CounterACT External Classifier Plugin

Configuration Guide

Version 2.2.2 and Above

Table of Contents

About the Plugin

The CounterACT External Classifier Plugin accesses a set of MAC addresses maintained in an FTP server or an LDAP server for the following purposes:

- Assign a configured text label to any host whose MAC address matches a MAC address in the retrieved set.
- Use the assigned text label in a policy to follow up with required actions.

For example, a corporate finance printer, whose MAC address is 01:2b:45:6a:89:5F, matches a MAC address in the set of MAC addresses that the plugin retrieved from a remote FTP server. The plugin assigns a matching host the configured label ***Inventory_NorthRegion_Printers***. In the organization's asset classification policy, hosts whose label is found to match the string *Printer* are added to the group (policy action) *Corp_Equip_Printers* and a notification of this match is sent to a corporate syslog server (policy action).

To effectively use this plugin, you should have a solid understanding of either FTP server functionality, LDAP server functionality or both functionalities.

For CounterACT version 7.0.0 and above: When classifying your network's hosts based on User Directory, ForeScout recommends using the CounterACT Data Exchange (DEX) Plugin, due to its (A) flexible query ability and (B) ability to reduce load on your LDAP servers.

How It Works

The CounterACT External Classifier Plugin operates as follows:

1. Based on its configured download frequency, the External Classifier Plugin retrieves a set of MAC addresses from an external server. The plugin is configured to obtain the MAC addresses using one or both of the following methods:
   - Retrieve the file from an FTP server
   - Query an LDAP server

   The configured download frequency is per data retrieval method. The configured value determines how frequently MAC address updates, applied in the FTP file or in the LDAP server, can be available to the plugin for its use.

2. When a CounterACT Appliance resolves the *External Classification* host property in a policy rule for a detected host, the Appliance queries the External Classifier Plugin to determine/assign the applicable classification.
3. The External Classifier Plugin compares host MAC addresses with its set of retrieved MAC addresses to determine whether to assign a host the configured text label (MAC address match found in set) or not.
4. For the given host, the plugin makes one of the following assignments:
   - The plugin assigns the configured, classification label to the *External Classification* host property, whenever it finds that the given host's MAC

address matches a MAC address found in the retrieved set of MAC addresses.

- The plugin assigns *Unknown* to the *External Classification* host property, whenever one of the following conditions is true:
  - The host's MAC address is not found among the retrieved set of MAC addresses.
  - The host's MAC address is unknown to the querying CounterACT Appliance.
- When working with CounterACT versions earlier than 6.3.0, the plugin assigns *None* to the *External Classification* host property, whenever the host's MAC address is not found among the retrieved set of MAC addresses.

5. Given the *External Classification* host property's text label assignment, the CounterACT Appliance determines the policy rule match status of the given host.

Requirements

The following are the CounterACT and third party products and software releases required for the operation of the CounterACT External Classifier Plugin:

- CounterACT version 7.0.0. It is recommended to install the latest hotfix.
- FTP files and LDAP query results must contain MAC addresses in the following format:

Format	Description
XX:XX:XX:XX:XX:XX	X is any one of the following characters: 0-9, A-F (case insensitive). For Example (valid MAC addresses appear in bold): Host 1,00:1A:4B:7F:5D:2E, Sao Paulo office, 00:1A:4B:7F:5D:2F 00:1A:4B:7F:5D:2E 600 Local Branch 00:1a:4b:7c:5d:2e, Accounts

What to Do

Once you have verified that requirements are met, perform the following:

1. Install the External Classifier Plugin on the Enterprise Manager. The Enterprise Manager automatically propagates the installed plugin on all its managed CounterACT Appliances. See Install the Plugin.
2. Ensure the following for the data retrieval:
   - You possess the required information to configure the External Classifier Plugin to retrieve a MAC address set from either FTP server, LDAP server or both types of servers. See Configure the Plugin.
3. Deploy:

   - Determine the number of CounterACT Appliances at which the plugin must be configured. See Deployment Considerations.
   - Configure the External Classifier Plugin. See Configure the Plugin.

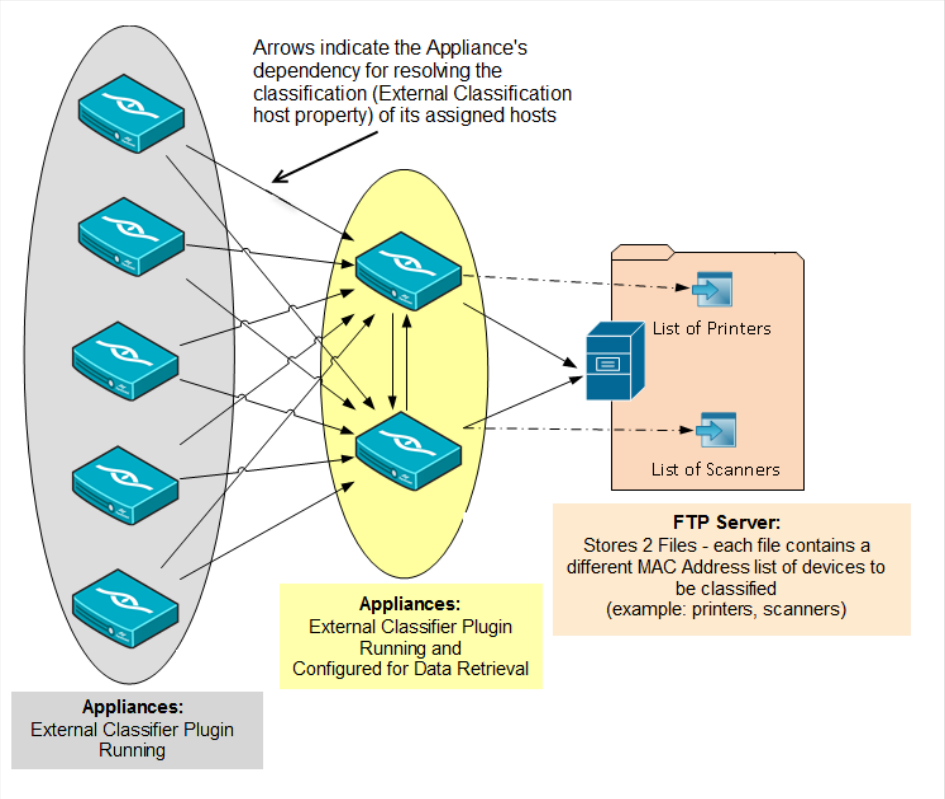
4. Start the External Classifier Plugin in *all* your CounterACT Appliances. See Start the Plugin.

Deployment Considerations

Before configuration, use the following guidelines to determine the number of CounterACT Appliances in which the plugin must be configured:

- If you have **one file** or **one LDAP query** that lists all the MAC addresses of a specific device classification, for example, an FTP file containing the MAC addresses of all your printers, configure the plugin in **one** CounterACT Appliance to classify devices using the one classification.
- If you require **two different files** or **two different LDAP queries** to retrieve the MAC addresses of **two different** device classifications, for example, an FTP file/LDAP query containing the MAC addresses of all your printers and another FTP file/LDAP query containing the MAC addresses of all your surveillance cameras, you must configure the plugin in **two different** CounterACT Appliances to classify devices using the two different classifications.
- For **n** number of **different files** or **different LDAP queries** to retrieve the MAC addresses of **n different** device classifications, you must configure the plugin in **n different** CounterACT Appliances.
- A single CounterACT Appliance can handle both an FTP file and an LDAP query.

When resolving the External Classification host property for a given host, the policy engine of the assigned Appliance queries its local plugin. The local plugin must be running, even though it does not download FTP files or perform LDAP queries, because the local plugin maintains the information pushed to it by the remote plugins configured to download/query, which are running on other appliances. By relying on information supplied from any configured plugins, the assigned Appliance manages to compile a complete list of the applicable classifications for that host. Therefore the External Classifier Plugin must run in all your CounterACT Appliances.



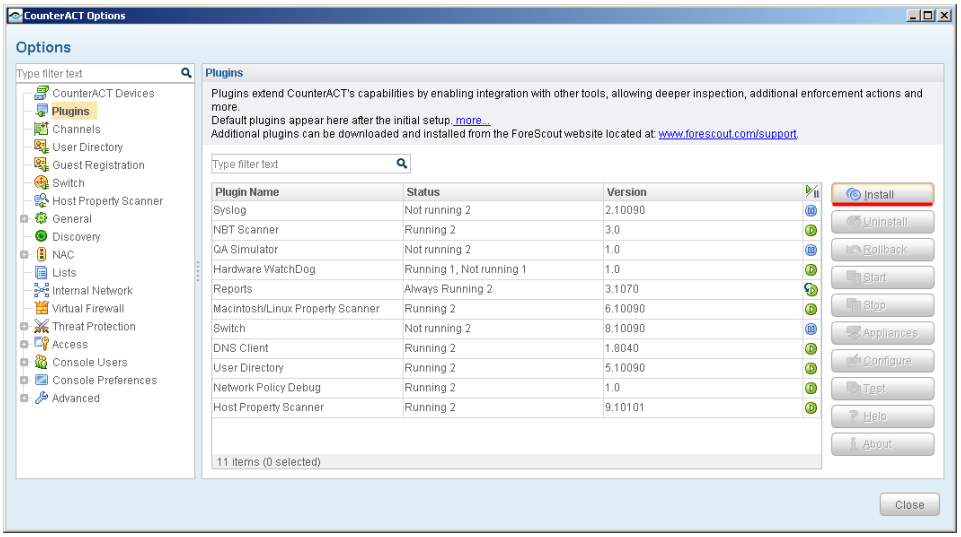
Install the Plugin

Install the External Classifier Plugin on the CounterACT Enterprise Manager. This section describes how to install the plugin.

To download and install the plugin:

1. Navigate to the Customer Support Plugins page.
2. Save the plugin installation file to the machine where the CounterACT Console is installed.
3. Select **Options** from the CounterACT Console toolbar. The Options pane opens.

4. In the Options pane, select the **Plugins** folder.
5. In the Plugins pane, select **Install**.



6. Install the plugin from the location where you saved it.

Configure the Plugin

Configure the External Classifier Plugin to obtain the set of MAC addresses - necessary for its comparison of detected hosts and assigning of the configured text label - using one or both of the following methods:

- Download a file from an FTP server
- Query an LDAP server

For guidelines as to the number of CounterACT Appliances in which the plugin must be configured, see section Deployment Considerations above.

For CounterACT version 7.0.0 and above: When classifying your network's hosts based on User Directory, ForeScout recommends using the CounterACT Data Exchange (DEX) Plugin, due to its (A) flexible query ability and (B) ability to reduce load on your LDAP servers.

This section describes how to configure the plugin.

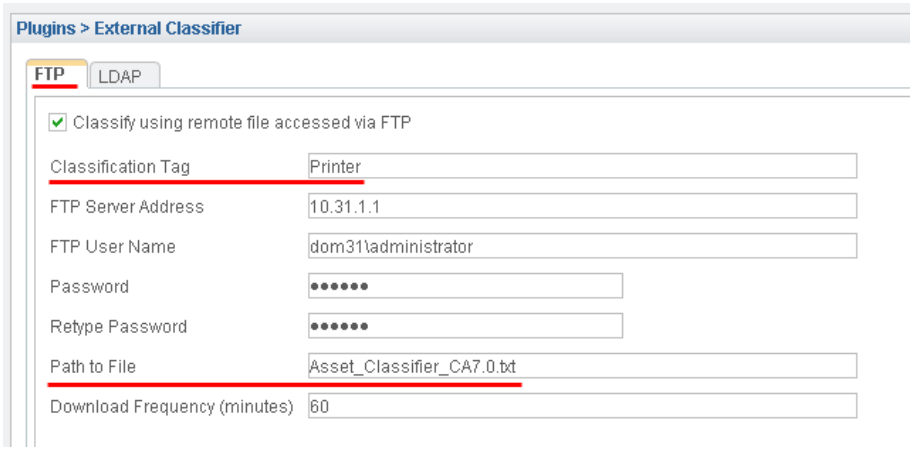
To configure the External Classifier Plugin:

1. Select **Options** from the CounterACT Console toolbar. The Options pane opens.

2. In the Options pane, select the **Plugins** folder. The Plugins pane opens.
3. In the Plugins pane, select the **External Classifier** plugin.
4. Select **Configure**. The Select Appliances dialog box opens.

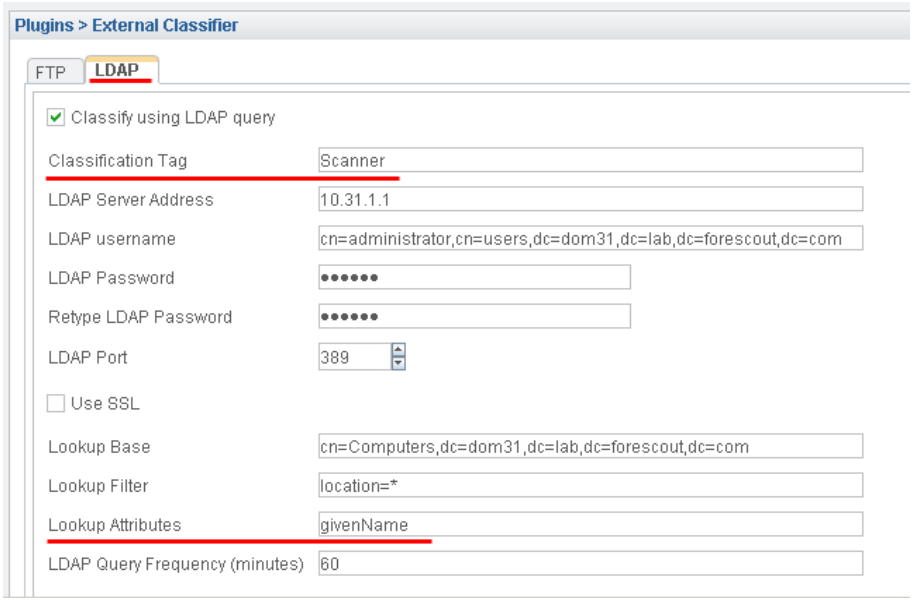
5. In the dialog box, select the checkbox of an Appliance to configure and select **OK**. The External Classifier Plugin Configuration dialog box opens with the FTP tab in view.
6. To configure the plugin for MAC address retrieval using an FTP file download, select the **FTP** tab and define the following information:

Field	Description
Classify using remote file accessed via FTP	Select checkbox to assign classification tag based on a MAC address set provided from an FTP server file Selecting this checkbox makes all other fields in this tab available for editing.
Classification Tag	Text label assigned to any detected host with a matching MAC address in the specified FTP file (see table entry Path to File).
FTP Server Address	IP address of the FTP server from which to download the file.
FTP User Name	Login username for the FTP server. Default is *anonymous*.
Password	Login password for the FTP server.
Retype Password	Login password confirmation.
Path to File	Path to the file to download. Provided path must be relative to the FTP root directory.
Download Frequency	The period, in minutes, the plugin waits before repeating the FTP file download. Provided value determines how frequently MAC address updates, applied in the FTP file, can be available to the plugin for its use.



7. To configure the plugin for MAC address retrieval using an LDAP query, select the **LDAP** tab and define the following information:

Field		Description
Classify using LDAP query		Select checkbox to assign classification tag based on a MAC address set provided from an LDAP server query. Selecting this checkbox makes all other fields in this tab available for editing.
Classification Tag		Text label assigned to any detected host with a matching MAC address in the specified LDAP query result (see table entry LDAP Query).
LDAP Server Address		IP address of the LDAP server to query.
LDAP username		Login username for the LDAP server.
LDAP Password		Login password for the LDAP server.
Retype LDAP Password		Login password confirmation.
LDAP Port		Port to use for the LDAP query.
Use SSL		Select checkbox to indicate that the LDAP query is performed using SSL (encryption and authentication).
LDAP Query	Lookup Base	Lookup base information to use in the LDAP query.
	Lookup Filter	Lookup filter information to use in LDAP query.
	Lookup Attributes	The LDAP attribute, containing the MAC address, to use in LDAP query.
LDAP Query Frequency		The period, in minutes, the plugin waits before repeating the LDAP server query. Provide value determines how frequently MAC address updates, applied in the LDAP server, can be available to the plugin for its use.



8. Select **OK**. The CounterACT Enterprise Manager Console dialog box opens.
9. Select **Yes**.

Following configuration, test the plugin. Testing verifies the following issues:

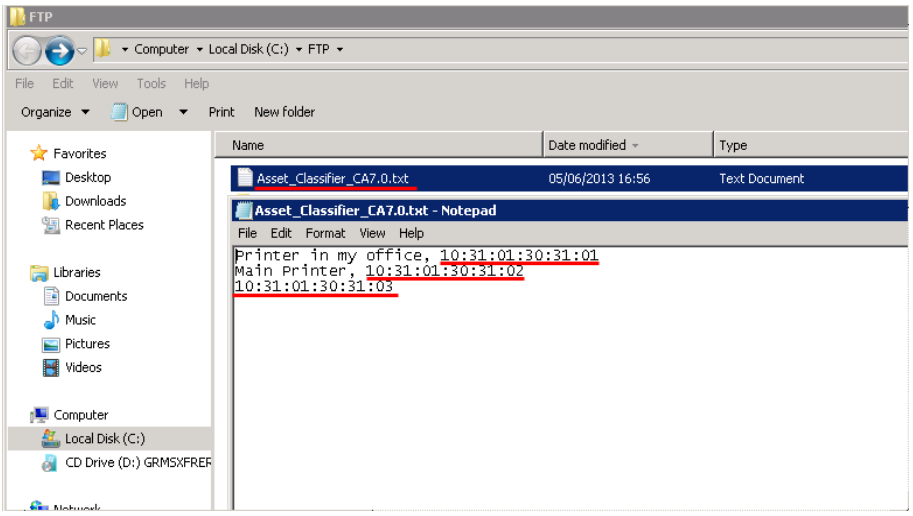
- Plugin connectivity
- Plugin authentication parameters are correct

ForeScout expects the operator to verify, using a known device such as a printer or a scanner, that the classification result assigned to the device by the plugin is correct

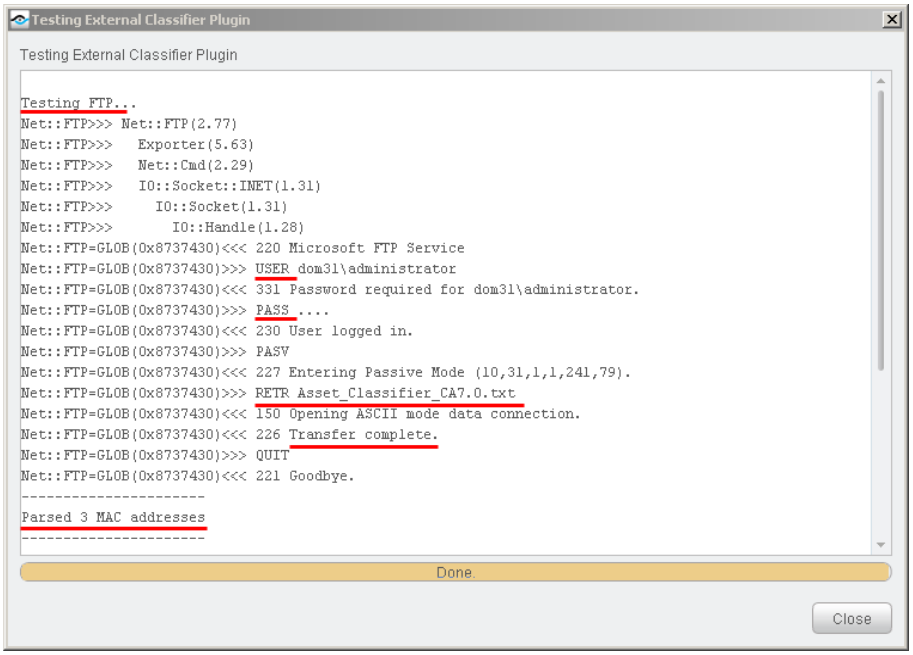
To test the configured External Classifier Plugin:

1. In the Plugins pane, double-click the **External Classifier** plugin. The External Classifier-Appliances Installed window opens and lists all the devices that are installed with the plugin.
2. From the list, select the device you recently configured and select **Test**. The CounterACT Enterprise Manager Console dialog box opens.
3. Select **Yes**. The Testing External Classifier Plugin window opens and displays the plugin test progress for the selected device.
4. When the window displays the test status **Done**, select **Close**.

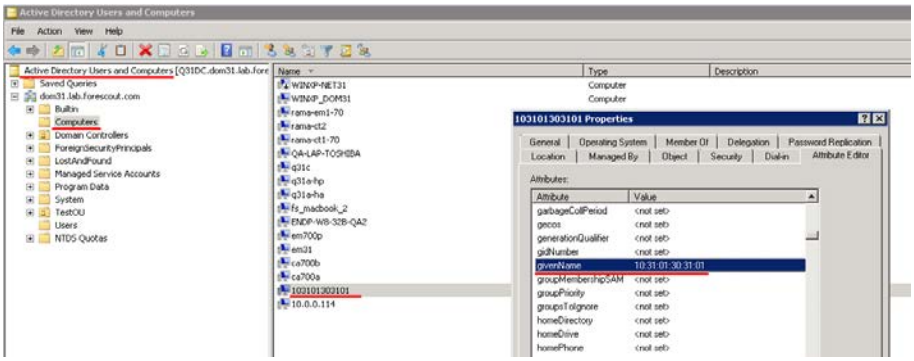
The following figure shows an example of an FTP file for download, containing a set of MAC addresses:



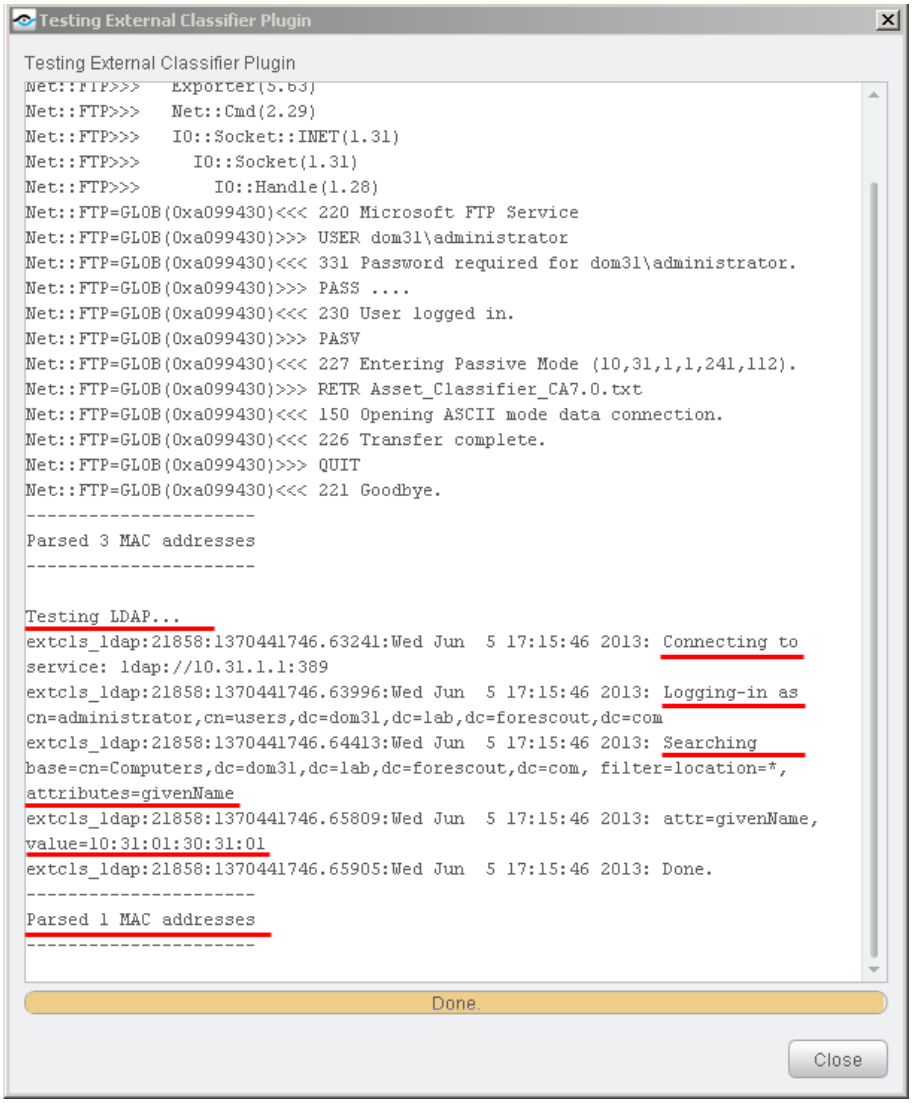
The following figure shows an example of the plugin test progress of an FTP file download:



The following figure shows an example of an LDAP entry with the attribute containing its MAC address:



The following figure shows an example of the plugin test progress of an LDAP query:



Start the Plugin

After configuring the plugin in the required CounterACT Appliances, you must start the External Classifier Plugin in *all* your CounterACT Appliances, even those appliances where the plugin is installed but not configured. Running the External Classifier Plugin in CounterACT Appliances where the plugin is not configured enables such Appliances to query all configured External Classifier Plugins and resolve the External Classification host property (assign applicable classifications) for their assigned hosts.

This section describes how to start the plugin.

To start the External Classifier Plugin in all Appliances:

1. In the Options pane, select the **Plugins** folder. The Plugins pane opens.
2. In the Plugins pane, select the **External Classifier** plugin.

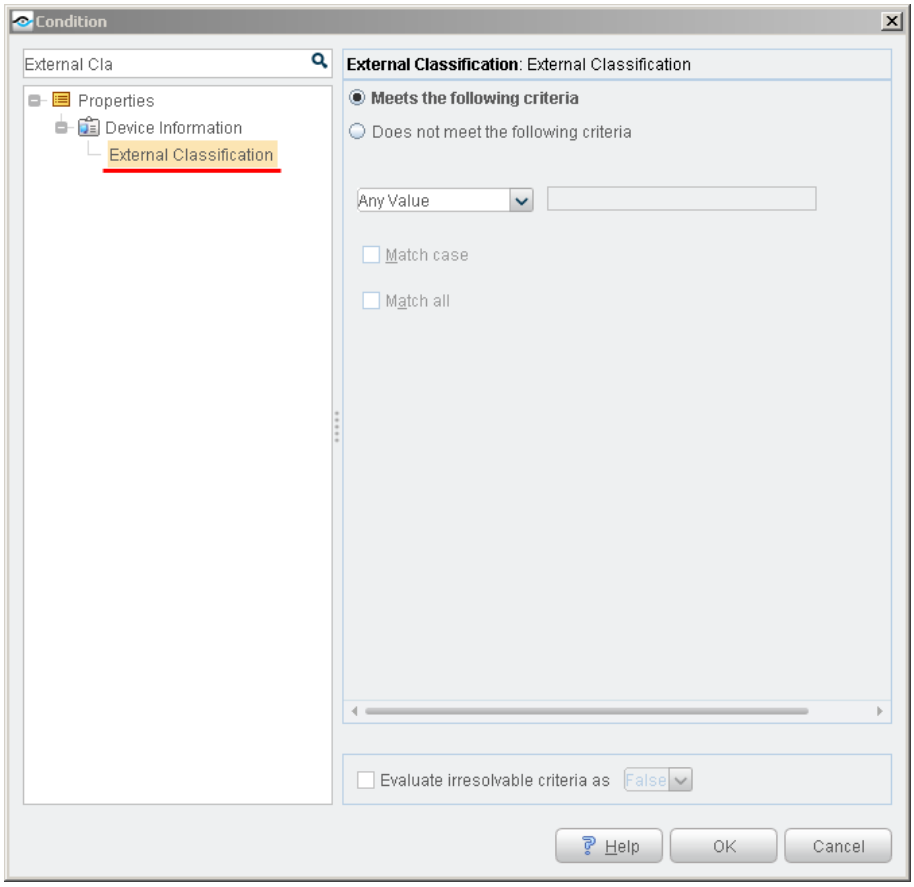
3. Select **Start**. The Select Appliances dialog box opens.
4. In the dialog box, select the checkbox of all listed devices – CounterACT Appliances and the Enterprise Manager – and select **OK**. The CounterACT Enterprise Manager Console dialog box opens.
5. Select **Yes**. The Plugin Start dialog box opens and displays the plugin start progress for every selected device.
6. In the dialog box, when the Start Status of each device displays **Done**, select **Close**.

Use External Classification Information in Policies

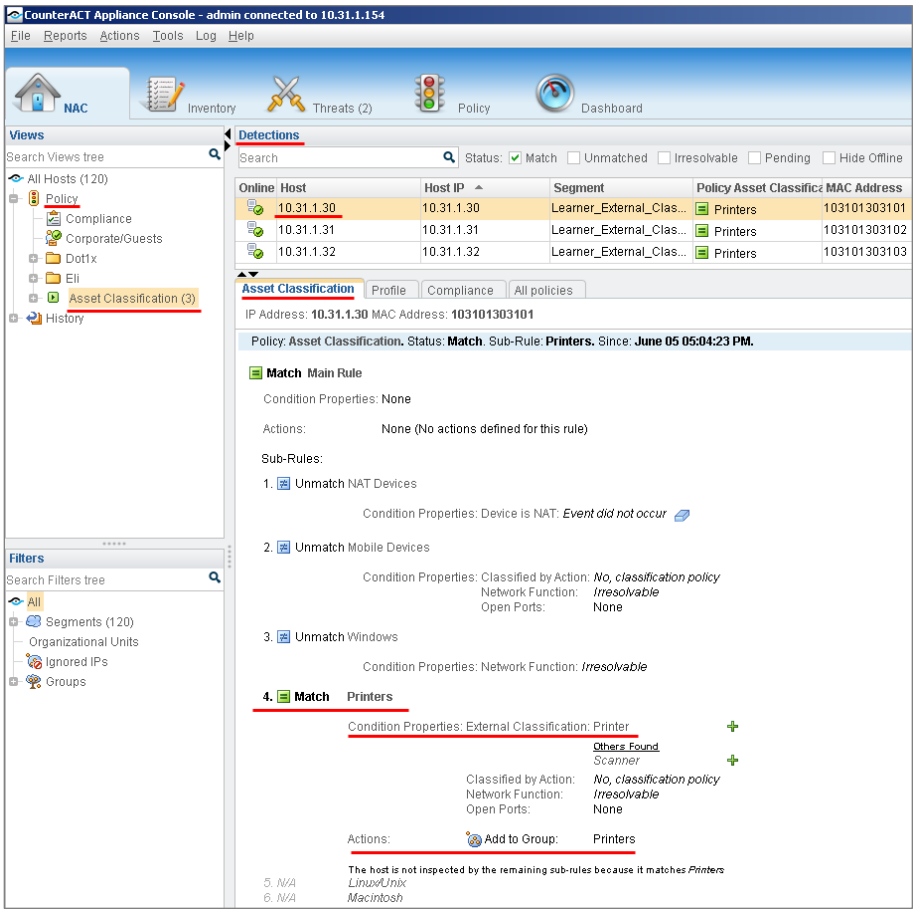
Use the *External Classification* host property in CounterACT policies to detect and control your network devices. In particular, for your unclassified network devices, extend Asset Classification policies by incorporating use of the *External Classification* host property into these policies. Refer to the *Policy Management* chapter of the *CounterACT Console User's Manual* or the Console Online Help for more information about creating and updating policies.

To work with a policy:

1. Log in to the CounterACT Console.
2. Select the Policy tab. The Policy Manager opens.
3. Create or edit a policy.
4. Navigate to the properties list.
5. Select **Device Information > External Classification** host property.



An example of the *Asset Classification* policy extended to use the *External Classification* host property. The following figure shows host detection by sub-rule property match and resulting action taken:



Display Detected Host Information

View *External Classification* host property information using any one of the following ways:

- Via the Console, **Detections** pane. Display selected host details and expand its **Host** tab information.
- Generate a Device Details report. Select **Reports Portal** from the CounterACT Console toolbar. The Reports Portal opens. In the Reports Portal, either edit an existing Device Details report or add a new Device Details report. In section **3. Detail**, add the table column **External Classification** property, which is grouped under **Device Information**. Run the report or schedule it to be run.

Legal Notice