ForeScout CounterACT®

Core Extensions Module: Flow Analyzer Plugin

Configuration Guide

Version 1.4

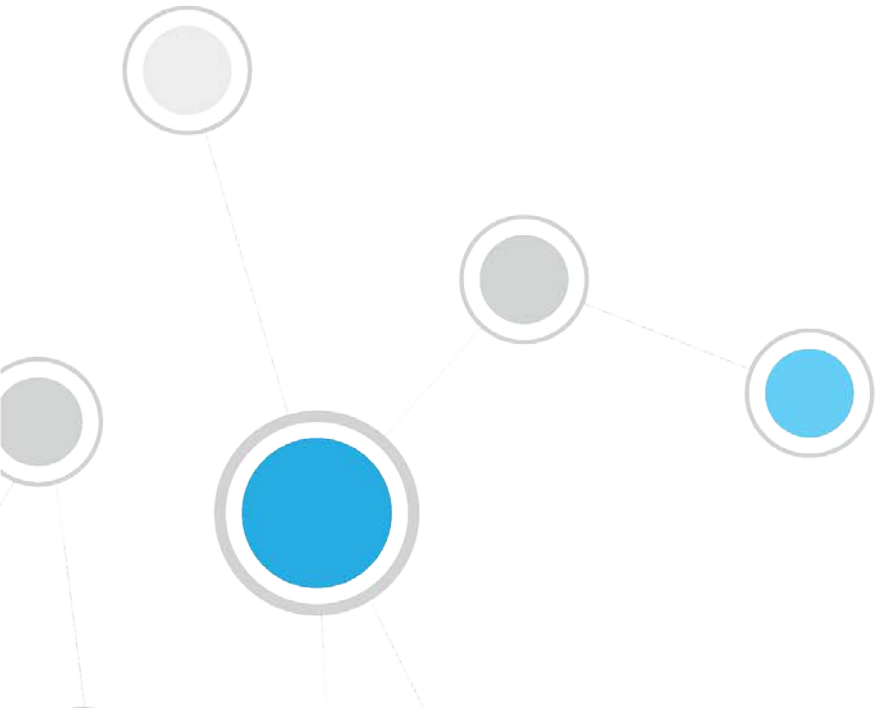


Table of Contents

About the Flow Analyzer

The Flow Analyzer Plugin is a component of the ForeScout CounterACT® Core Extensions Module. See Core Extensions Module Information for details about the module.

The CounterACT Flow Analyzer 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 CounterACT 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 CounterACT 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 processed by the CounterACT NetFlow Plugin (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.

CounterACT Software Requirements

The Flow Analyzer requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0
- An active Maintenance Contract for CounterACT devices
- It is recommended to have the NetFlow Plugin 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:

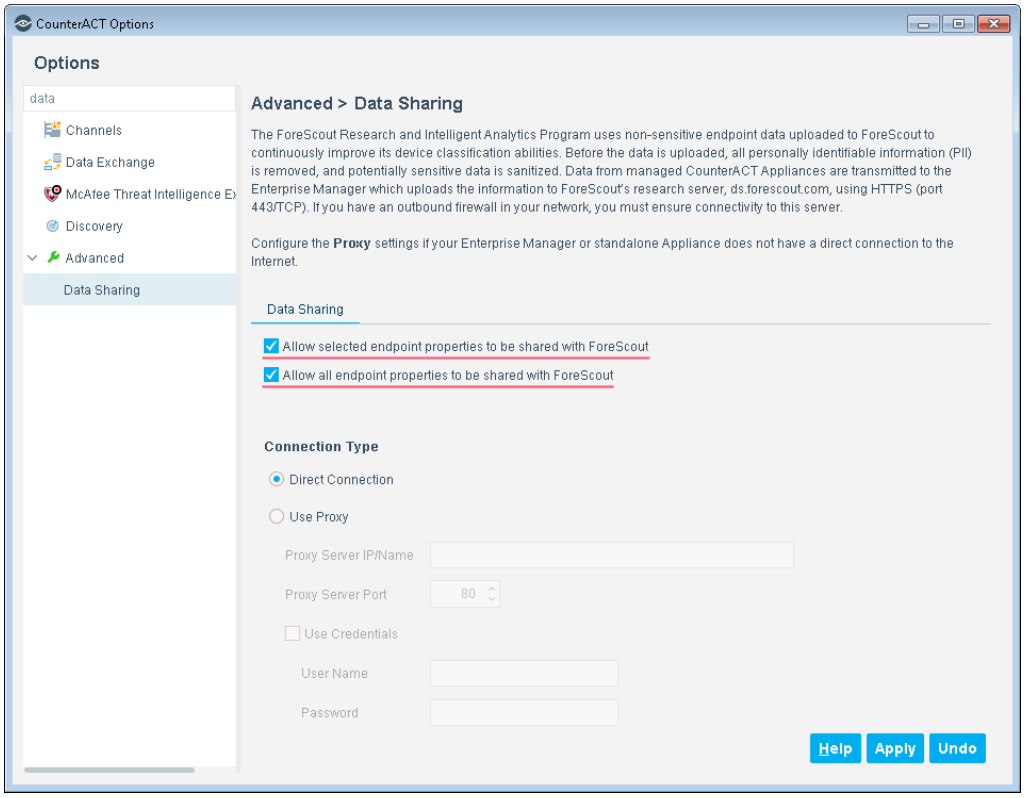
1. Enable Flow Analyzer Data Sharing
2. Configure the Flow Analyzer

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 CounterACT Administration Guide.

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

1. In the CounterACT 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.

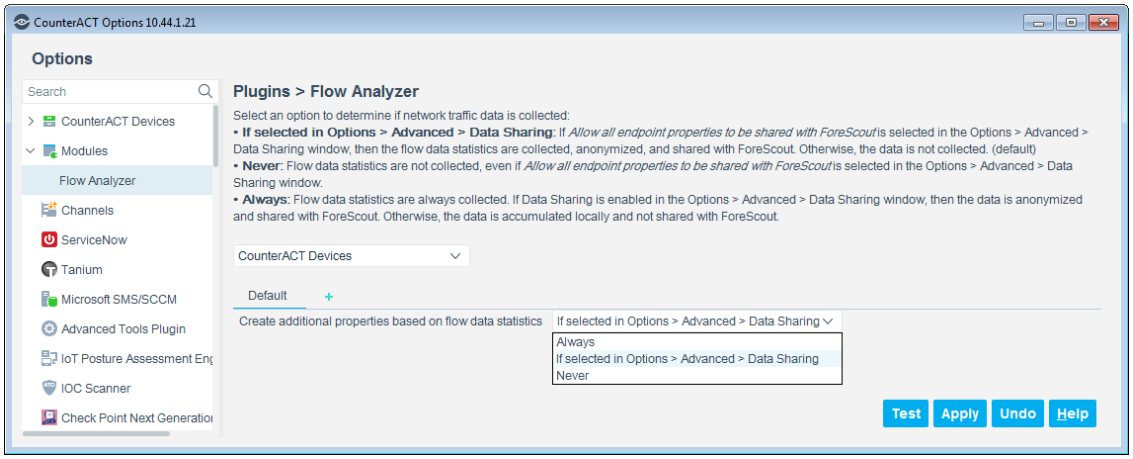
c. Share the properties with ForeScout.

- 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 CounterACT Administration Guide.

To configure the Flow Analyzer:

1. In the CounterACT 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 CounterACT Core Extensions Module.

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

- Advanced Tools Plugin
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
- IOC Scanner Plugin
- IoT Posture Assessment Engine
- NBT Scanner Plugin

- NetFlow Plugin
- Reports Plugin
- Syslog Plugin
- Technical Support Plugin
- Web GUI Plugin

The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are released and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Guide* for more module information, for example module requirements, upgrade and rollback instructions. See Additional CounterACT Documentation for information about how to access the module guide.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

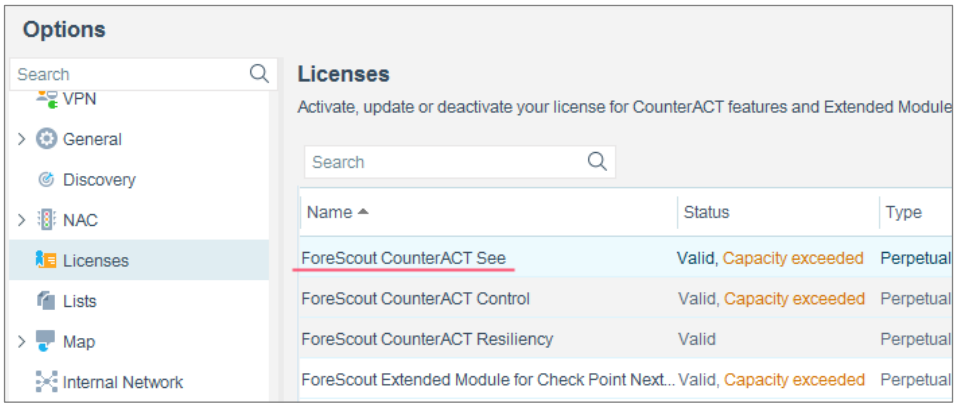
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21