FORESCOUT

Forescout

Core Extensions Module: External Classifier Plugin

Configuration Guide

Version 2.2.5

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

2020-04-15 13:04

Table of Contents

About the Plugin 4
How It Works 4
Requirements 5
What to Do 5
Deployment Considerations 5

Configure the Plugin..... 6
Start the Plugin.....11
Verify That the Plugin Is Running.....11
Test the Plugin.....11

Use External Classification Information in Policies..... 14

Display Detected Host Information 16

Core Extensions Module Information 16

Additional Forescout Documentation..... 16
Documentation Downloads 17
Documentation Portal 17
Forescout Help Tools.....18

About the Plugin

The External Classifier Plugin is a component of the Forescout® Core Extensions Module. See Core Extensions Module Information for details about the module.

The External Classifier Plugin accesses a set of MAC addresses maintained in an FTP server or an LDAP server to:

- 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 Primary 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.

When classifying your network's hosts based on User Directory, Forescout recommends using the Forescout 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 Forescout 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 following methods can be used:
   - Download from an FTP server
   - Query an LDAP server
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, and makes one of the following assignments:
   - When the host's MAC address matches a MAC address found in the retrieved set of MAC addresses, the plugin assigns the corresponding classification label to the *External Classification* host property.
   - The plugin resolves the *External Classification* host property as *Unknown* when the host's MAC address is not found among the retrieved MAC addresses, or when the host's MAC address is unknown to the querying CounterACT Appliance.
4. The Appliance evaluates the policy rule based on the resolved value of the *External Classification* host property.

Requirements

The plugin requires the following:

- Forescout version 8.1.
- Files and query results must contain MAC addresses in the following format:

  XX:XX:XX:XX:XX:XX

  Where X is any one of the following characters: 0-9, A-F (case insensitive).

What to Do

Once you verify that requirements have been met, perform the following:

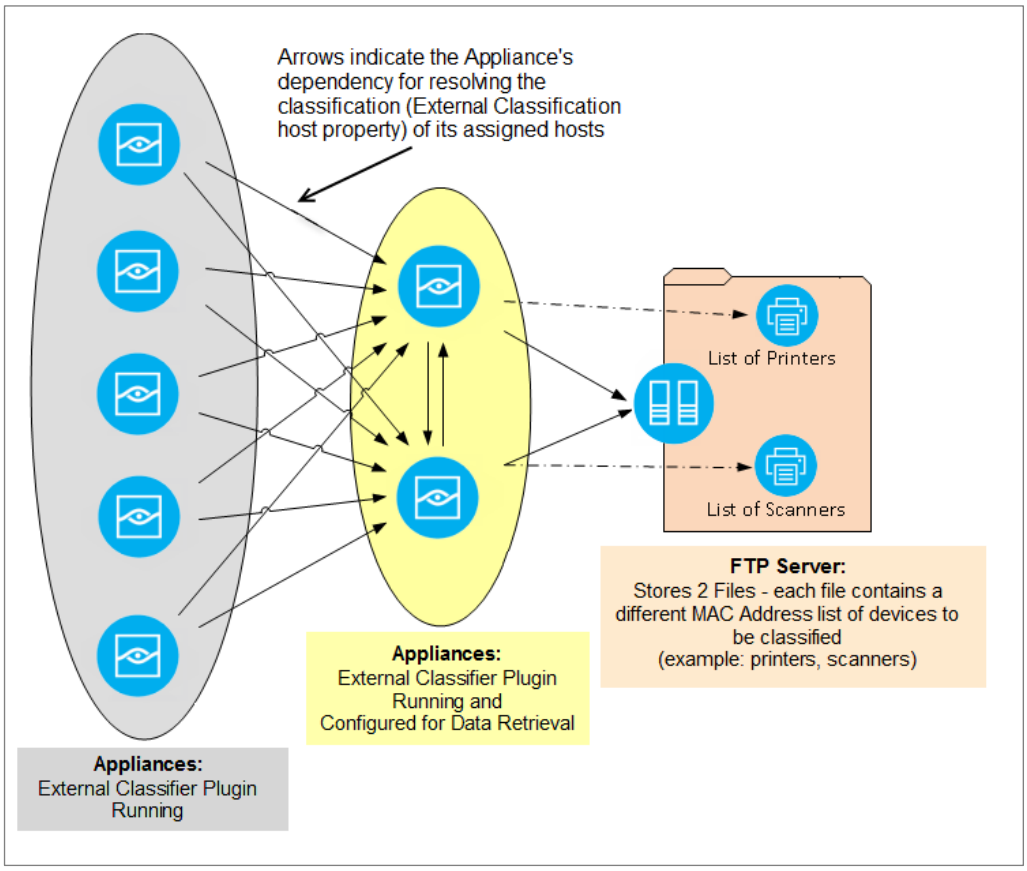
1. Ensure the following for the data retrieval:
   - You possess the required information to configure the External Classifier Plugin to retrieve a MAC address set from either FTP server, LDAP server or both types of servers. See Configure the Plugin.
2. Deploy:
   - Determine the number of CounterACT Appliances at which the plugin must be configured. See Deployment Considerations.
   - Configure the External Classifier Plugin. See Configure the Plugin.
3. 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.



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

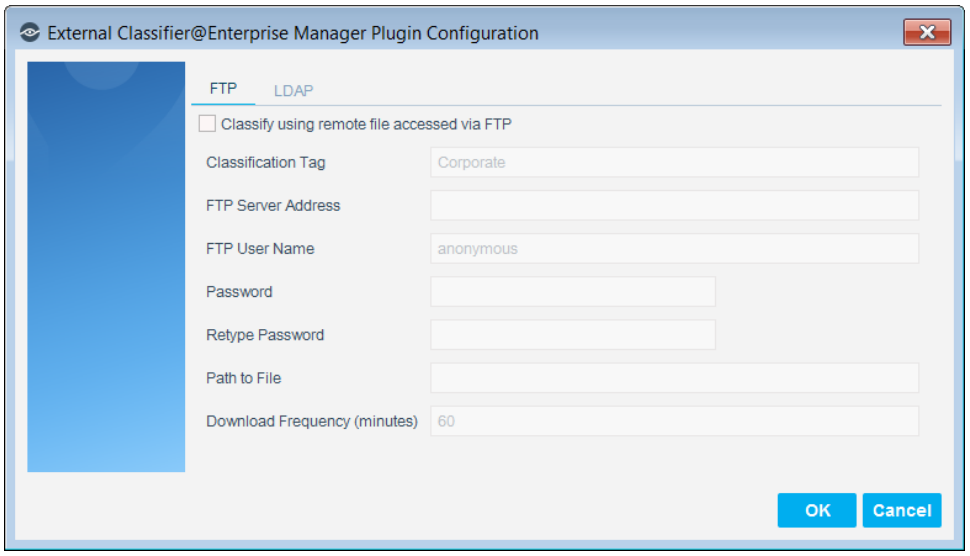
For guidelines as to the number of CounterACT Appliances in which the plugin must be configured, see Deployment Considerations.

When classifying your network's hosts based on User Directory, Forescout recommends using the Forescout 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:

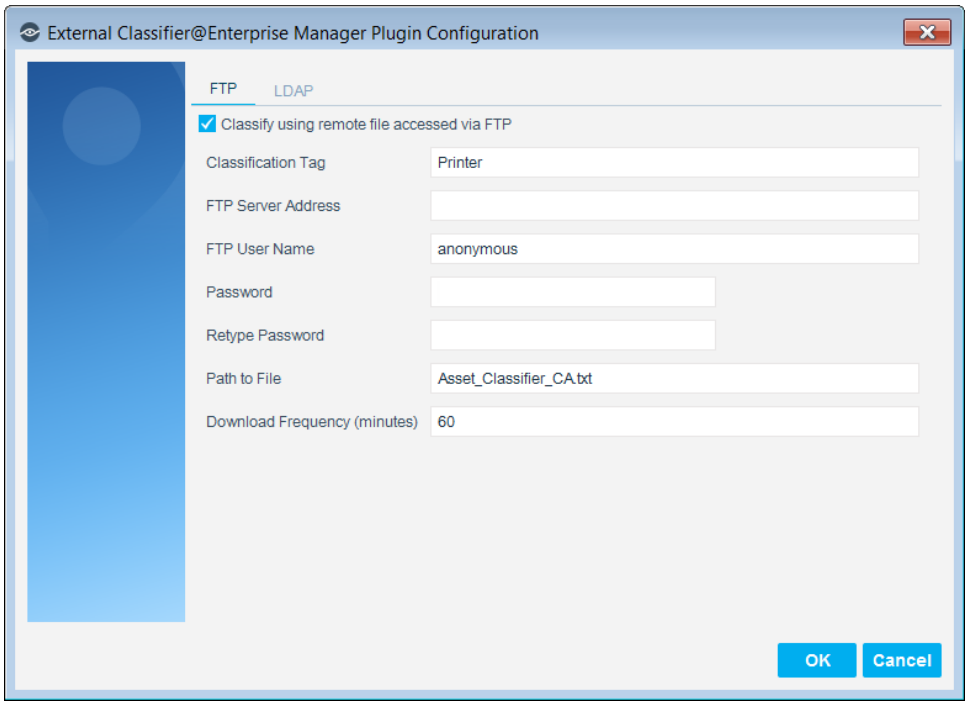
1. In the Forescout Console, select **Options** from the **Tools** menu. The Options pane opens.
2. Open the **Modules** pane and select **Core Extensions** > **External Classifier**.
3. Select **Configure**. The Select Appliances dialog box opens.
4. In the dialog box, select the checkbox of an Appliance to configure and select **OK**. The External Classifier Plugin Configuration dialog box opens.



5. 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.

Field	Description
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.

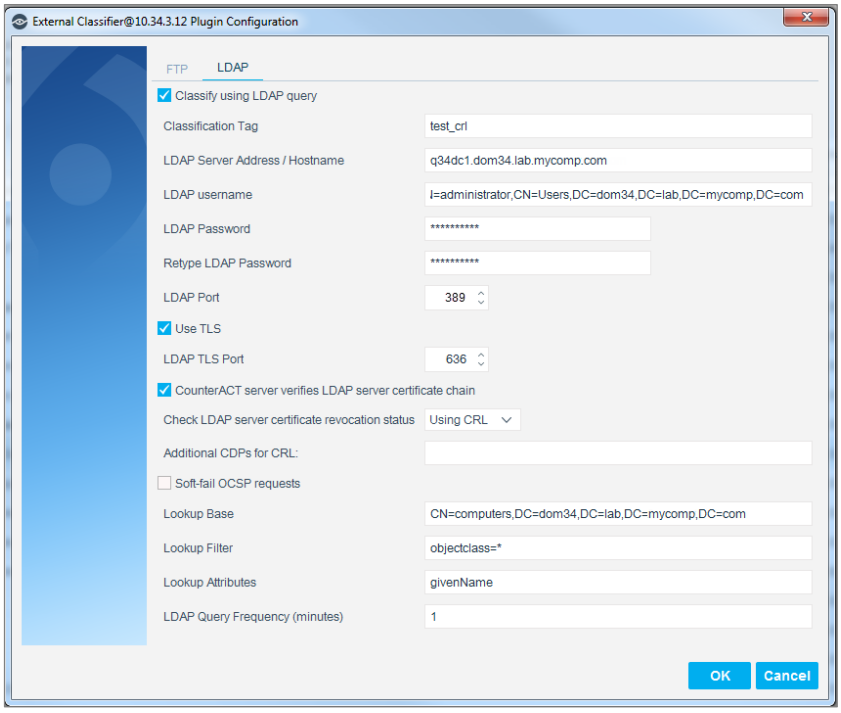


6. To configure the plugin for MAC address retrieval using an LDAP query, select the **LDAP** tab and define the following information:

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).

Field		Description
LDAP Server Address/Hostname		Identify the LDAP server to query, by defining this field as follows: ▪ When using a standard LDAP connection, enter either the IP address or the fully qualified domain name (FQDN) of the LDAP server to query. ▪ When using an LDAP over TLS connection, enter the fully qualified domain name (FQDN) 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 the plugin uses with a standard LDAP connection. By default, this port is 389.
Use TLS		Selecting this checkbox instructs the plugin to use a TLS connection to perform LDAP queries (LDAP over TLS). By default, this checkbox is disabled (not selected). If this checkbox is not selected, the plugin uses a standard LDAP connection to query the LDAP server. When this checkbox is selected, the following become available for configuration: - **LDAP TLS Port** - **The Forescout platform's server verifies LDAP server certificate chain** - **Check LDAP server certificate revocation status** - **Additional CDPs for CRL** - **Soft-fail OCSP requests**
LDAP TLS Port		Port the plugin uses with an LDAP over TLS connection. By default, this port is 636.
Authenticate LDAP Server Certificate	**The Forescout platform's server verifies LDAP server certificate chain**	Selecting this checkbox instructs the Forescout platform to verify the certificate authority trust chain of the certificate that the LDAP server presents to the Forescout platform. By default, this checkbox is disabled (not selected). To support the Forescout platform's certificate-based authentication of external servers, use the Console certificates interface (**Options** > **Certificates**) to configure certificate authority trust chains for the Forescout platform's use.

Field		Description
	Check LDAP server certificate revocation status	Instruct the Forescout platform to verify/not to verify the revocation status of the server certificate. In the field's drop-down menu, make one of the following selections: ▪ *Do not check* (default) – do not verify certificate revocation status. ▪ *Using CRL* – consult the Appliance's Certificate Revocation List (CRL) to verify the revocation status of the certificate. ▪ *Using OCSP* – look for an OCSP responder URL in the certificate and verify the revocation status of the certificate against the OCSP responder.
	Additional CDPs for CRL	Additional CRL distribution points (CDPs). (Optional) Enter one or more additional URLs from which the Forescout platform downloads additional CRLs that it uses to verify the revocation status of the certificate provided by the LDAP server. Use the comma (,) to separate between multiple URLs. The Forescout platform only supports the use of HTTP to download CRLs.
	Soft-fail OCSP requests	Selecting the **Soft-fail OCSP Requests** option instructs Forescout to accept the provided server certificate even though the Forescout platform did not receive a response from the OCSP responder about the certificate's revocation status. By default, this checkbox is disabled (not selected).
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. Provided value determines how frequently MAC address updates, applied in the LDAP server, can be available to the plugin for its use.



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

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 these Appliances to query all configured External Classifier Plugins and resolve the External Classification host property (assign applicable classifications) for their assigned hosts.

Verify That the Plugin Is Running

After configuring the plugin, verify that it 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 Plugin

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

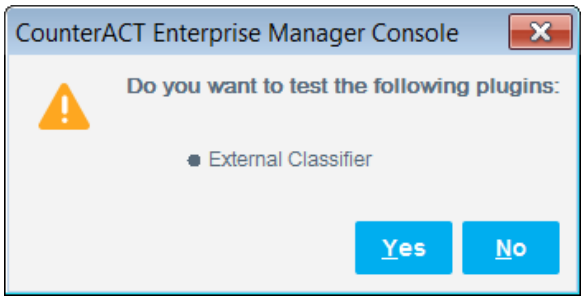
- Plugin connectivity

- Plugin authentication parameters are correct

The Forescout platform 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.

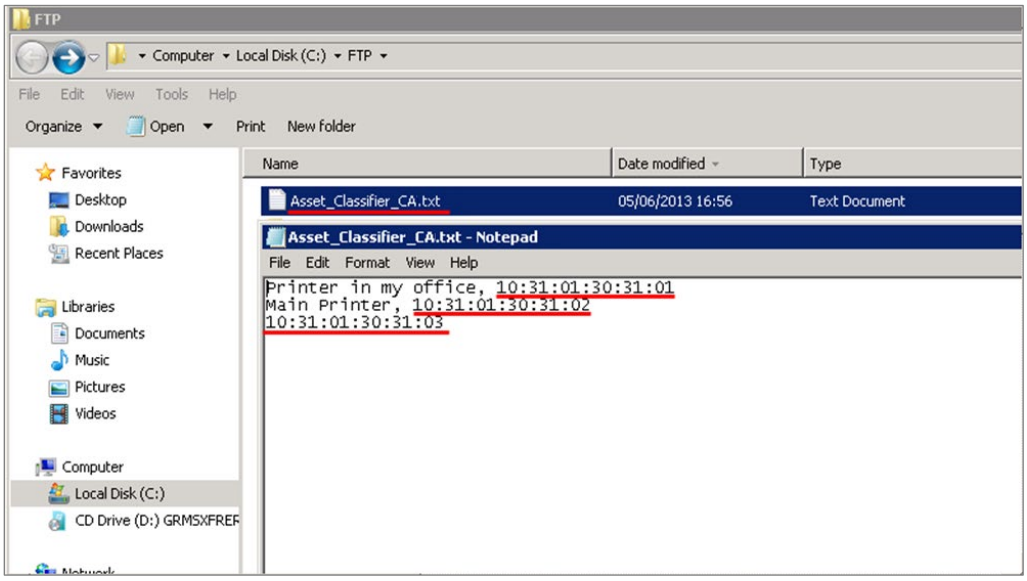
To test the configured External Classifier Plugin:

1. In the Forescout Console, select **Options** from the **Tools** menu. The Options pane opens.
2. Open the **Modules** pane, expand **Core Extensions**, and double-click **External Classifier**. The External Classifier-Appliances Installed window opens and lists all the devices that are installed with the plugin.
3. From the list, select the device you recently configured and select **Test**. The CounterACT Enterprise Manager Console dialog box opens.

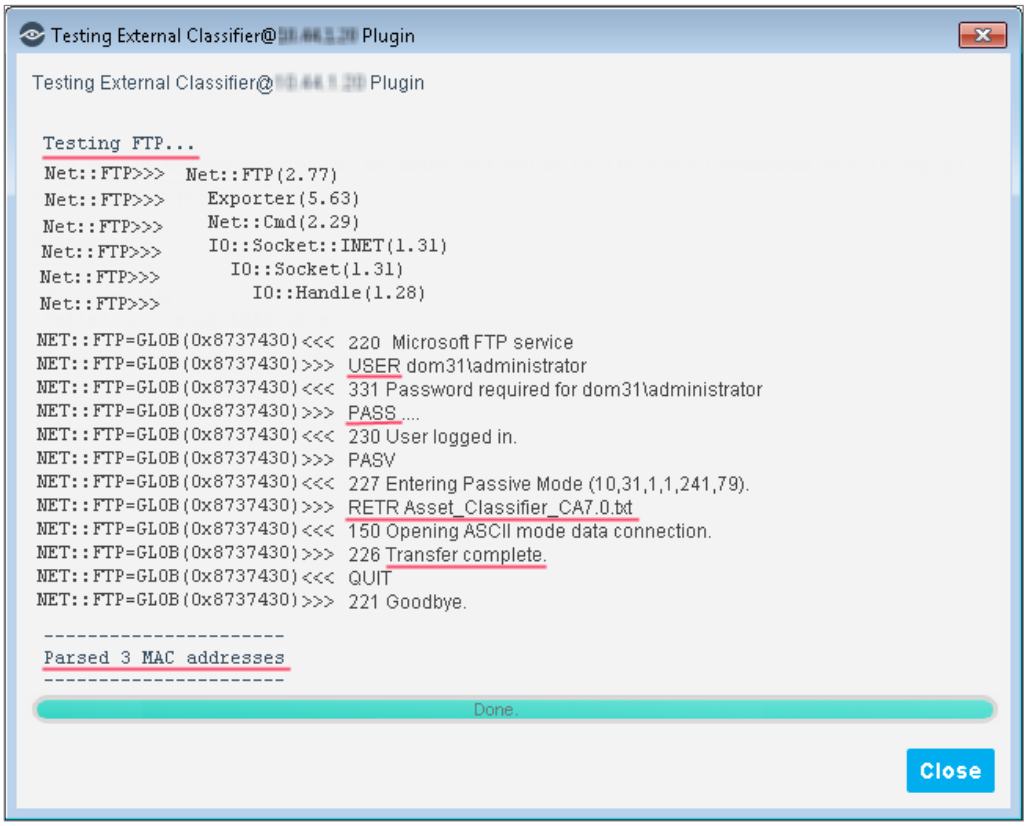


4. Select **Yes**. The Testing External Classifier Plugin window opens and displays the plugin test progress for the selected device.
5. When the window displays the test status **Done**, select **Close**.

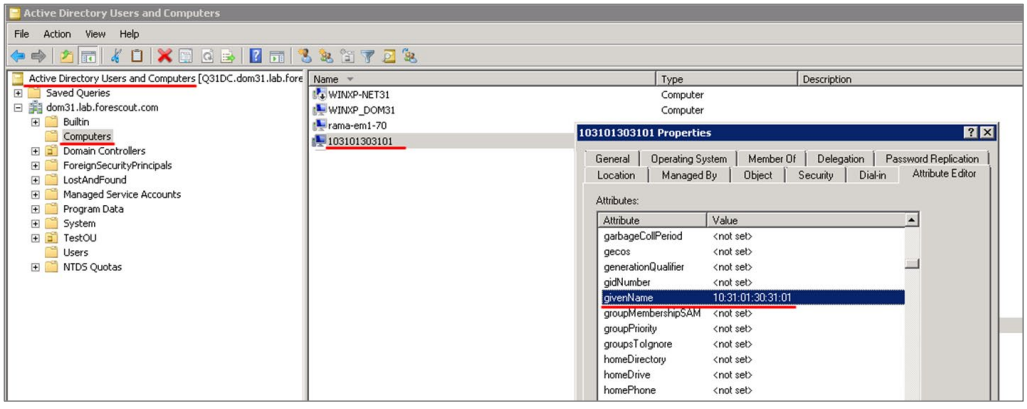
The following figure shows an example of an FTP file for download, containing a set of MAC addresses:



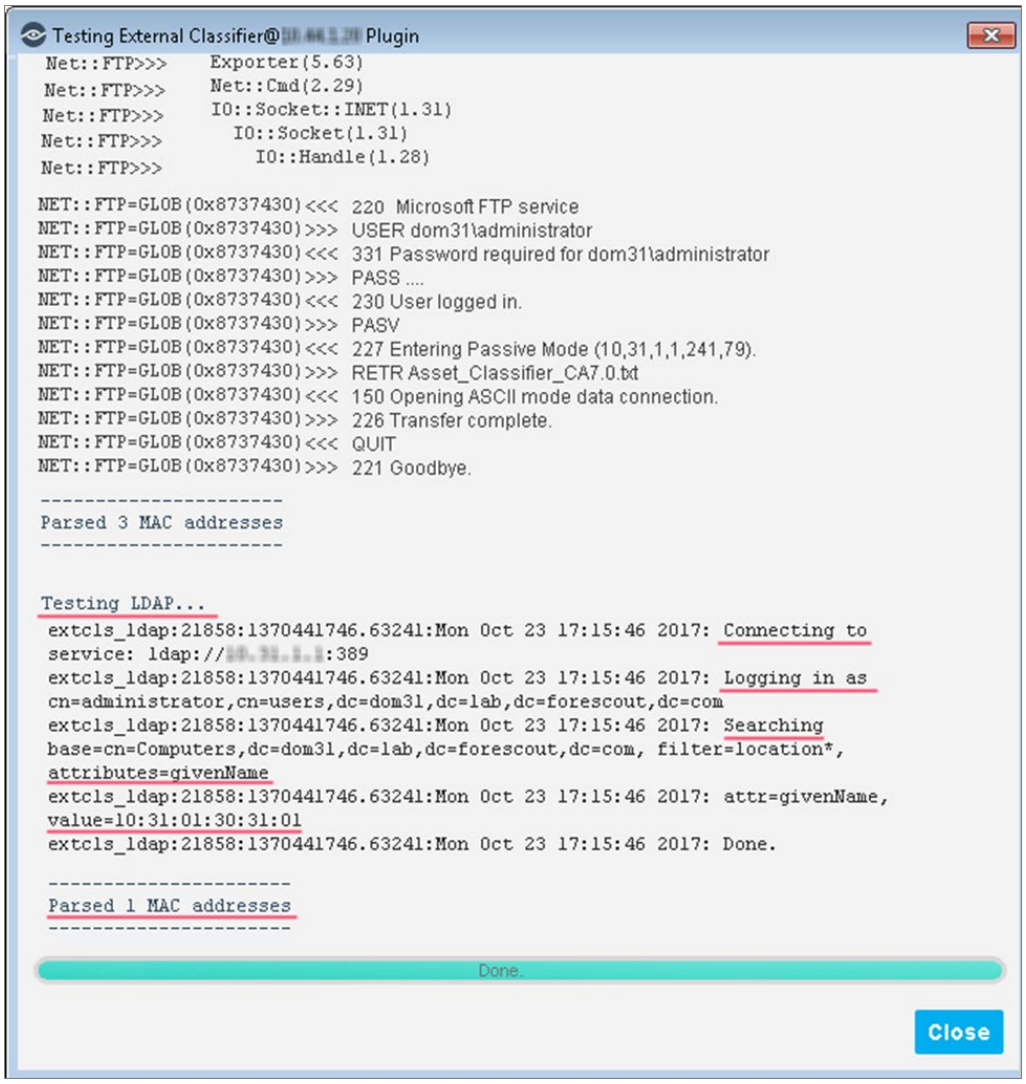
The following figure shows an example of the plugin test progress of an FTP file download:



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:



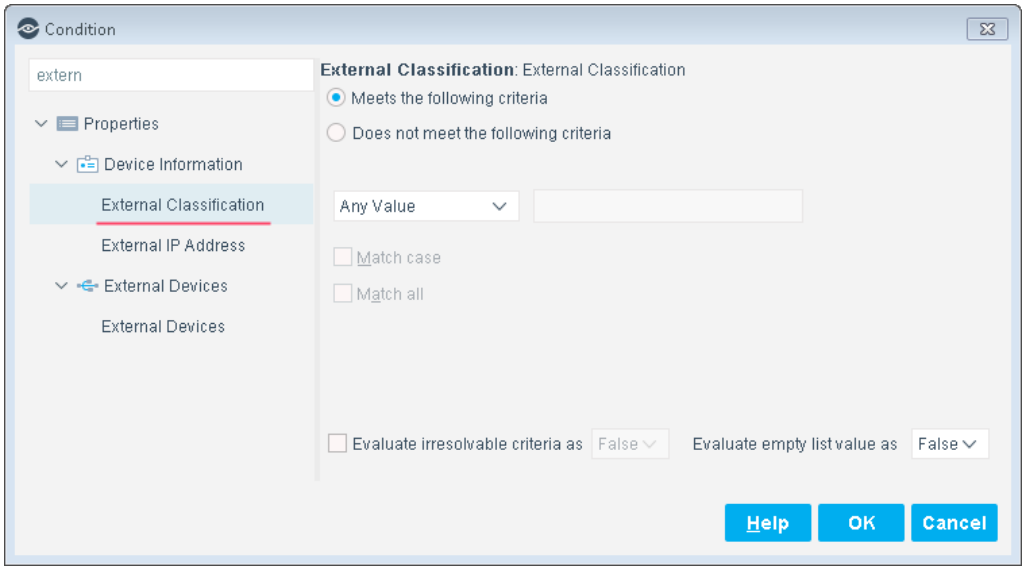
Use External Classification Information in Policies

Use the *External Classification* host property in Forescout platform policies to detect and control your network devices. In particular, for your unclassified network devices, extend *Primary Classification* and *Asset Classification* policies by incorporating use of the *External Classification* host property into these policies. Refer to the *Policy Management* chapter of the *Forescout Administration Guide* for more information about creating and updating policies. See Additional Forescout Documentation for information about how to access the guide.

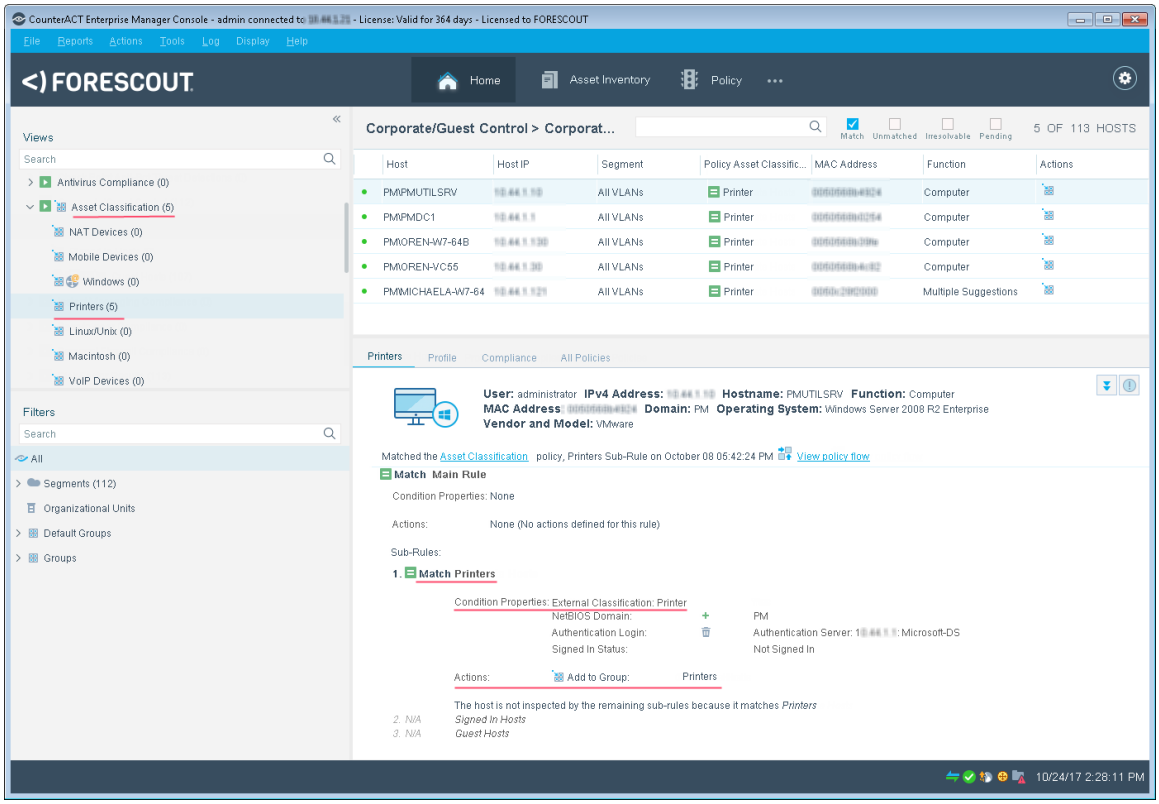
To work with a policy:

1. Log in to the Forescout 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.



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 one of the following ways:

- Via the Console, **All Hosts** pane. Display selected host details and expand its **Host** tab information.
- Generate a Device Details report. Select **Reports** from the Forescout 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.

Core Extensions Module Information

The External 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	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 Forescout Resources 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 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 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.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

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

Plugin Help Files

- After installing the plugin, 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).