



Fore Scout

Core Extensions Module: DHCP Classifier Plugin

Configuration Guide

Version 2.2



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.

2019-03-19 13:36

Table of Contents

About the DHCP Classifier Plugin	4
What to Do.....	4
Requirements.....	5
Verify That the Plugin Is Running	5
Concepts, Components, Considerations.....	5
Concepts.....	5
Components	7
Deployment Considerations	7
Detect Hosts without Known IP Addresses	8
Configure and Test the Plugin	8
Use DHCP Properties in Policies	10
DHCP Properties.....	11
Extend DHCP Fingerprint Values.....	13
Core Extensions Module Information	15
Additional Forescout Documentation.....	16
Documentation Downloads	16
Documentation Portal	17
Forescout Help Tools.....	17

About the DHCP Classifier Plugin

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

The DHCP Classifier Plugin extracts host information from DHCP messages. Hosts communicate with DHCP servers to acquire and maintain their network addresses. The Forescout platform extracts host information from DHCP message packets, and uses DHCP fingerprinting to determine the operating system and other host configuration information.

The information retrieved by this plugin complements information sources used by the Forescout platform such as the HPS Inspection Engine and Nmap queries.

- This plugin lets the Forescout platform retrieve host information when methods such as the Forescout Packet Engine or HPS Nmap scanner are unavailable, or in situations where the Forescout platform cannot monitor all traffic. For example, if traffic in a network segment cannot be monitored directly, a CounterACT appliance on another segment can extract host information based on relayed DHCP messaging.
- This plugin can be used in concert with the above discovery methods to obtain timely, complete host information.
- This plugin reveals DHCP properties that can be used to improve classification of unclassified devices obtained from DHCP-enabled network-connected devices.

For a list of these properties, see [DHCP Properties](#).

What to Do

Perform the following steps, in order, to carry out the integration:

- Verify that requirements are met. See [Requirements](#) for details.
- Review configuration and deployment considerations. See [Deployment Considerations](#) for details.
- [Verify That the Plugin Is Running](#).
- Test the plugin. See [Test the Plugin](#) for details.
- (Optional) Use DHCP Properties in policies to improve classification. See [Use DHCP Properties in Policies](#) for details.

No plugin configuration is required.

Requirements

The plugin requires the following:

- Forescout version 8.1.
- Endpoint Module version 1.1 with the HPS Inspection Engine running. The DHCP Classifier Plugin relies on information from *Primary Classification* templates and policies provided by the HPS Inspection Engine.
- The endpoint (computer or any other network-aware device) must be configured to send a DHCP broadcast query requesting necessary information to a DHCP server.
- For endpoint DHCP classification, the DHCP Classifier Plugin must be running on a CounterACT device capable of receiving the DHCP client requests from traffic inspection or explicit message forwarding.

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.

Concepts, Components, Considerations

This section provides background information and guidelines for configuring network nodes to work with this plugin. It covers the following information:

- [Concepts](#) – how this plugin audits DHCP messaging.
- [Components](#) – nodes in your network that participate in DHCP messaging, and their interaction with Forescout 8.1 to support this plugin.
- [Deployment Considerations](#) – Setup details and common network structure issues to keep in mind when you implement this plugin.

Concepts

Dynamic Host Configuration Protocol (DHCP) determines how endpoints in a network identify themselves and communicate in the network. Hosts query DHCP servers to acquire and maintain their network addresses and other routing information. When an endpoint joins the network, it broadcasts a request for an IP address. DHCP servers reply, offering an available IP address, IP gateway, DNS server IP and possibly other information as well.

In addition to obtaining IP networking information, the DHCP protocol has the flexibility to exchange vendor-specific information about the hardware or operating

system of the device. This exchange is done by using DHCP options as defined by RFC 2132 and other relevant RFCs. For more information, see <http://www.rfc-editor.org/info/rfc2132>.

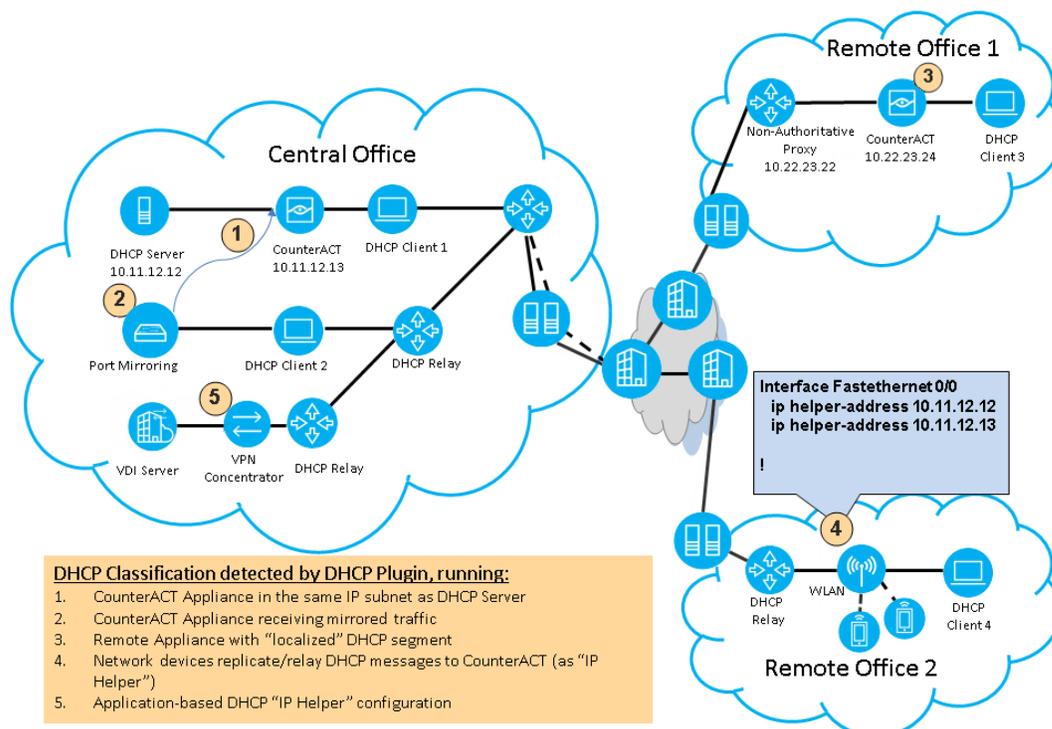
The DHCP Classifier Plugin allows you to leverage DHCP request message options by using vendor-, device-, and OS-dependent differences in the DHCP packets generated by various devices to support the endpoint device classification process.

The plugin is passive, and does not intervene with the underlying DHCP exchange. Instead, it inspects the client request messages (DHCP fingerprint) to propagate DHCP information about the connected client to Forescout 8.1 (such as operating system and other host configuration information).

While DHCP fingerprinting yields information quickly before in-depth discovery can take place, the values gleaned from DHCP messaging may be partial or inconclusive. For example:

- A device can have multi-NIC configuration – such as a laptop with wired and wireless NICs. The plugin handles each NIC as a separate host.
- Similarly, devices may have more than one IP address. DHCP properties reflect the most recent IP address detected by Forescout 8.1.
- A device with a static IP does not invoke DHCP interaction, and is invisible to the plugin.

The following diagram provides an overview of the capabilities of the DHCP Classifier Plugin. It provides a conceptual outline of theoretical deployment possibilities, indicating the various ways that DHCP messages are detected by Forescout 8.1.



The figure above shows the following typical routing paths for DHCP traffic:

DHCP Classification learned from traffic inspection: (No additional network configuration needed.)

- Example 1 – The CounterACT device (10.11.12.13) monitors DHCP broadcast messages (Client1) from the same IP subnet.
- Example 2 – The CounterACT device (10.11.12.13) receives mirrored traffic from DHCP directly (Client2).
- Example 3 – The CounterACT device (10.22.23.24) monitors DHCP broadcast messages (Client3).

DHCP Classification learned from replicated messages: (DHCP traffic is replicated to a CounterACT device acting as an additional, or secondary, DHCP server. Additional network configuration needed.)

- Example 4 – The CounterACT device (10.11.12.13) receives explicit DHCP requests (Client4) forwarded/replicated from network devices in Remote Office 2.
- Example 5 – The CounterACT device (10.11.12.13) receives replicated/forwarded DHCP requests from an application or network service (such as a VPN Concentrator or Virtual Desktop Infrastructure Server).

Components

The following components are typically involved in DHCP interactions:

Several **DHCP Servers** are deployed in the network to handle configuration and information requests.

When an **endpoint** is first admitted to a segment of the network, it broadcasts a DHCP request message, expecting a DHCP server to respond.

In some cases, network devices, such as routers, pass DHCP messages to DHCP Servers on other segments. When this happens, the network device serves as a **DHCP Relay** or **IP Helper** (different vendors may use different names for this term).

Sometimes **edge devices** for segmented traffic such as VPN Concentrators, Wireless Access Points or Virtual Desktop Infrastructure (VDI) handle similar configuration requests for their clients, or act as gateways to a DHCP server.

Deployment Considerations

- Identify network devices providing DHCP services and ensure that you have one or more CounterACT devices running the DHCP Classifier Plugin within their incoming data-path.
- Use traffic mirroring where possible, as this is expected to reduce the maintenance overhead as well as reduce the risk of network configuration errors.
- If you are not using traffic mirroring, you must explicitly add Forescout 8.1 IP addresses to participating DHCP relays or network applications.

Example of DHCP Relay Configuration

Use the following commands to enable the DHCP service and define DHCP helpers on Cisco routers:

- Use the **service dhcp** command to enable DHCP relay functionality on a router.
 - Use the **ip helper-address** command to specify the forwarding broadcast or host IP for DHCP traffic.
-  *For more information on configuring external software, refer to the relevant product documentation.*

Detect Hosts without Known IP Addresses

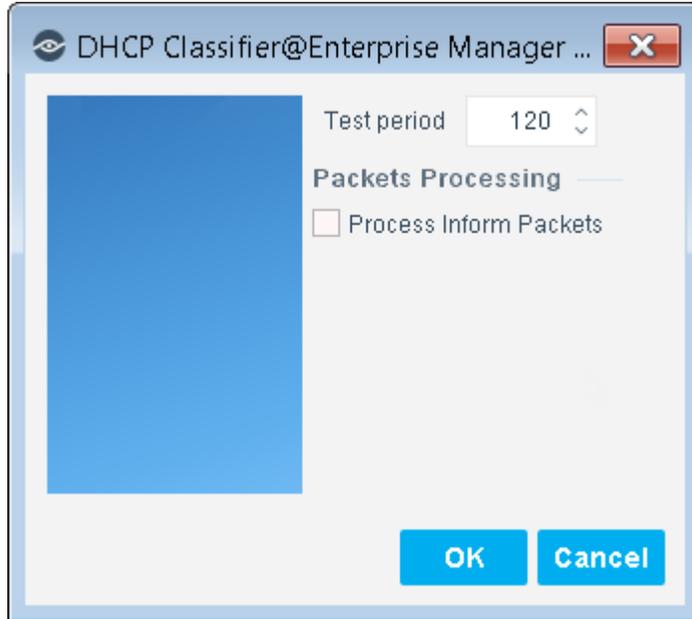
You can configure your network to detect hosts without known IP addresses. This allows you to expedite endpoint classification for endpoints that have not yet received an IP address. For details, refer to "Working with the Internal Network" in the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information about how to access the guide.

Configure and Test the Plugin

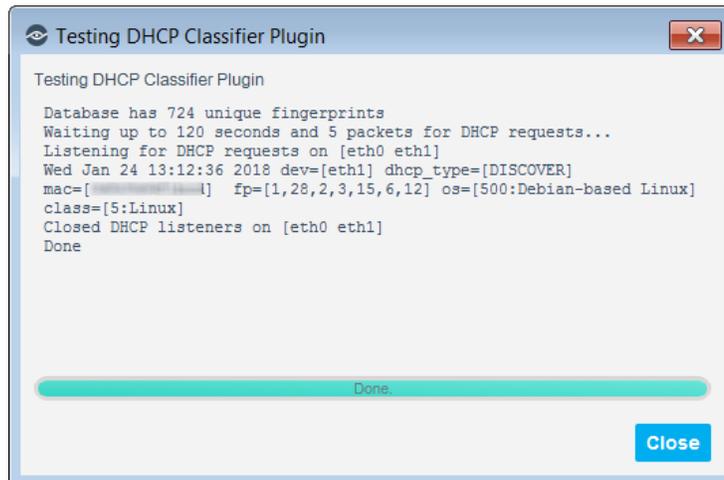
After you configure the plugin, you can test the DHCP service to verify that the plugin detects DHCP requests. You must first run the test from the plugin to listen for DHCP requests and then trigger the DHCP request from an endpoint with a known MAC address to verify that the request was recorded.

To configure and test the plugin:

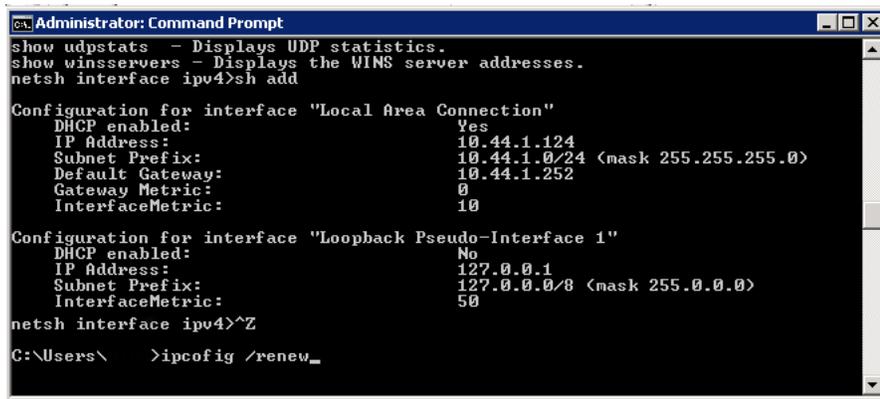
1. Select **Options** from the **Tools** menu. The Options pane opens.
2. Open the **Modules** pane and select **Core Extensions > DHCP Classifier**.
3. If the plugin is not running, select the **Start** button. Forescout 8.1 confirms that the plugin is running.
4. (Optional) Select **Configure**. Select the relevant appliances and select **OK**. The following configuration options are available:
 - Change the test period. The value is in seconds. The value you define should allow you to trigger the DHCP request and allow Forescout 8.1 to detect the triggered DHCP request (see step [6](#) below). If the test period is too long, Forescout 8.1 may collect unrelated information (see step [7](#) below). Typically test interval setting is a onetime process retained within the plugin configuration.
 - Select the **Process Inform Packets** option if you want the plugin to parse DHCP INFORM messages.



5. Select the **Test** button. A confirmation popup opens. For the duration of the test (as configured in step 4), the plugin listens for DHCP requests on the device.



6. Trigger the DHCP request from an endpoint with a known MAC address within the managed network segment.



```
Administrator: Command Prompt
show udpstats - Displays UDP statistics.
show winservers - Displays the WINS server addresses.
netsh interface ipv4>sh add

Configuration for interface "Local Area Connection"
Dhcp enabled: Yes
IP Address: 10.44.1.124
Subnet Prefix: 10.44.1.0/24 <mask 255.255.255.0>
Default Gateway: 10.44.1.252
Gateway Metric: 0
InterfaceMetric: 10

Configuration for interface "Loopback Pseudo-Interface 1"
Dhcp enabled: No
IP Address: 127.0.0.1
Subnet Prefix: 127.0.0.0/8 <mask 255.0.0.0>
InterfaceMetric: 50

netsh interface ipv4>^Z

C:\Users\ >ipconfig /renew_
```

7. Verify that Forescout 8.1 recorded the DHCP request with the specified MAC address from the tested endpoint. If Forescout 8.1 did not detect the request, verify port mirroring or recheck the configuration of the DHCP relay and/or server.
8. Select **Close**. If necessary, restart the test.

Use DHCP Properties in Policies

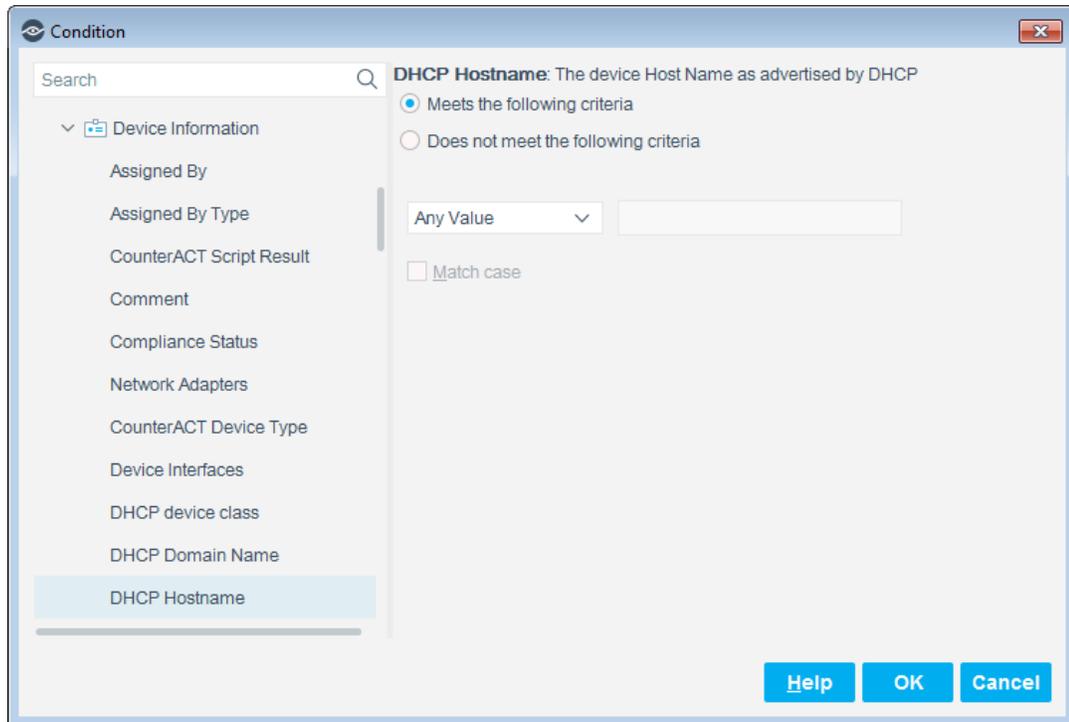
When you configure this plugin, DHCP host properties are made available for use in Forescout 8.1 policies. Property values are extracted from fields of DHCP messages, or are deduced from these messages by DHCP fingerprinting. DHCP host properties return basic information about the host, and can be used as conditions in Forescout 8.1 *Primary Classification* policies.

You can use DHCP properties in Forescout 8.1 policies to classify unclassified devices. You may need to edit *Primary Classification* policies when DHCP properties report a new asset or product type not currently included in these policies. See [Extend DHCP Fingerprint Values](#).

For more information about using properties in policies, refer to the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information about how to access the guide.

DHCP Properties

This plugin provides the following DHCP-based host properties.



DHCP Domain Name: The device Domain Name as advertised by DHCP.

DHCP Hostname: The host name of the device as it appears in option tag 12 of the DHCP_DISCOVER message.

This information may not be available for all hosts, depending upon equipment vendor, operating system, or host configuration.

DHCP Vendor Class: The vendor class of the device, as it appears in option tag 60 of the DHCP_DISCOVER message.

This information may not be available for all hosts, depending upon equipment vendor, operating system, or host configuration.

DHCP device Class: The general operating system or type of the device. This value is deduced from the DHCP fingerprint. Valid values in this release are listed below.

To add additional device class values based on DHCP fingerprints in your network environment, see [Extend DHCP Fingerprint Values](#).

Windows

Video Conferencing

Macintosh

BSD

VoIP Phones/Adapters

Misc

Routers and APs	Dead OSes
Linux	Network Boot Agents
Gaming Consoles	CD-Based OSes
Home Audio/Video Equipment	Solaris
Printers	Smartphones/PDAs/Tablets
Switches	Monitoring Devices
Projectors	Thin Clients
Physical Security	Datacenter appliance
Point of Sale devices	

DHCP device OS: The specific operating system running on the device. This value is deduced from the DHCP fingerprint. Valid values in this release are listed below:

 *To add additional device values based on DHCP fingerprints in your network environment, see [Extend DHCP Fingerprint Values](#).*

Android 0.9	Linux 2.4
Android 1.0	Linux 2.6
Android 1.5-2.1	Mac OS 9.1
Android 2.2	Mac OS 9.2
Android 3.0	Mac OS 9.x
BeOS 4	Mac OS X
BeOS 5	Maemo
FreeBSD	Microsoft
FreeBSD 6.0	OpenBSD 3.8
FreeBSD 6.1	OpenBSD 4
FreeBSD 6.2	OpenSolaris
FreeBSD 6.3	OS/2 Warp
FreeBSD 7	Sun 5.6
FreeBSD 7.1	VxWorks 5.4

FreeBSD 7.2	VxWorks 5.5
FreeNAS	Windows
Haiku	Windows 2000
iOS	Windows 7
IOS	Windows 95
Linux	Windows 95 B
Linux 2.0	Windows 98
Linux 2.2	Windows 98 SE
Windows CE	Windows Server 2003
Windows ME	Windows Server 2008
Windows NT 4	Windows Vista
Windows Phone	Windows XP

DHCP request fingerprint: The contents of the Parameter Request field (option tag 55) of the DHCP_DISCOVER message. Use this field with Forescout string matching options to create policy conditions that find specific DHCP tag values you discover in your environment.

DHCP options fingerprint: The contents of the option declarations section of the DHCP_DISCOVER message. Use this field with Forescout string matching options to create policy conditions that find specific DHCP tag values you discover in your environment.

 *DHCP server properties, including the **DHCP Server Address** property, are discovered by Forescout 8.1 without this plugin.*

DHCP Server Address: The device IP received from a DHCP server and used as the IP address of the DHCP server.

Extend DHCP Fingerprint Values

The DHCP Classifier Plugin identifies most commonly encountered operating systems and device types. However, you may discover values in DHCP message fields that are common, useful markers in your environment – yet are not included in the valid values provided by the plugin.

Use string matching conditions to identify and use these values in Forescout 8.1 policies. The **DHCP request fingerprint** property and the **DHCP options fingerprint** property let you match any pattern of values in these sections of the DHCP_Request message. In effect, you use these properties to define a DHCP fingerprint for a device that is not identified by the plugin.

For example, follow this procedure if a printer or other device is not automatically categorized by Forescout 8.1, or is unmanaged.

1. Capture the DHCP_Request Message of the device.
2. Identify a unique fingerprint of values in the Parameter Request or Options sections of the DHCP_Request message. For example, the Options section of the message may contain the following unique pattern of option flags:
6,3,1,67,15
3. Edit a relevant *Primary Classification* policy. Define a string matching condition that classifies the device when the unique fingerprint pattern is found in the ***DHCP request fingerprint*** property or the ***DHCP options fingerprint*** property.

To classify this device based on its DHCP fingerprint:

1. Edit the relevant *Primary Classification* template. Add a new condition to the *Printers* sub-rule.

Policy: 'Asset Classification'-->Sub-Rule: 'Printers' -

Name
Name Printers Edit
Description None.

Condition
A host matches this rule if it meets the following condition:
Advanced view ⚙️ 🔗

Not	(Criteria)	And/Or	
<input type="checkbox"/>		Network Function - Printer		OR	Add Edit
<input type="checkbox"/>	(NOT Classified by Action		AND	Remove
<input type="checkbox"/>		Open Ports - 9100/TCP		AND	Up
<input type="checkbox"/>		NOT Open Ports - 111/TCP)		Down

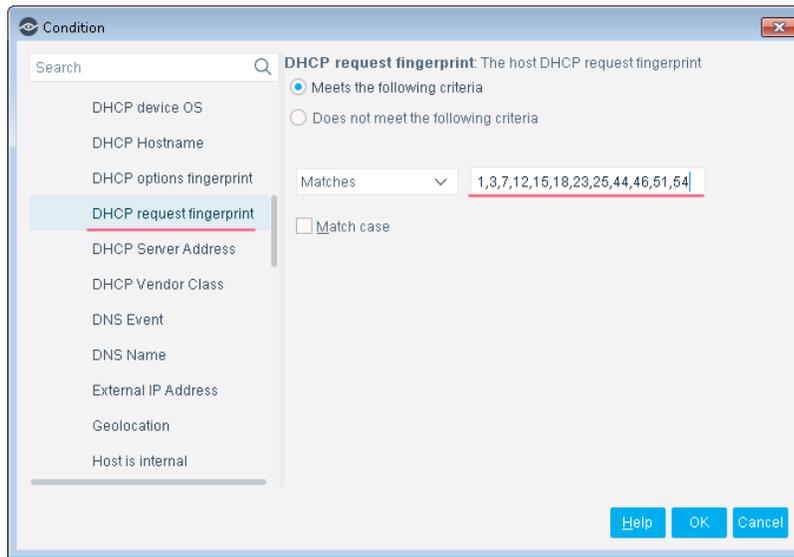
Actions
Actions are applied to hosts matching the above condition.

Ena...	Action	Details	
<input checked="" type="checkbox"/>	🔗 Add to Group	Add to Group. Schedule: ...	Add Edit Remove

Advanced
Recheck match Every 8 hours, All admissions Edit
Exceptions None.

Help OK Cancel

- The new condition matches the DHCP request fingerprint of the printer.



All devices with this DHCP request fingerprint are classified as printers.

Core Extensions Module Information

The DHCP Classifier 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).