core Extensions Module. See [Core Extensions Module Information](#) for details about the module.

The Flow Analyzer Plugin detects flow information regarding the endpoints in your environment. It collects a statistical sampling of data about the network traffic in your environment, such as average packet size, average packet rate per second, inbound and outbound bandwidth usage, and DNS resolutions.

Forescout researchers continually attempt to provide better classification and posture assessment services to customers. Customers who opt to allow the anonymous information detected by the Flow Analyzer in their environments to be shared with Forescout provide an important contribution to the Forescout Research and Intelligent Analytics Program. For more information about the program, see *Data Sharing for the Forescout Research and Intelligent Analytics Program* in the Forescout Administration Guide.

By default, after you accept the Forescout Research and Intelligent Analytics Program participation terms, your CounterACT devices share selected endpoint properties with Forescout. The purpose of the Flow Analyzer is to provide additional properties to be shared with Forescout. Properties resolved by the Flow Analyzer are not available to Forescout users from the Policy Manager.

The Forescout Research and Intelligent Analytics Program is a voluntary program. Customers are under no obligation to share their data to help Forescout improve classification. The Forescout Research and Intelligent Analytics Program and the Flow Analyzer provide no immediate benefits to an individual customer. In the long term, the program benefits customers in the form of more precise classification profiles.

How It Works

If additional property creation is enabled in your Flow Analyzer configuration, the following happens:

1. Network traffic data statistics are continuously collected and converted to hidden properties. The statistics are collected from two sources:
 - Routers and switches that export NetFlow traffic that is analyzed by either the Forescout NetFlow Plugin or the Forescout Flow Collector (if installed and configured)
 - SPAN traffic, which is converted to NetFlow protocol by the Flow Analyzer

For the complete list of created properties, refer to Appendix I of the *Forescout Research and Intelligent Analytics Program Data Security Document*.

2. If [data sharing is enabled](#):
 - a. All personally identifiable information (PII) is removed from the network traffic data statistics properties. The IP and MAC addresses of endpoints are converted to simulated addresses using a one-way function which ensures that the data can never reveal the actual addresses of endpoints in your network. For more information, see the *Forescout Research and Intelligent Analytics Program Data Security Document*.

- b. Managed CounterACT Appliances transmit the properties through the Enterprise Manager for upload to the Forescout Research and Intelligent Analytics Program.

Forescout Requirements

The Flow Analyzer requires the following:

- Forescout version 8.1
- It is recommended to have the Forescout Flow Collector installed and running

Configure the Sharing of Anonymized Flow Data Statistics

By default, the Flow Analyzer is not enabled. To enable the creation and sharing of anonymized flow data statistics with Forescout, do the following:

1. [Enable Flow Analyzer Data Sharing](#)
2. [Configure the Flow Analyzer](#)

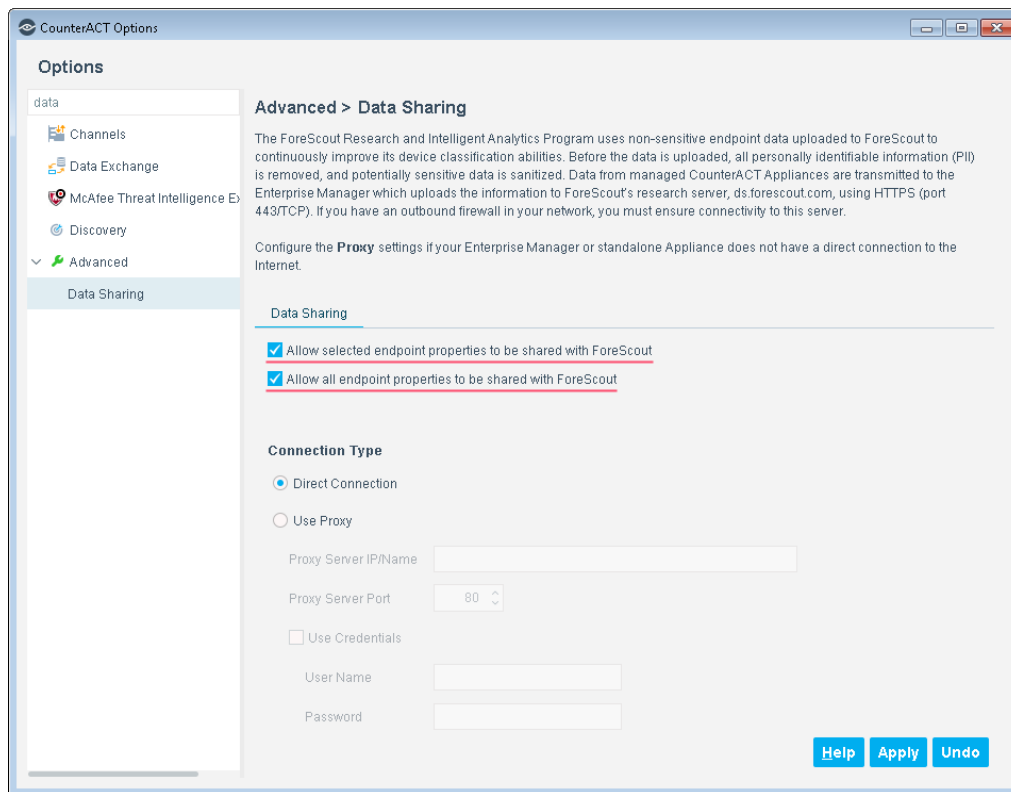
Enable Flow Analyzer Data Sharing

Configure the Data Sharing option for sharing properties with Forescout. For more information, see *Data Sharing for the Forescout Research and Intelligent Analytics Program* in the Forescout Administration Guide.

To enable data sharing of properties, including those created by the Flow Analyzer:


1. In the Forescout Console, select **Options** from the **Tools** menu. The Options dialog box opens.

2. Select **Advanced > Data Sharing**.



3. Select both checkboxes:

- **Allow selected endpoint properties to be shared with Forescout**
This allows basic data sharing.
- **Allow all endpoint properties to be shared with Forescout**
This allows the sharing of endpoint properties created by the Flow Analyzer.

 *Data sharing can be enabled only if you accept the Forescout Research and Intelligent Analytics Program participation terms. To read the terms, select the **Allow selected endpoint properties to be shared with Forescout** checkbox.*

Configure the Flow Analyzer

Configure the Flow Analyzer to create properties based on anonymized network traffic data statistics. The following options are available:

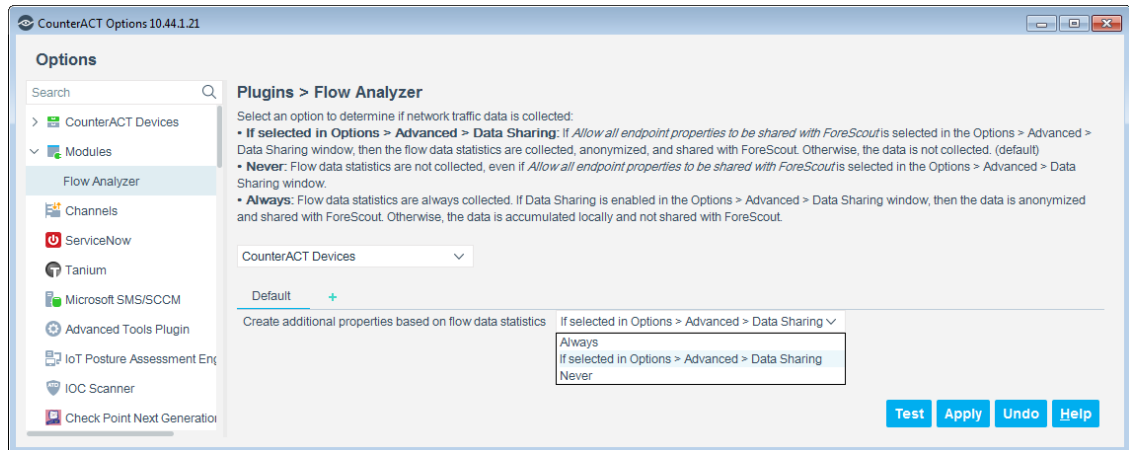
- Always collect network traffic data statistics and create the hidden properties. Share the properties with Forescout if data sharing is enabled.
- (Default) If the **Allow all endpoint properties to be shared with Forescout** option is selected in the Options > Advanced > Data Sharing window, do the following:

- a. Collect network traffic data statistics.
 - b. Create the hidden properties.
 - c. Share the properties with Forescout.
- Never collect network traffic data statistics for creating additional properties.

By default, the settings defined for the Flow Analyzer are applied to all CounterACT devices. You can create separate configurations for individual devices or for groups of devices. See *Configuring Features for an Appliance or Group of Appliances* in the Forescout Administration Guide.

To configure the Flow Analyzer:

1. In the Forescout Console, select **Options** from the **Tools** menu.
2. In the navigation pane, select **Modules > Flow Analyzer**. The Flow Analyzer configuration pane opens.



3. Select an option to determine if the additional properties are created.

Always	Anonymized flow data statistics are always used for creating additional properties. If Data Sharing is enabled in the Options > Advanced > Data Sharing window, then the properties are shared with Forescout. Otherwise, the data is collected locally and the properties are not shared with Forescout.
If selected in Options > Advanced > Data Sharing	If the Allow all endpoint properties to be shared with Forescout option is selected in the Options > Advanced > Data Sharing window, then anonymized flow data statistics are used for creating properties that are shared with Forescout. Otherwise, the network traffic data is not collected. This is the default option.
Never	Flow data statistics are never collected, even if the Allow all endpoint properties to be shared with Forescout option is selected in the Options > Advanced > Data Sharing window.

4. Select **Apply** to save the configuration.
5. Select **Test** to test the configuration on one or more CounterACT devices, and select **OK**.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

1. Select **Tools > Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Test the Configuration

To test that the Flow Analyzer receives network traffic data, do one of the following:

- To test the configuration of all devices, in the Options > Modules pane, select **Core Extensions > Flow Analyzer** and select **Test**.
- In the Flow Analyzer configuration pane, select **Test** and specify the devices you want to test.

During the test, the Flow Analyzer listens for network traffic data for several seconds. The test fails if:

- Property creation from flow data statistics is not enabled.
- No network traffic data is detected.

Core Extensions Module Information

The Flow Analyzer Plugin is installed with the Forescout Core Extensions Module.

The Forescout Core Extensions Module provides an extensive range of capabilities that enhance the core Forescout solution. These capabilities enhance detection, classification, reporting, troubleshooting and more. The following components are installed with the Core Extensions Module:

Advanced Tools Plugin	Dashboard Plugin	NBT Scanner Plugin
CEF Plugin	Device Classification Engine	Packet Engine
DHCP Classifier Plugin	External Classifier Plugin	Reports Plugin
DNS Client Plugin	Flow Analyzer Plugin	Syslog Plugin
DNS Enforce Plugin	Flow Collector	Technical Support Plugin
DNS Query Extension Plugin	IOC Scanner Plugin	Web Client Plugin
	IoT Posture Assessment Engine	

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation.

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](#), or 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 will 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.

- *If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.*

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

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 **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, 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).