FORESCOUT

Forescout

Core Extensions Module: Flow Collector

Configuration Guide

Version 1.1.1

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 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

2020-07-07 17:29

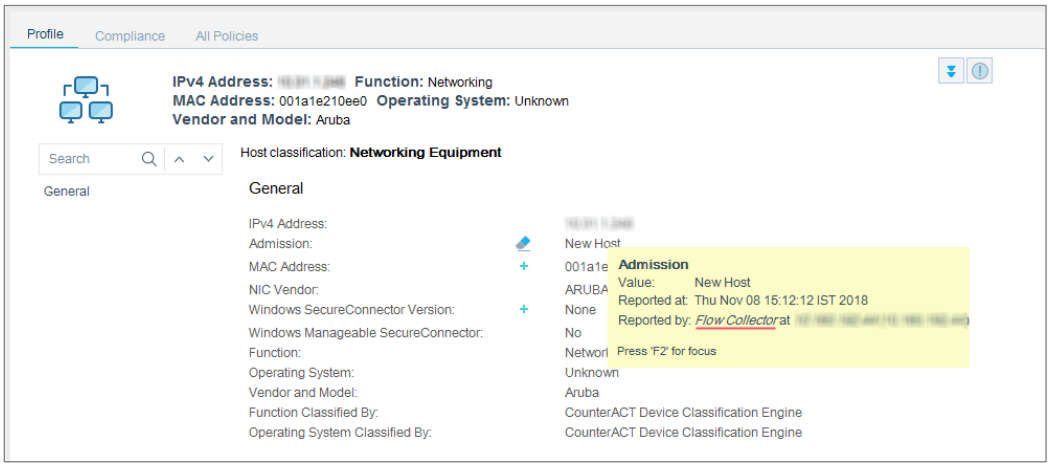
Table of Contents

About the Flow Collector

The Flow Collector is a component of the Forescout® Core Extensions Module. See Core Extensions Module Information for details about the module.

The Flow Collector analyzes the traffic flows exported by network devices, such as switches, firewalls, and routers. It reports flow session data that is used to resolve endpoint properties and that can be used to map visualized traffic patterns. The flow session data can also be used by other Forescout modules.

The Flow Collector can detect endpoints or endpoint property values that the Forescout Packet Engine might not learn. This capability is relevant in large scale deployments where the Packet Engine is limited in its ability to detect activity in remote sites and branch offices. Use of the information reported by the Flow Collector improves visibility and speeds detection of new endpoints.



How It Works

The Flow Collector audits information from switches, routers and other networks devices that report traffic flow data. It filters the information and applies heuristic logic to enable the Forescout platform to report endpoint properties and session information.

Overlapping IP Address Support

The Flow Collector supports working with networks that use overlapping IP addresses. For details about enabling and configuring the Forescout platform's support of overlapping IP address use in an enterprise's network, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access this document.

Deployment Scenarios

The Forescout platform is configured to collect traffic data in one of the following ways:

- Distributed Traffic Collection: Appliances analyze traffic for the endpoints they manage.
- Centralized Traffic Collection: One or more designated Appliances analyze the network traffic, and extract and distribute the endpoint properties and session information to the Appliances that manage the relevant endpoints.

What to Do

This section describes what to do to begin working with the Flow Collector.

1. Verify that you have met system requirements. See Requirements.
2. Configure and Test the Flow Collector.
3. Create Custom Policies. (Optional)

Requirements

This section describes system requirements, including:

- Forescout Requirements
- Supported Flow Protocols
- Networking Requirements
- Port Availability

Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Core Extensions Module 1.2.1 with the Flow Collector

Supported Flow Protocols

The Flow Collector supports the following protocols, with or without Flexible NetFlow technology:

- NetFlow v9
- IPFIX
- sFlow

- NetFlow v5

When configuring the flow data exporter, such as NetFlow, ensure that the flow records include the following information:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol
- TCP flags (recommended)

Networking Requirements

Enable the flow protocol on Layer 3 network devices in the network segments of interest. Flow exporting network devices that are in these segments must be configured to report flow data to the CounterACT device that monitors the segment.

Port Availability

To support flow data communication to the Forescout platform:

- Ensure that the communication ports are open on enterprise firewalls.
- Define exceptions for these ports in the Virtual Firewall action.

You can configure the Flow Collector port assignments. By default, the flow exporting network devices use the following ports to communicate with the Flow Collector:

- For NetFlow v9: port 4729 UDP
- For IPFIX: port 4739 UDP
- For sFlow: port 6343 UDP
- For NetFlow v5: port 9996 UDP

If the legacy NetFlow Plugin is running, ensure that it is not configured to use any of the ports used by the Flow Collector.

Configure and Test the Flow Collector

Flow Collector is installed with the Forescout platform, but it is disabled by default. After it is enabled, it produces session data that can be accessed by other components.

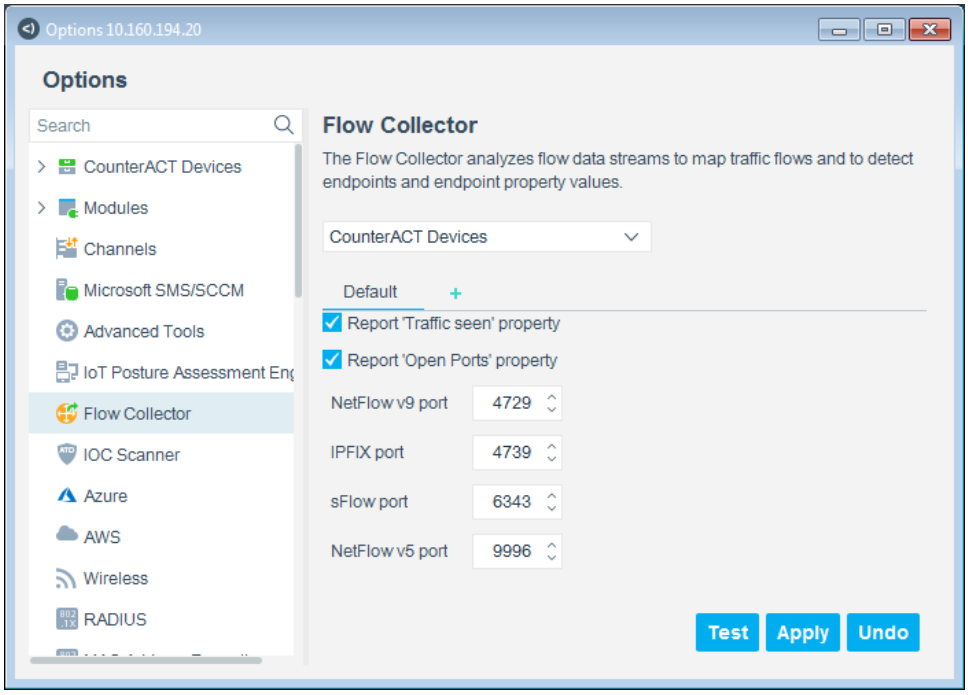
Configure the Flow Collector

In the configuration window, select:

- Properties that the Flow Collector reports
- Ports that the Flow Collector uses to communicate with network devices

To configure the Flow Collector:

1. In the Console, select **Tools** > **Options** and then select **Flow Collector**.



2. If you are configuring the Flow Collector on an Enterprise Manager, you can select specific devices for each configuration.
3. In some situations, such as when a switch is not defined to the Forescout platform, the traffic flows to or from endpoints might only be discovered by the Flow Collector and not by any other method. You can configure the Flow Collector to report properties that may otherwise not be reported:
   - **Report 'Traffic seen' property**
   - **Report 'Open Ports' property**

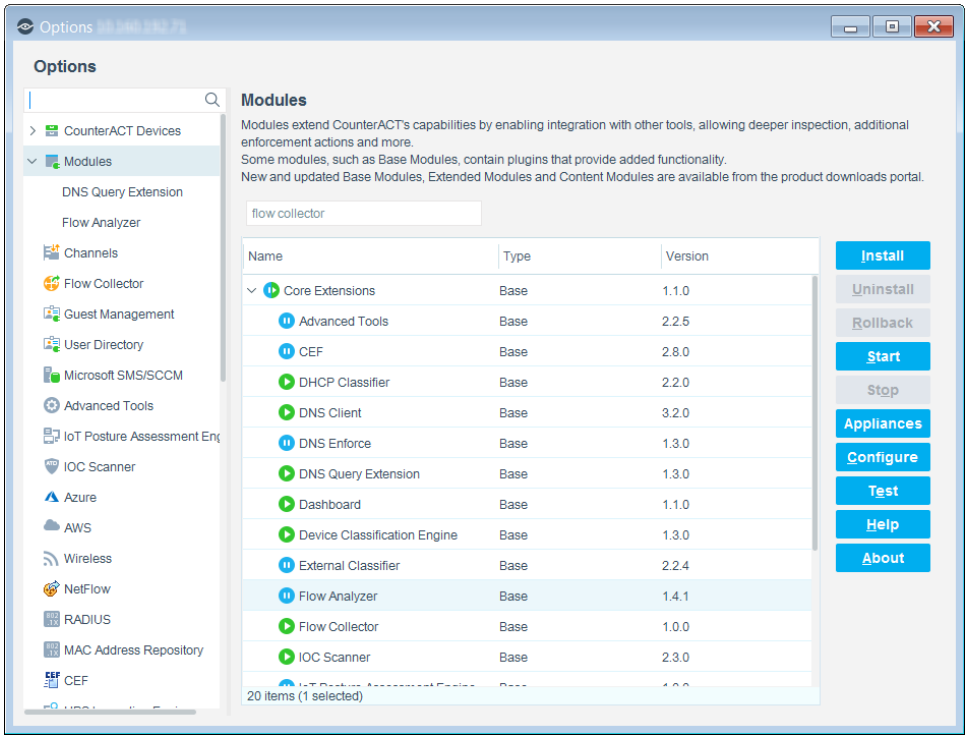
   For other properties that can be detected by the Flow Collector, see Properties Resolved When Used in Policies.
4. For each supported flow protocol version, define the port to be used by the Flow Collector for communication with network devices. See Port Availability.
5. Select **Apply** to save the configuration.

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.

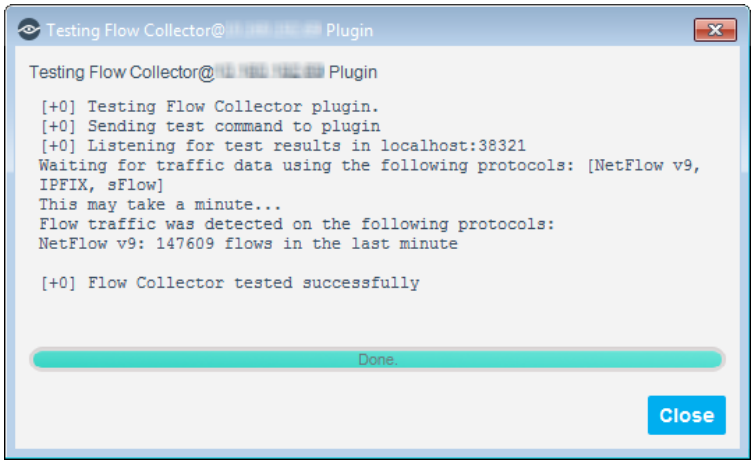


Test the Flow Collector

Test the plugin to ensure that traffic flows are detected.

To test the Flow Collector:

1. In the Options navigation pane, select **Flow Collector** and then **Test**.
2. If you are working on an Enterprise Manager, you can select specific devices for the test.
3. Run the test.



Create Custom Policies

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

Information reported to Forescout 8.1 is stored in a *property*. Property values are displayed in Console views, and can be evaluated and examined by Forescout *policies* to trigger management and remediation *actions*.

The Flow Collector reports information to Forescout 8.1 that is used to resolve existing properties. These properties can be included in Forescout policies – increasing the accuracy, granularity, and reach of policy-based management.

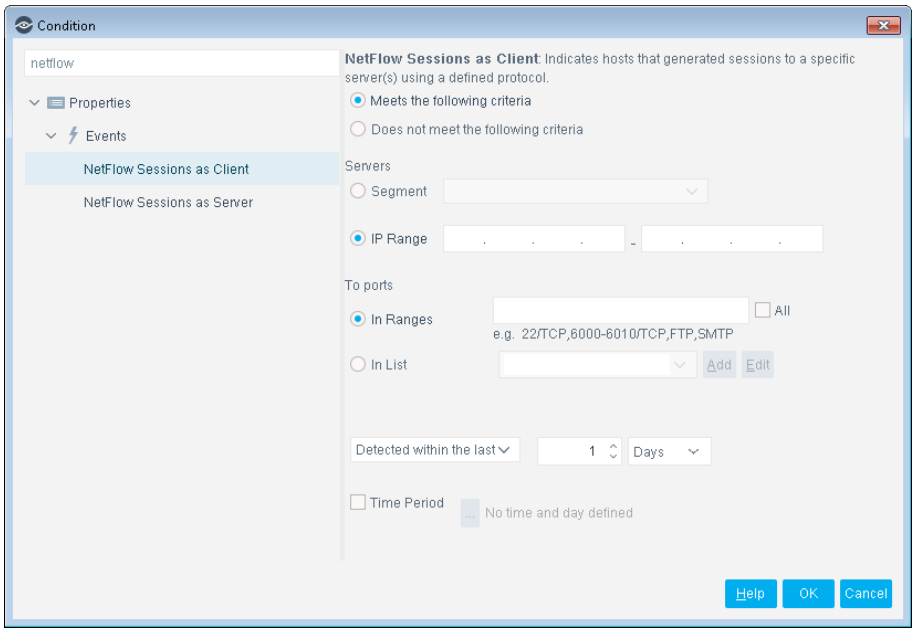
For more information about working with policies, select **Help** from the policy wizard.

To create a custom policy:

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

Properties Resolved When Used in Policies

Two of the properties provided by the Flow Collector are only resolved when used in a policy.



To access these Flow Collector properties:

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

   The Flow Collector provides the following properties:

Property	Description
NetFlow Sessions as Client	The server target with which this endpoint initiated a session. The session is detected whenever traffic is seen. You can define matching conditions based on the server-side IP address port and the session protocol.
NetFlow Sessions as Server	The client that initiated a session with this endpoint. The session is detected whenever traffic is seen. You can define matching conditions based on the client-side IP address, port and the session protocol.

Properties Not Requiring Policies

The Flow Collector resolves the following properties if they are selected in the Flow Collector configuration window:

- Traffic seen
- Open Ports

See Configure the Flow Collector.

Core Extensions Module Information

The Flow Collector 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	DNS Enforce Plugin	NBT Scanner Plugin
CEF Plugin	DNS Query Extension Plugin	Packet Engine
DHCP Classifier Plugin	External Classifier Plugin	Reports Plugin
Dashboard Plugin	Flow Analyzer Plugin	Syslog Plugin
Device Classification Engine	Flow Collector	Technical Support Plugin
DNS Client 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. Upgrading the Forescout version or performing a clean installation installs this module automatically.

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 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**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based Documentation Portal, as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

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

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides 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 product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation 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

You can access individual documents, as well as the Documentation Portal, 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 in the Console.

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**.

Content Module, eyeSegment Module, and eyeExtend Module Help Files

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

Documentation Portal

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