ForeScout

CounterACT NetFlow Plugin

Configuration Guide

Version 1.1.0 and Above

Table of Contents

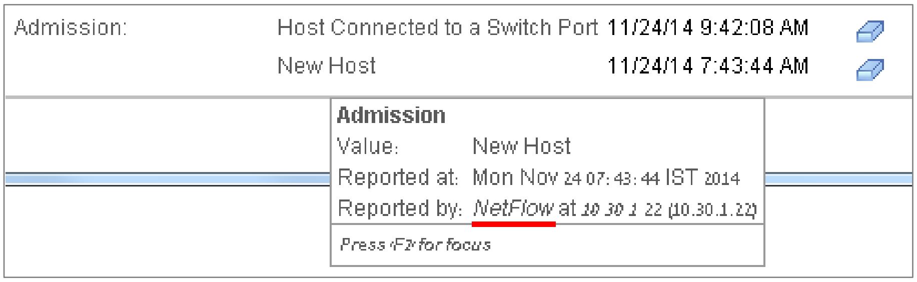
About NetFlow Integration

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.



Admission: Host Connected to a Switch Port 11/24/14 9:42:08 AM

New Host 11/24/14 7:43:44 AM

Admission

Value: New Host

Reported at: Mon Nov 24 07:43:44 IST 2014

Reported by: *NetFlow* at 10 30 1 22 (10.30.1.22)

Press <F2> for focus

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. Install the Plugin
4. Configure the Plugin
5. 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 7.0.0 running Service Pack 2.0.0 or above

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.

Install the Plugin

This section describes how to install the plugin.

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways:
   - If you are installing a Beta release of this plugin, acquire the plugin from your ForeScout representative or contact beta@forescout.com.
   - Otherwise, navigate to the Customer Support Plugins page and download the plugin.
2. Save the plugin **`.fpi`** file.
3. Select **Options** from the Console **Tools** menu.
4. Navigate to and select the **Plugins** folder. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **`.fpi`** file.

7. Select **Install**.

🗎 *If your system is running CounterACT 7.0.0 Hotfix 1.7.1 or above, an installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.*

To start the installed plugin:

1. Select **Start** to start the NetFlow plugin. The Select Appliances dialog appears.
2. Select the CounterACT Appliances on which to start the plugin.

🗎 *Typically, the NetFlow Plugin runs only on specific Appliances that are designated to audit and process NetFlow data.*

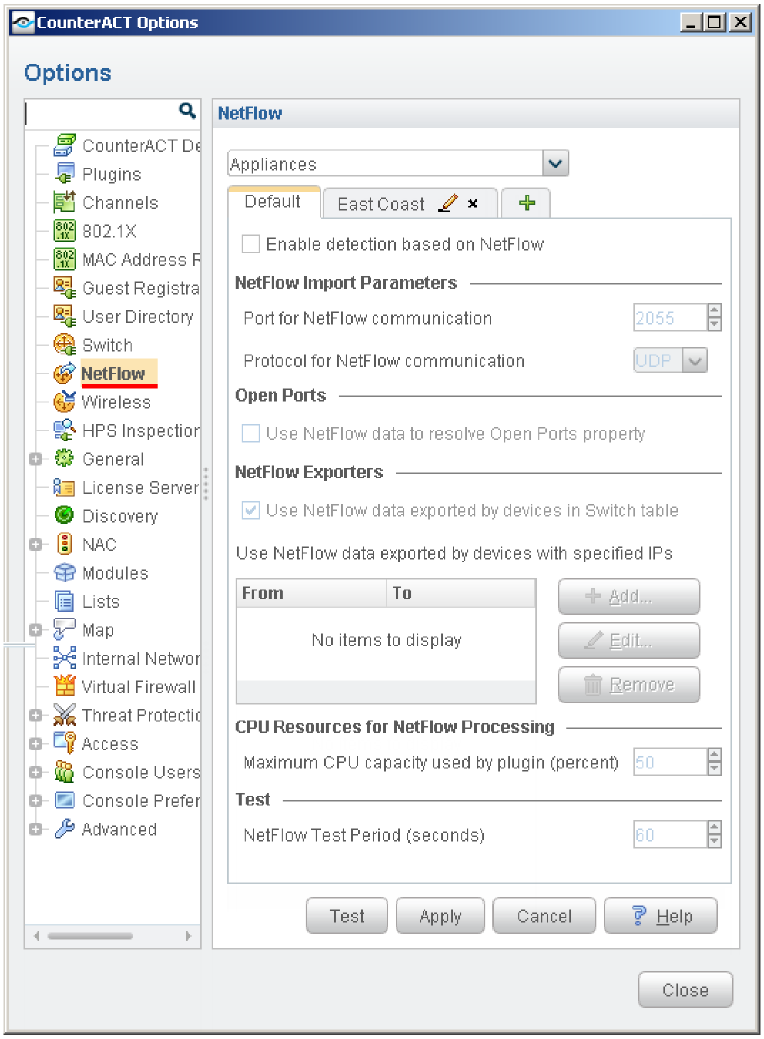
3. Select **OK**. The NetFlow Plugin runs on the selected Appliances.

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 **Plugins**.
3. In the Plugins pane, select the NetFlow plugin and select **Configure**. The NetFlow configuration pane appears.



☐ Enable detection based on NetFlow

NetFlow Import Parameters

Port for NetFlow communication: 2055

Protocol for NetFlow communication: UDP

Open Ports

☐ Use NetFlow data to resolve Open Ports property

NetFlow Exporters

☑ Use NetFlow data exported by devices in Switch table

Use NetFlow data exported by devices with specified IPs

From	To
No items to display	

CPU Resources for NetFlow Processing

Maximum CPU capacity used by plugin (percent): 50

Test

NetFlow Test Period (seconds): 60

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.

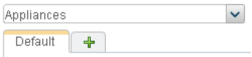
🗎 *This percentage is mapped downward to the number of CPUs on the machine. For example, if you specify 75 percent of processing resources:*
- On a machine with two CPUs the maximum resource usage is one CPU.
- On a machine with four CPUs the maximum resource usage is three CPUs.

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

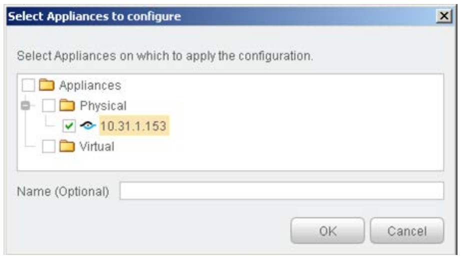
The configuration settings of the Default tab are applied to the Enterprise Manager. By default these settings are also applied to all Appliances.



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

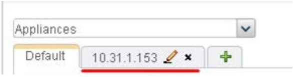
To create configuration settings for an Appliance or group of Appliances:

1. Select the Plus (+) tab . The Select Appliances to configure dialog box appears.

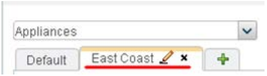

Select Appliances to configure

Select Appliances on which to apply the configuration.

2. Do one of the following:
   - Select one Appliance and select **OK**. A configuration tab appears for the Appliance you selected.



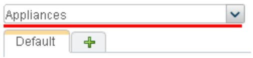
   - Select several Appliances and enter a name in the **Name (Optional)** field. Select **OK**. A configuration tab appears for the group you created.



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.



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

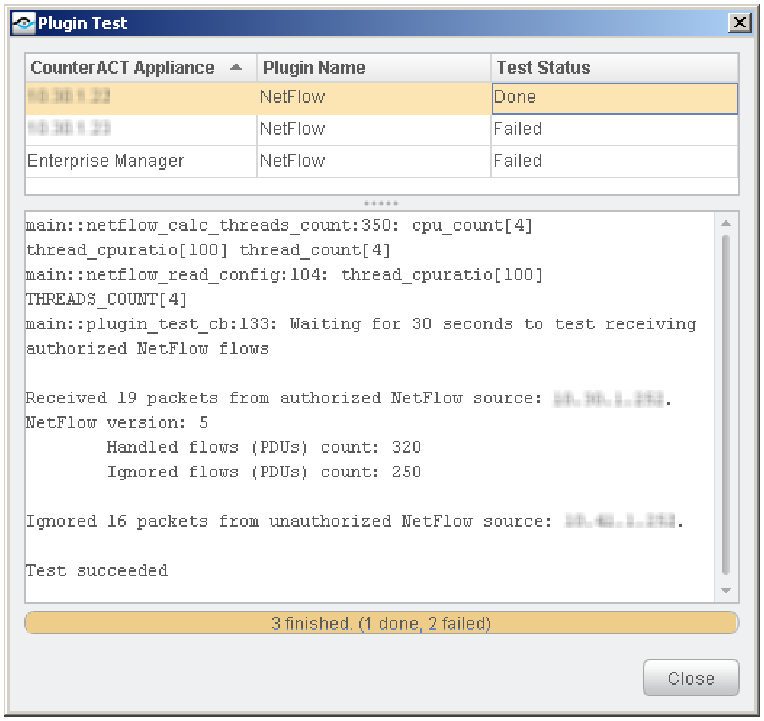
During the test, the plugin listens for NetFlow data with the configured port and protocol, and selects data from the NetFlow sources that match the configured filters. If no NetFlow data from the specified sources is detected, the test fails.

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.



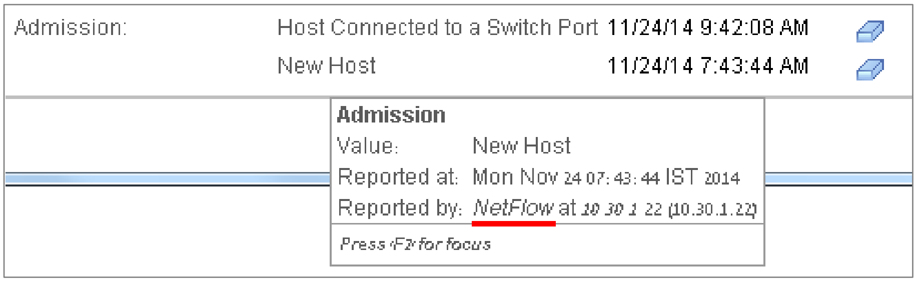
CounterACT Appliance	Plugin Name	Test Status
[redacted]	NetFlow	Done
[redacted]	NetFlow	Failed
Enterprise Manager	NetFlow	Failed

```
main::netflow_calc_threads_count:350: cpu_count[4]
thread_cpuratio[100] thread_count[4]
main::netflow_read_config:104: thread_cpuratio[100]
THREADS_COUNT[4]
main::plugin_test_cb:133: Waiting for 30 seconds to test receiving
authorized NetFlow flows

Received 19 packets from authorized NetFlow source: [redacted].
NetFlow version: 5
        Handled flows (PDUs) count: 320
        Ignored flows (PDUs) count: 250

Ignored 16 packets from unauthorized NetFlow source: [redacted].

Test succeeded
```

3 finished. (1 done, 2 failed)

Detect New Endpoints

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



Admission:	Host Connected to a Switch Port	11/24/14 9:42:08 AM
	New Host	11/24/14 7:43:44 AM

Admission
Value: New Host
Reported at: Mon Nov 24 07: 43: 44 IST 2014
Reported by: *NetFlow* at 10 30 1 22 (10.30.1.22)

Press ‹F2› for focus

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.

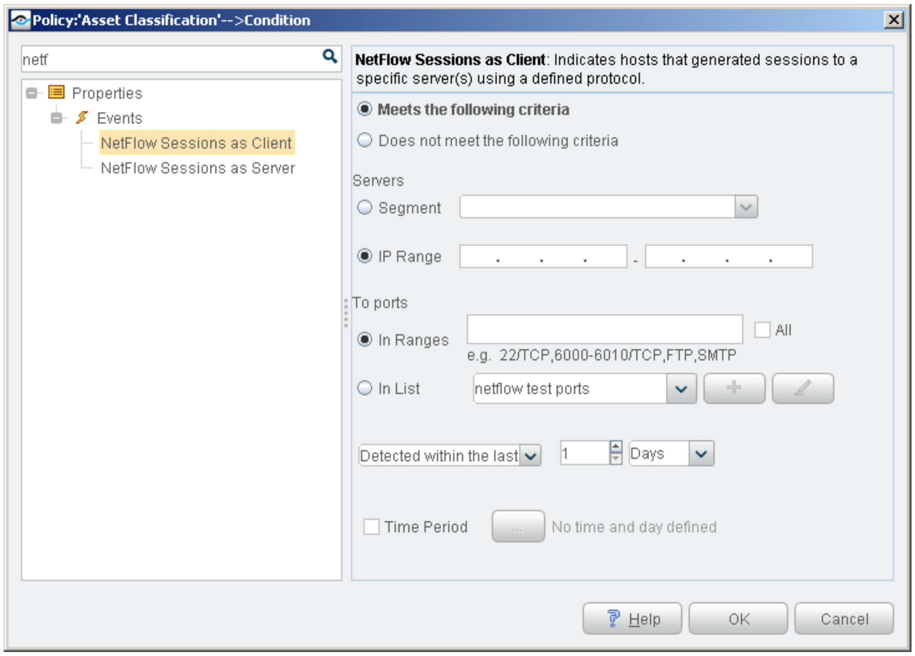
For more information about working with policies, select **Help** from the policy wizard.

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.



Policy:'Asset Classification'-->Condition

netf

Properties
Events
NetFlow Sessions as Client
NetFlow Sessions as Server

NetFlow Sessions as Client: Indicates hosts that generated sessions to a specific server(s) using a defined protocol.

● **Meets the following criteria**
○ Does not meet the following criteria

Servers
○ Segment
● IP Range . . . - . . .

To ports
● In Ranges □ All
e.g. 22/TCP,6000-6010/TCP,FTP,SMTP
○ In List netflow test ports

Detected within the last 1 Days

□ Time Period ... No time and day defined

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.

Property	Description
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.

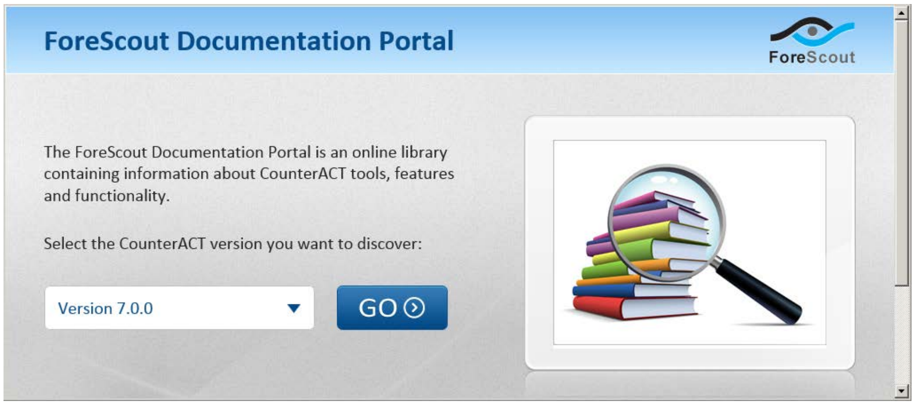
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, you can refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Help Tools

Documentation Portal

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


ForeScout Documentation Portal

The ForeScout Documentation Portal is an online library containing information about CounterACT tools, features and functionality.

Select the CounterACT version you want to discover:

To access the Documentation Portal

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

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, hotfixes, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation guides and more.

To access the Customer Portal:

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

CounterACT Console 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.

Console User Manual

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

Plugin Help Files

1. Select **Options** from the **Tools** menu and then select **Plugins**.
2. Select a plugin and then select **Help**.

Documentation Portal

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

Legal Notice

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
    - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
    - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
    - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
    - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

6/14/2015 3:31 PM