ForeScout CounterACT®

Core Extensions Module: NetFlow Plugin

Configuration Guide

Version 1.2

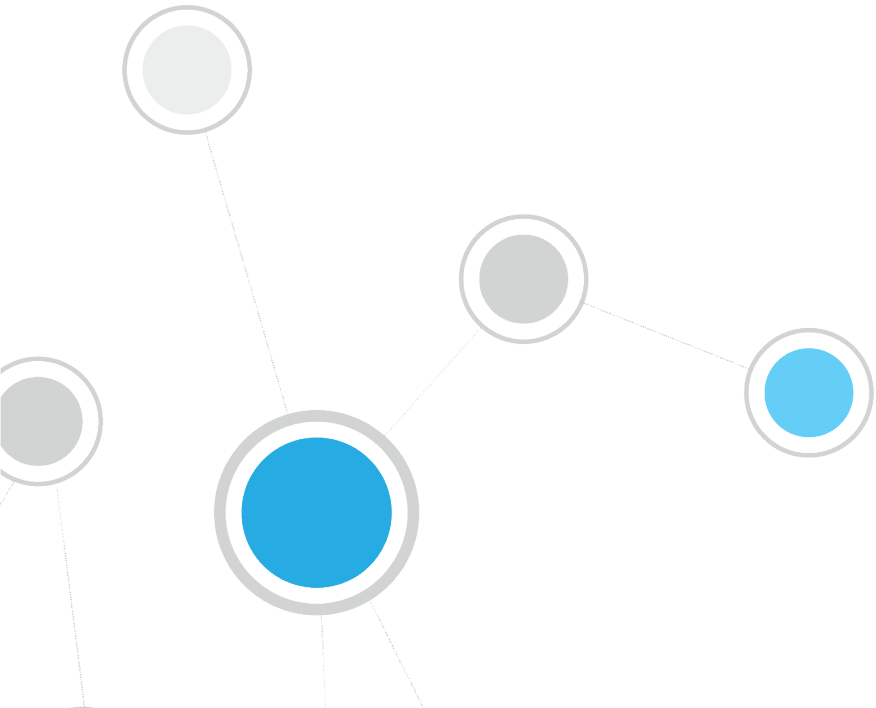


Table of Contents

About NetFlow Integration

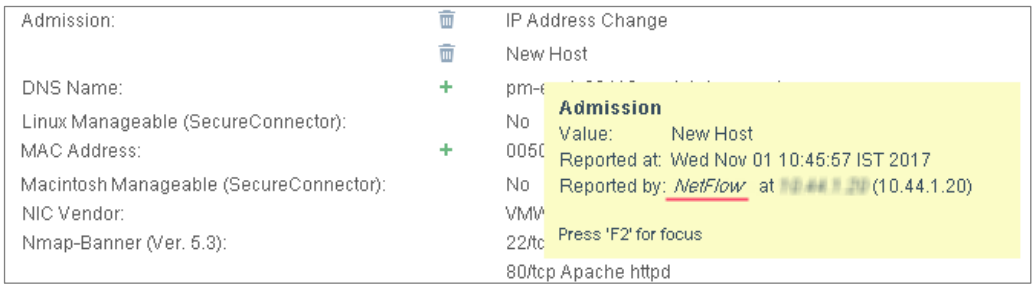
The NetFlow Plugin is a component of the ForeScout CounterACT® Core Extensions Module. See Core Extensions Module Information for details about the module.

This plugin integrates the NetFlow reporting protocol with CounterACT.

NetFlow is a widely supported protocol that allows switches and routers to capture and report IP network traffic statistics.

The plugin listens to NetFlow data streams and analyzes them to detect endpoints or endpoint property values that the CounterACT Packet Engine might not learn.

This capability becomes more relevant in large scale deployments, where the CounterACT packet engine is limited in its ability to detect activity in remote sites and branch offices. Use of information reported by NetFlow improves visibility and speeds detection of new endpoints.



How it Works

The NetFlow Plugin audits data from any of the following NetFlow sources:

- *Flow Exporters* - switches and routers in the network that report NetFlow data.
- *Flow Collector* - in larger networks, a server or load-balanced cluster that is used as a *Flow Collector* for centralized reporting of NetFlow data.

The plugin filters the information and applies heuristic logic to detect endpoints and to report endpoint property information.

Supported NetFlow Versions

The plugin supports communication using NetFlow v5 and v9.

What to Do

This section describes steps you should take to integrate with NetFlow:

1. Verify that you have met system requirements. See Requirements.
2. Configure relevant network devices that are NetFlow exporters or collectors to send NetFlow data to CounterACT.
3. Configure the Plugin.

4. Create Custom Policies.

Requirements

This section describes system requirements, including:

- CounterACT Requirements
- Networking Requirements

CounterACT Requirements

The plugin requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0.
- An active Maintenance Contract for CounterACT is required.

Networking Requirements

The NetFlow data link uses the UDP communication protocol.

The NetFlow protocol should be enabled on Layer 3 network devices in network segments that are of interest. Flow Exporters and/or load-balanced Flow Collectors in these segments must be configured to report NetFlow data to the CounterACT Appliances that monitor the segments.

The port used to communicate with the NetFlow server or load balancer must be open on enterprise firewalls to support NetFlow data communication to CounterACT. Specify this port when you configure the plugin. The default is 2055/UDP.

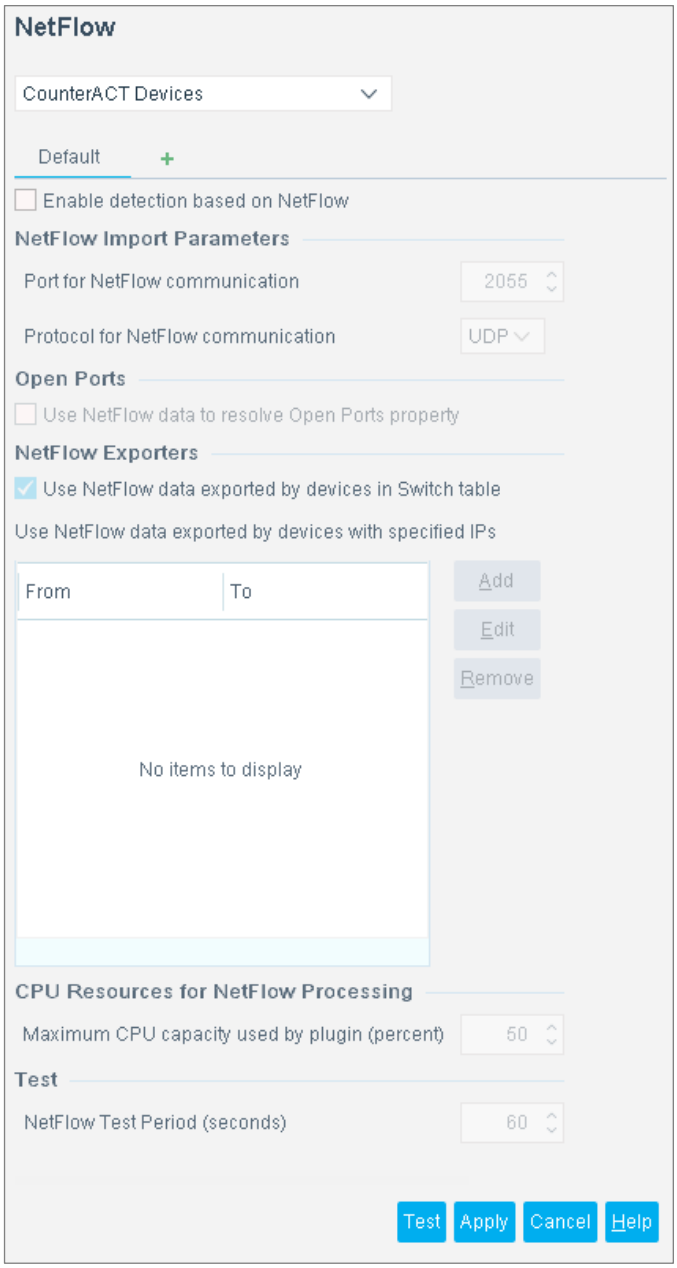
In addition, define exceptions to the Virtual Firewall action for this port.

Configure the Plugin

By default, the settings defined for the plugin are applied to all Appliances. You can create separate configurations for each Appliance or for groups of Appliances. For example, you can define different NetFlow traffic sources for different segments of the network. See Per-Appliance Configuration.

To configure the plugin:

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Select **Modules**.
3. In the Modules pane, select the NetFlow plugin and select **Configure**. The NetFlow configuration pane appears.



4. By default, the plugin is not enabled. To use the functionality of the plugin, select the **Enable detection based on NetFlow** checkbox.

   Typically the plugin runs only on designated Appliances that audit and process NetFlow data.

5. In the NetFlow Import Parameters section, define the port and protocol CounterACT uses to receive NetFlow traffic.

6. In the Open Ports section, select the **Use NetFlow data to resolve Open Ports property** checkbox to enable reporting of open ports. When this option is selected, the plugin adds open ports that it has detected for an endpoint to the Open Ports property.

7. In the NetFlow Exporters section, define filters that the plugin applies to received NetFlow data.
   - To use switches and network devices managed by the Switch Plugin as NetFlow data sources, select the **Use NetFlow data exported by devices in the Switch Table** checkbox
   - To specify IP addresses of NetFlow data sources, select **Add** and define a range of IP addresses. You can define multiple ranges. For example, define all the IP addresses of a load-balanced Flow Collector cluster as NetFlow data sources.

   The plugin only analyzes NetFlow information that was reported by the specified data sources. Other NetFlow data is not analyzed.

   A logical OR links these filters: if you use both filters simultaneously. NetFlow data is analyzed for devices in the Switch Plugin pane, even if their IP addresses are not in the specified ranges, and data from devices with the specified IP addresses is also analyzed, even if they do not appear in the Switch Plugin table.

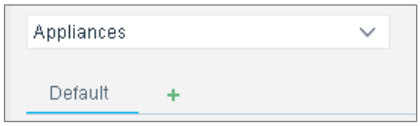
8. In the CPU Resources for NetFlow Processing section, specify the maximum percentage of Appliance processing capacity that can be used by this plugin.

   This percentage is mapped downward to the number of CPUs on the machine. For example, if you specify 75 percent of processing resources:
   - On a machine with two CPUs the maximum resource usage is one CPU.
   - On a machine with four CPUs the maximum resource usage is three CPUs.

9. In the Test section, specify the time period that the plugin waits to identify NetFlow traffic during plugin testing, in seconds.
10. Select **Apply** to save configuration changes.

Per-Appliance Configuration

The configuration settings of the Default tab are applied to the Enterprise Manager. By default these settings are also applied to all Appliances.

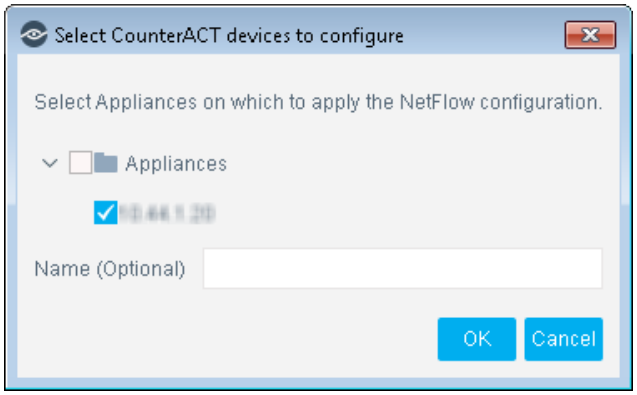


You can create and apply plugin configurations for individual Appliances, or for a group of Appliances.

To create configuration settings for an Appliance or group of Appliances:

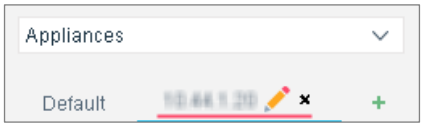
1. Select the Plus (+) tab 

. The *Select CounterACT devices to configure* dialog box appears.

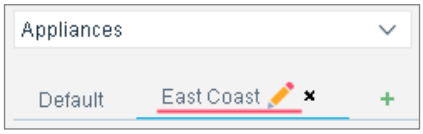


2. Do one of the following:

   – Select one Appliance and select **OK**. A configuration tab appears for the Appliance you selected.



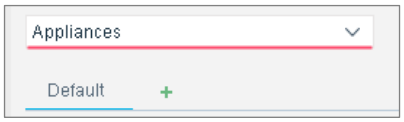
   – Select several Appliances and enter a name in the **Name (Optional)** field. Select **OK**. A configuration tab appears for the group you created.



3. Edit the configuration. Settings in the tab are applied to the selected Appliance or Appliances.

   If you delete the configuration, the settings of the Default tab are applied to the Appliance or Appliances.

When several configuration groups have been defined, it may be difficult to remember which settings apply to a specific Appliance. Select the Appliance from the Appliances drop-down. The tab with relevant configuration settings is selected.



Verify That the Plugin Is Running

After installation, verify that the plugin 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 Plugin

To test that the plugin receives NetFlow data using the configured communication and filter settings, do one of the following:

- In the Modules pane, select the NetFlow plugin and select **Test**.
- In the NetFlow plugin configuration pane, select **Test** and specify the appliances you want to test.

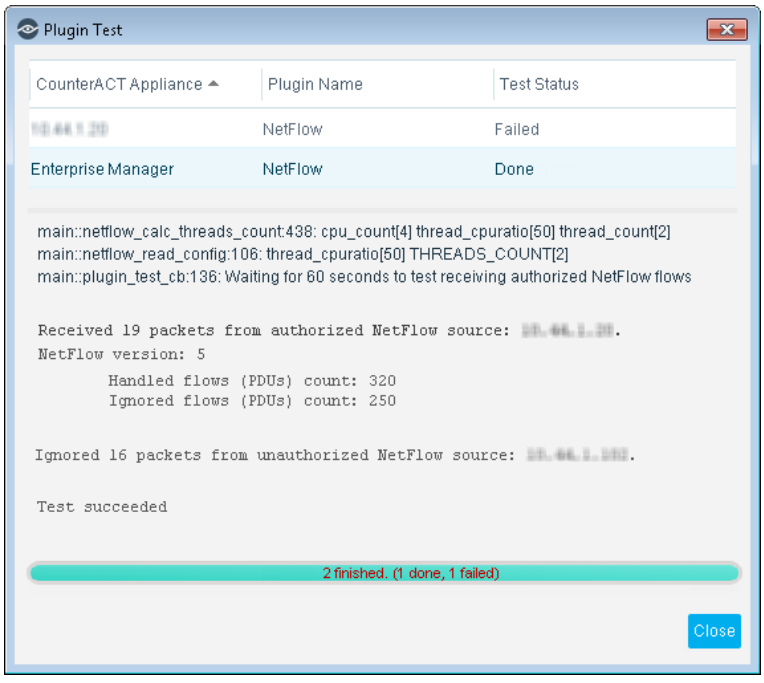
During the test, the plugin listens for NetFlow data with the configured port and protocol, and selects data from the NetFlow sources that match the configured filters. If no NetFlow data from the specified sources is detected, the test fails.

The time period of the test is determined by the **NetFlow Test Period** configuration field. See Configure the Plugin.

The test lists data flows from authorized NetFlow exporters as follows:

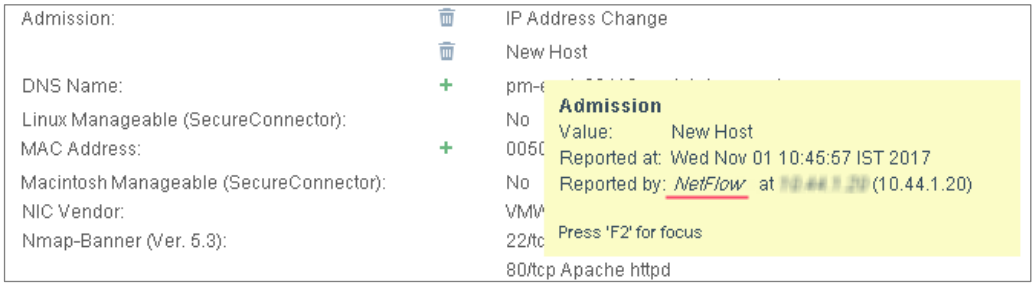
- Handled flows – data flows with port and other information that is relevant to the properties resolved by the plugin.
- Ignored flows – data flows that are not relevant to the properties resolved by the plugin.

The test fails for Appliances that are not running the plugin.



Detect New Endpoints

The plugin detects new endpoints based on NetFlow data. CounterACT endpoint admission processes and classification policies are applied to these endpoints.



Create Custom Policies

CounterACT *policies* are powerful tools for automated endpoint access control and management.

Information reported to CounterACT is stored in *property*. Property values are displayed in Console views, and can be evaluated and examined by CounterACT *policies* to trigger management and remediation *actions*.

This plugin provides new *properties* and reports information to CounterACT that is used to resolve existing properties. These properties can be included in CounterACT policies – increasing the accuracy, granularity, and reach of CounterACT policy-based management.

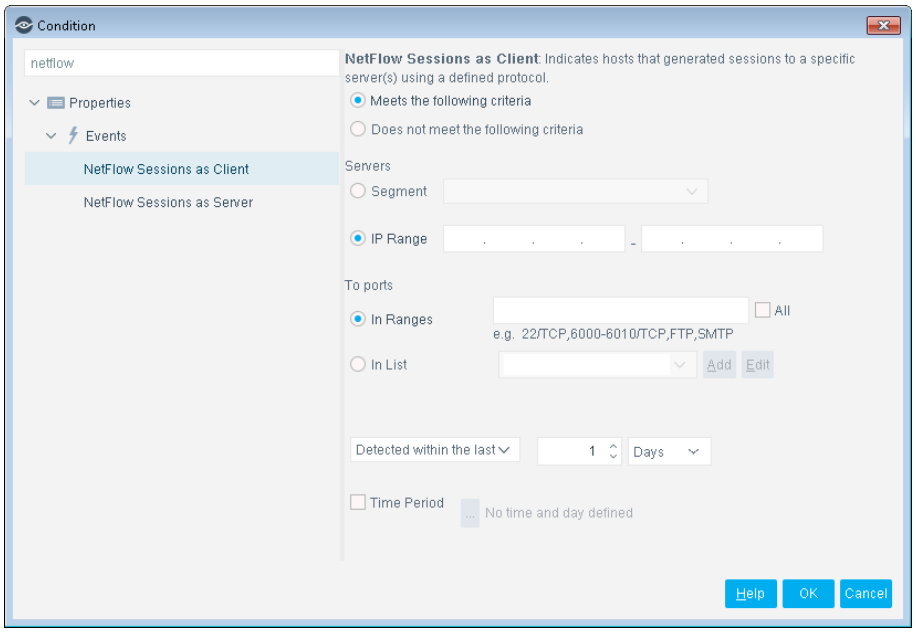
For more information about working with policies, select **Help** from the policy wizard.

To create a custom policy:

1. Log in to the CounterACT Console.
2. Select the **Policy** icon from the Console toolbar.
3. Create or edit a policy.

Properties

This section describes the properties that the installed NetFlow Plugin makes available.



To access NetFlow properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the Events folder in the Properties tree.

   The plugin provides the following properties:

Property	Description
NetFlow Sessions as Client	Indicates that an endpoint initiated a session with a server target. This session is detected based on NetFlow data reports. You can define matching conditions based on the server-side IP address port, and protocol of the session.
NetFlow Sessions as Server	Indicates that an endpoint established a session with a client. This session is detected based on NetFlow data reports. You can define matching conditions based on the client-side IP address, port, and protocol of the session.

In addition to the properties it provides, the plugin reports information for the following, existing properties based on NetFlow data:

- **Traffic Seen** property
- **Open Ports** property

The information reported by the plugin complements information from other sources that is used to resolve both the **Traffic Seen** and the **Open Ports** properties.

Core Extensions Module Information

The NetFlow 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**.

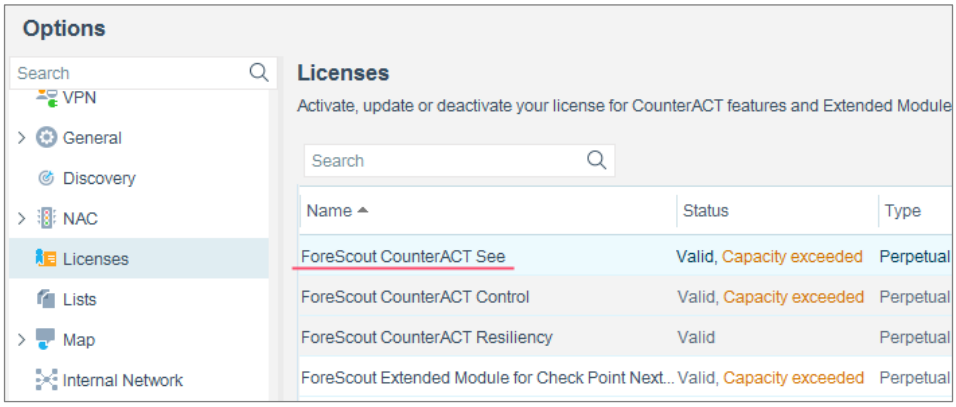
Documentation Portal

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