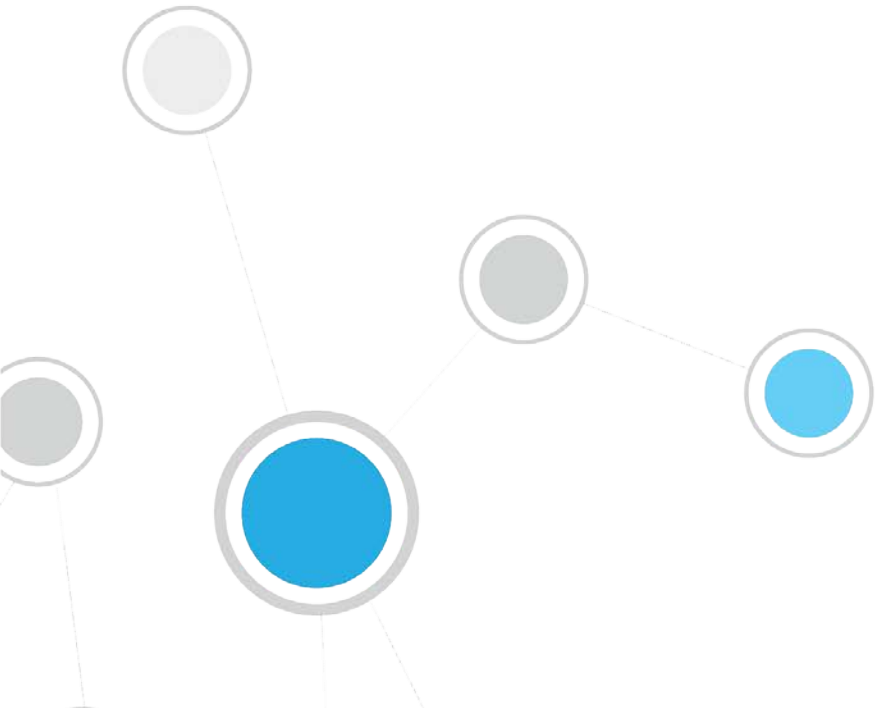
ForeScout

# CounterACT® DHCP Classify Plugin

## Configuration Guide

**Version 2.0.6 and Above**



# Table of Contents

# About the CounterACT® DHCP Classify Plugin

This plugin extracts host information from DHCP messages. Hosts communicate with DHCP servers to acquire and maintain their network addresses. When this plugin is installed, CounterACT 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 CounterACT such as the HPS Inspection Engine and Nmap queries.

- This plugin lets CounterACT retrieve host information when methods such as the CounterACT packet engine or HPS Nmap scanner are unavailable, or in situations where CounterACT 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.
- Download and install the plugin. See Installation for details.
- Review configuration and deployment considerations. See Deployment Considerations for details.
- 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

- CounterACT version 7.0.0 or above.
- HPS Inspection Engine plugin version 9.5.5 (or later). The DHCP plugin relies on information from Asset Classification templates and policies provided by the HPS Inspection plugin.

> *When the plugin is installed on systems running earlier versions of the HPS Inspection Engine plugin, edit Asset Classification templates and policies to include DHCP-based information as conditions in these policies. For more information about using properties in policies, see the CounterACT Console User Manual.*

- 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.
- Endpoint DHCP classification requires running the DHCP plugin on a CounterACT device capable of receiving the DHCP client requests from traffic inspection or explicit message forwarding.

# Installation

**To install the plugin:**

1. Navigate to the Customer Support, Base Plugins page and download the plugin **`.fpi`** file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. 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**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

# 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 CounterACT 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 .

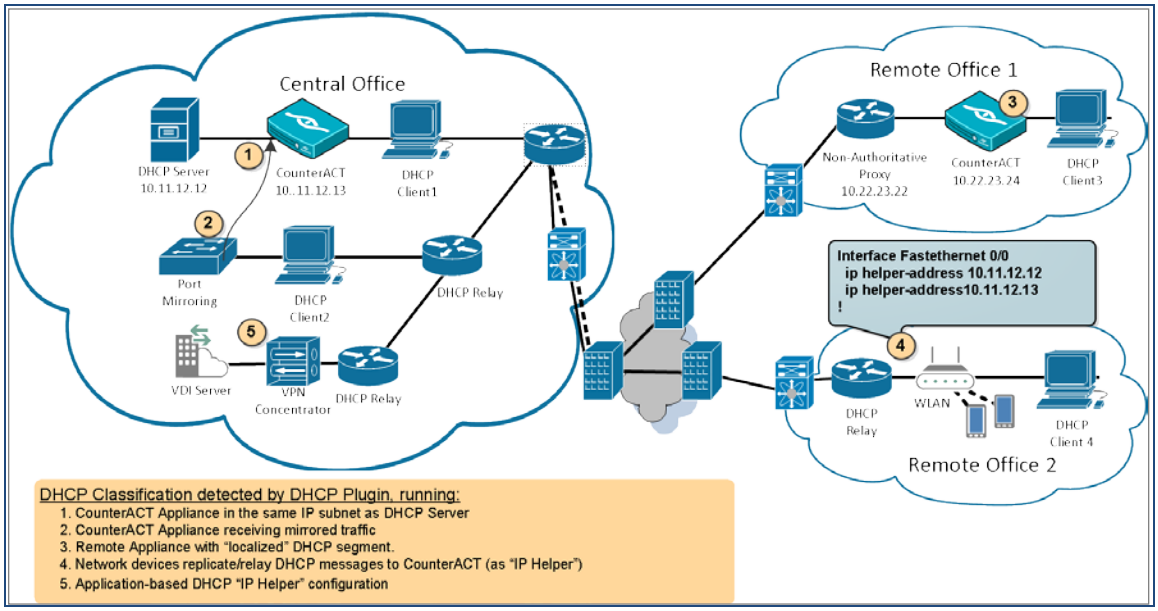
The DHCP plugin allows you to leverage DHCP request message options by using vendor-, device-, and OS-dependent differences in the DHCP packets generated by various devices to support the endpoint device classification process.

> *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 CounterACT (like 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 CounterACT.
- 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 plugin. It provides a conceptual outline of theoretical deployment possibilities, indicating the various ways that DHCP messages are detected by CounterACT.




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 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 CounterACT 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.*

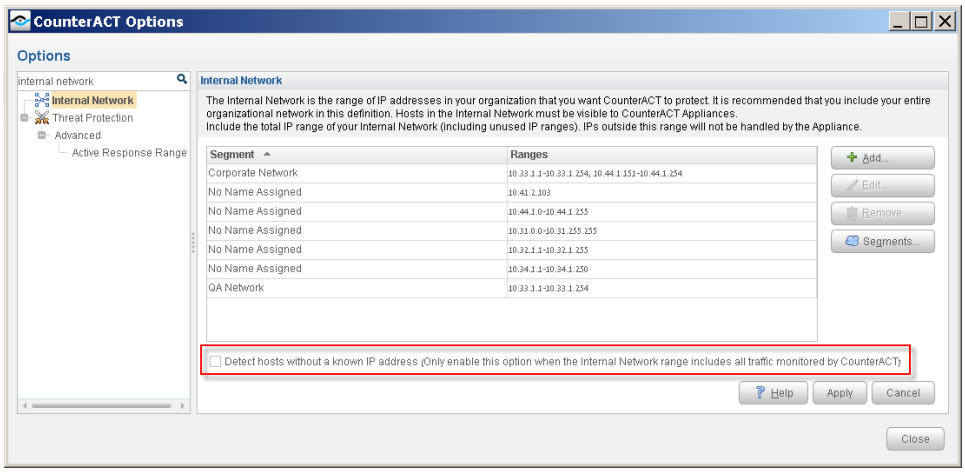
## Detect Hosts without Known IP Addresses

In CounterACT 7.0.0 and above, you need to configure your network to detect hosts without known IP addresses. This allows you to expedite endpoint classification in situations where the endpoint has not yet received an IP address.

**To detect hosts without known IP addresses:**

1. Select **Options** from the toolbar.
2. Select Internal Network from the list of options.
3. Select the checkbox **Detect hosts without a known IP address**.

*For more information about the impact of detecting hosts without a known IP address, see the section about Working with Unknown IP Addresses in the CounterACT Console User Manual.*

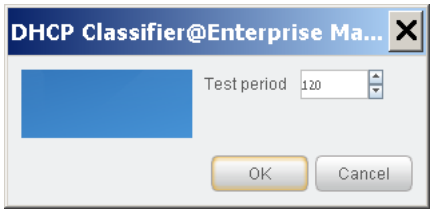



# Test the Plugin

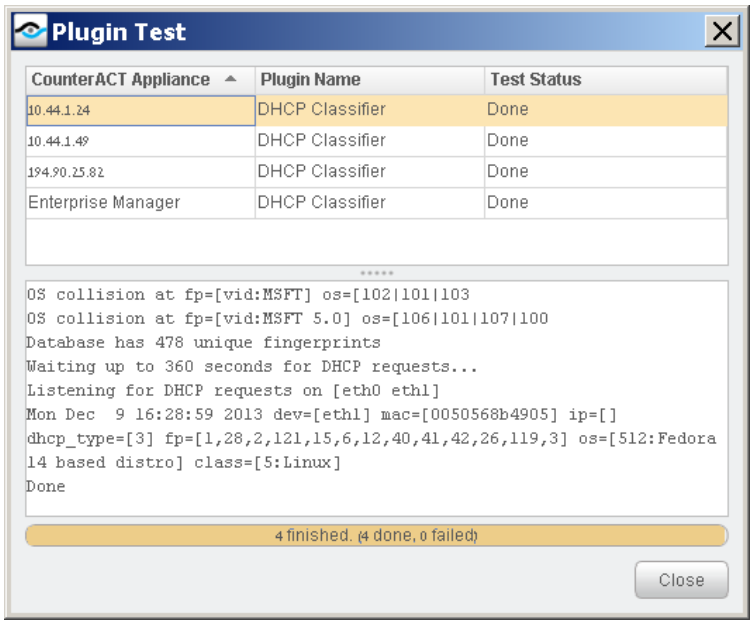
After you install the plugin, you can test the DHCP service to verify that the plugin detects DHCP requests. You must first run the test from the plugin to listen for DHCP requests and then trigger the DHCP request from an endpoint with a known MAC address to verify that the request was recorded.

1. Select **Options** from the **Tools** menu. The Options pane opens.
2. Open the **Plugins** pane and select **DHCP Classifier**.
3. If the plugin is not running, select the **Start** button. CounterACT confirms that the plugin is running.
4. (Optional) Select **Configure**, then select the relevant appliances and change the test period accordingly. The value is in seconds.

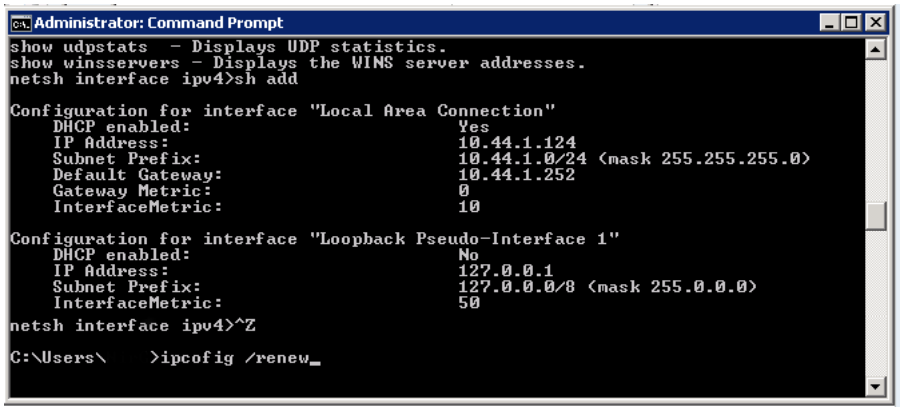
   The value you define should allow you to trigger the DHCP request and allow CounterACT to detect the triggered DHCP request (see step 6 below). If the test period is too long, CounterACT may collect unrelated information (see step 7 below). Typically test interval setting is a onetime process retained within the plugin configuration.



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.




7. Verify that CounterACT recorded the DHCP request with the specified MAC address from the tested endpoint. If CounterACT 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

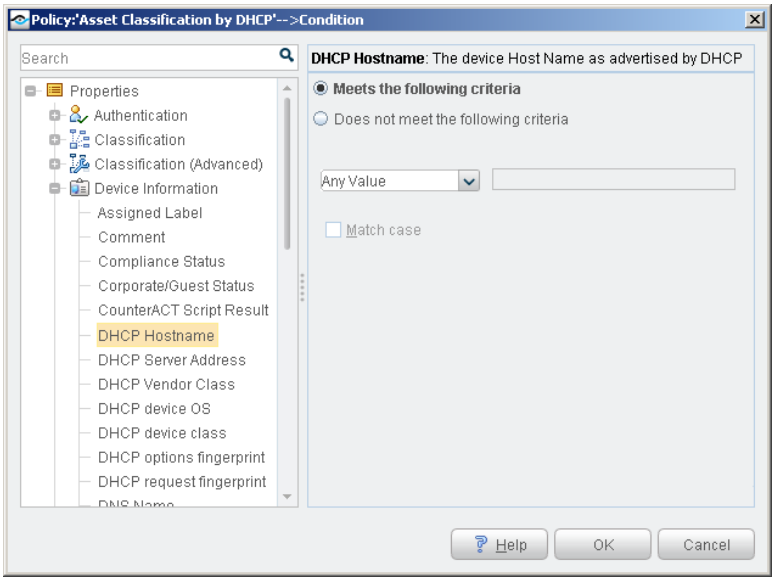
When you install this plugin, DHCP host properties are made available for use in CounterACT policies. Property values are extracted from fields of DHCP messages, or are deduced from these messages by DHCP fingerprinting. DHCP host properties return basic information about the host, and can be used as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

You can use DHCP properties in CounterACT policies to classify unclassified devices. You may need to edit Asset 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, see the *CounterACT Console User Manual*.

## DHCP Properties

This plugin provides the following DHCP-based host properties.




**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 CounterACT 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 CounterACT 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 CounterACT without this plugin.*

# Extend DHCP Fingerprint Values

The DHCP 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.

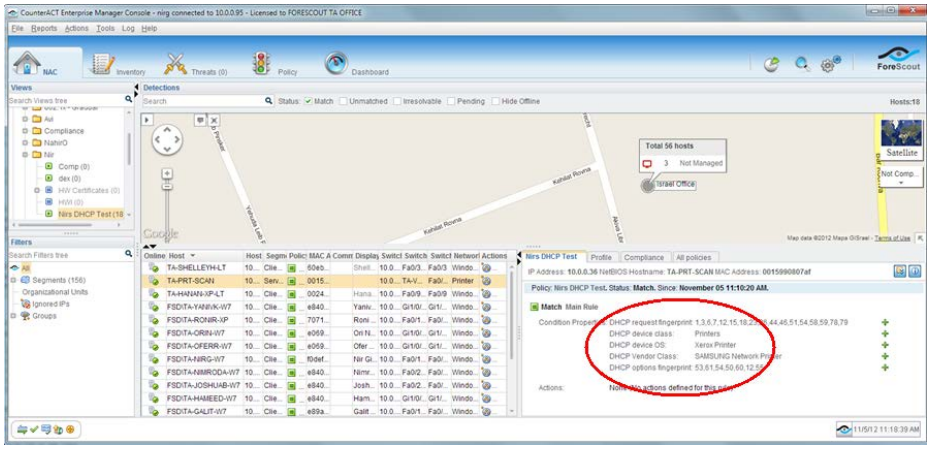
Use string matching conditions to identify and use these values in CounterACT policies. The ***DHCP request fingerprint*** property and the ***DHCP options fingerprint*** property let you match any pattern of values in these sections of the DHCP_Request message. In effect, you use these properties to 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 CounterACT, 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 Asset 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.

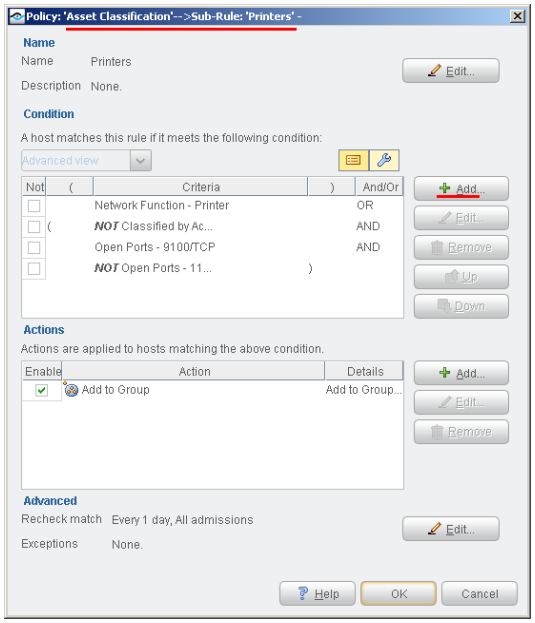
***Example***

In the following example, a network printer is not correctly identified by existing Asset Classification policies, and is displayed as Unmanaged. The DHCP Request Fingerprint property shows the unique tag fingerprint of the device. Other DHCP properties show additional device information.

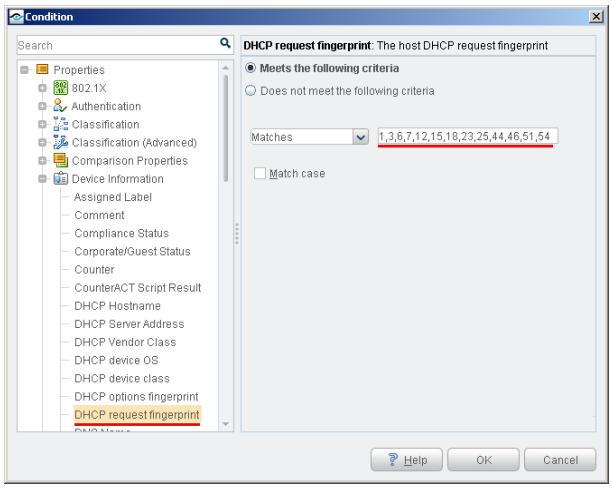


**To classify this device based on its DHCP fingerprint:**

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




**2.** The new condition matches the DHCP request fingerprint of the printer.




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

# Legal Notice



2017-04-02 20:31