Forescout

Core Extensions Module: Advanced Tools Plugin

Configuration Guide

Version 2.3.2

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 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

2020-04-16 12:27

Table of Contents

About the Forescout Advanced Tools Plugin

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

The Advanced Tools Plugin provides host properties and actions that enhance and extend existing functionality. For example, the plugin provides:

- More detailed endpoint detection

- Enhanced use of commands and scripts to retrieve endpoint information

- Use of labels and counters to implement complex policy logic, and to retain endpoint status across policy rechecks

Network Segments

These properties let you create policies that examine the network segment to which the endpoint is assigned:

- Segment path

- Segment name

Evaluate Commands and Scripts

This property-action pair lets you create policies that run scripts and check script results:

- Run Script on CounterACT action

- CounterACT Script Result property

Apply Text Labels

These properties and actions let you define and apply labels, and use those labels to select endpoints for further action:

- Assigned Label property

- Add Label action

- Delete Label action

Setting and Incrementing Counters

This property-action pair lets you define and increment counters based on policy matches, and use counter values to trigger further action:

- Set Counter action

- Counter property

Retrieve Endpoint Information

These properties let you invoke commands or run scripts on endpoints and use the results to select endpoints for further action.

- URL Content

- SNMPwalk Command Output

- SSH Command Output

- SSH Command Output (Interactive)

Resolve Dual-homed Endpoints as Managed or Unmanaged by SecureConnector

This property identifies dual-homed endpoints that are managed by SecureConnector on at least one interface:

- Windows Manageable SecureConnector (via any interface)

Add Property Values to a List

This action lets you place property values that match a policy condition into a list.

- Add Value to List action

What to Do

Perform the following to work with these properties and actions:

1. (Optional) Configure the plugin. You only need to configure the plugin if you are using the **Windows Manageable SecureConnector (via any interface)** host property.

2. Create policies that use these properties and actions and/or invoke actions when you review endpoints in various Console views.

Forescout Requirements

This section describes Forescout requirements for this release. Refer to the module Release Notes for updates regarding these requirements.

- Forescout version 8.1.4

- Endpoint Module version 1.1 with the HPS Inspection Engine running.

- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

Configure the Plugin

This section describes how to configure the plugin. This configuration is optional. Only enable this option if the property is required in your environment. See Resolve Dual-homed Endpoints as Managed or Unmanaged by SecureConnector.

To configure the plugin:

1. In the Forescout Console, select **Options** from the **Tools** menu.

2. Select **Modules > Core Extensions** and select **Advanced Tools Plugin** from the Modules pane.

3. Select **Configure**. The Advanced Tools Plugin configuration pane opens.

4. Select **Enable the Windows Manageable SecureConnector (via any interface) host property**.
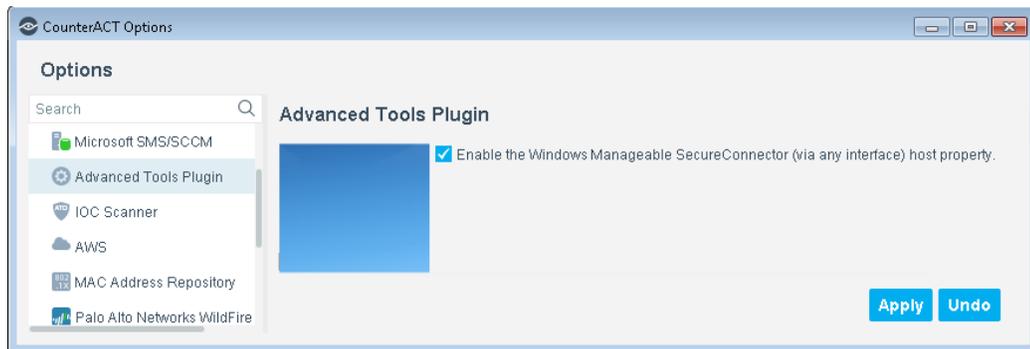
5. Select **Apply** to save configuration changes.

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.

Using Advanced Host Properties and Actions

Forescout *policies* use a wide range of conditions to trigger various management and remediation actions. When the *conditions* of the policy are met by an endpoint, the *actions* are implemented on the endpoint. In addition, you can apply actions directly to hosts at various Console views by right-clicking the host.

The following sections describe advanced properties and actions that are available with this plugin.

Network Segments

This section describes properties that examine the network segment in which a endpoint resides. Use these properties to create policies that apply actions to endpoints on a particular network segment. These properties are located in the Device Information group of the Properties tree.

Segment Name Property

This property retrieves the *leaf node name* of the network segment on which the endpoint resides. Condition options let you apply string matching criteria to this value.
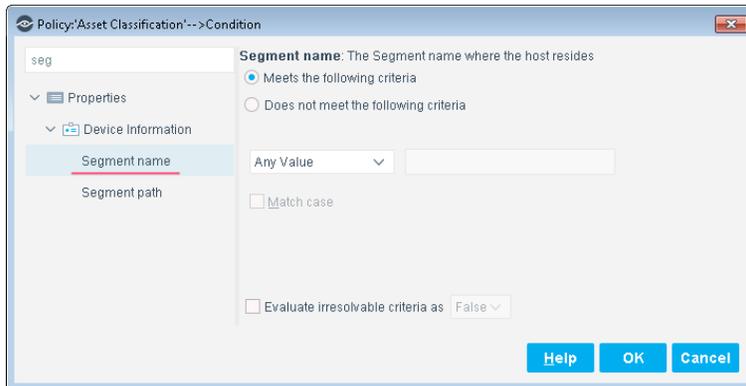
Segment Path Property

This property retrieves the *full pathname* of the network segment on which the endpoint resides. Condition options let you apply various string matching criteria to this value.
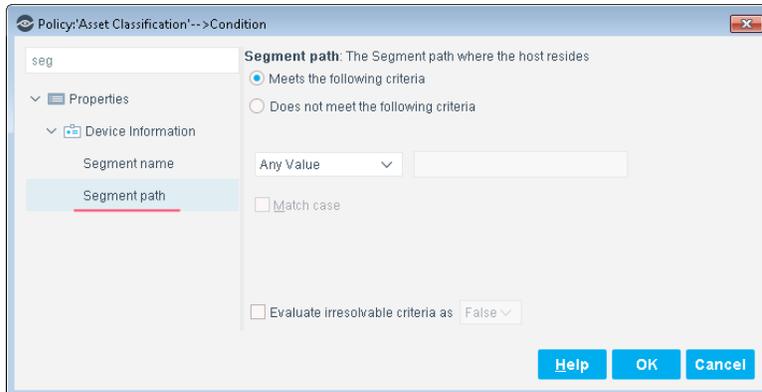
Evaluate Commands and Scripts

This section describes properties and actions that let you evaluate a script, command, or property value in a policy.

> 📄 *Unlike other script actions, these properties and actions run scripts and commands on the CounterACT appliance itself, and not on endpoints. In addition, you can use the script result as a policy condition.*

To specify a script or command for these properties and actions, do one of the following:

- Enter a script name or command directly in the **Command or Script** field. To include host properties in the command statement, select **Add Tags** to insert data tags that resolve to host property values.

- Select the **Command or Script** drop-down to view recently selected scripts and commands.

- Select the ellipsis icon [⋯] to build a library of scripts for this action. Scripts that you add appear in the command or script drop-down.

CounterACT Script Result Property

This condition runs a script or command on the CounterACT Appliance and examines the result. This property is located in the Device Information group of the Properties tree.

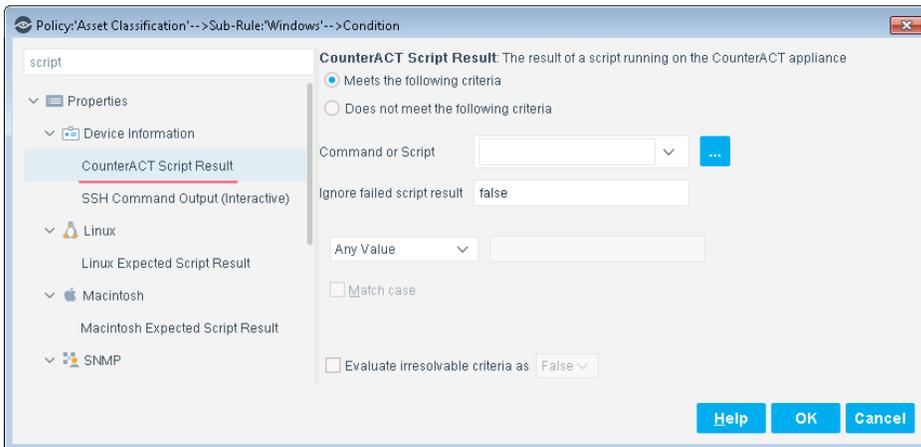The Forescout platform evaluates the script or command for each endpoint that matches previous conditions of the policy. This result is compared to the specified values and matching logic of the condition.

> 📑 *If you are running a script to retrieve a value that includes the endpoint's IP address, the script should not include the {IP} tag, as the IP address is automatically appended to the list of arguments passed to the script.*

Ignore Failed Script Result	Enter *true* to ignore any partial output received by before the session failed. The property is evaluated as *Irresolvable*.
	Enter *false* to preserve output from the failed session in the property and use that output to evaluate the condition.

Run Script on CounterACT Action

This action runs a script or command for endpoints that match the conditions of the policy. This action is located in the Remediate group of the Actions tree.

If you are using Flexx licensing, ensure that you have a valid *Forescout eyeControl* license to use this action. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.
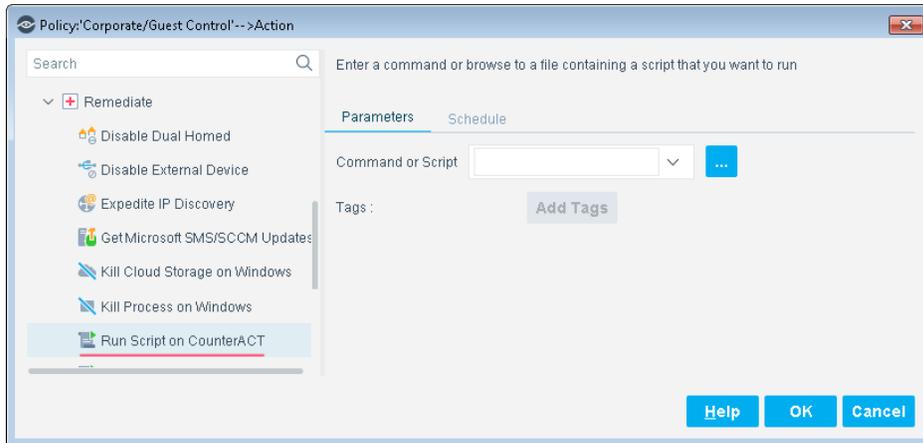
The Forescout platform evaluates the script or command for each endpoint that matches previous conditions of the policy.

> 📄 *If you are running a script in an action, the {IP} tag should be added to the script by the Administrator if it is required as an argument.*

Select the **Schedule** tab to apply scheduling options to this action.

Apply Text Labels

This section describes properties and actions that let you work with labels in policies. Labels mark and group endpoints based on properties or other evaluated values. Policies can apply further management logic based on labels assigned by a previous policy. This allows you to construct complex policy behaviors that track endpoint history.

For example, you can use labels to identify mobile devices by the gateways they use to enter the network. You can then identify usage patterns or cross-reference this information with other endpoint data to verify the user and limit access.

Assigned Label Property

This condition compares a text string to the labels assigned to the endpoint. This condition is located in the Device Information group of the Properties tree.
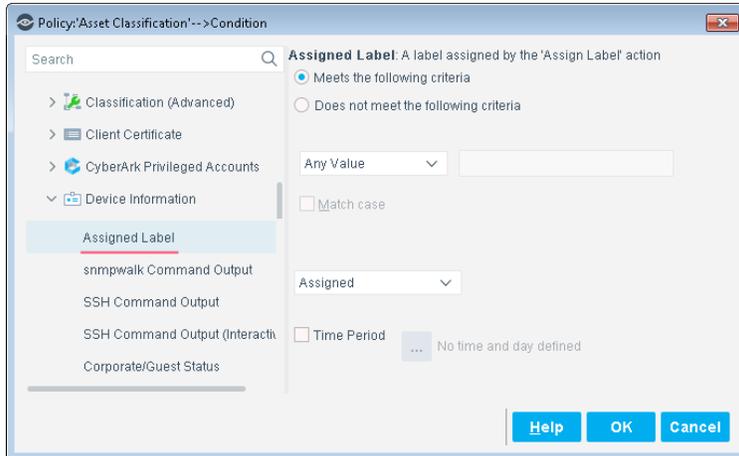
The text string you specify is compared to each of the labels assigned to the endpoint.

You can specify various matching logic options, such as partial string matching.

You can apply time constraints to the condition. Only endpoints that satisfy the matching condition during the specified time period are matched.

Add Label Action

This action assigns a text label to endpoints that match the conditions of the policy. This action is located in the Manage group of the Actions tree.
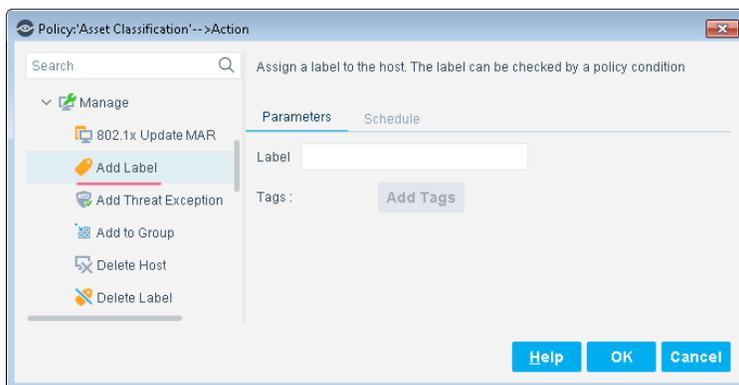
In the Label field, define the label text. The label can combine static text strings and endpoint-specific information. Select **Add Tags** to insert data tags that resolve to host property values. Labels are listed with other endpoint details in the Home and Asset Inventory views.

Delete Label Action

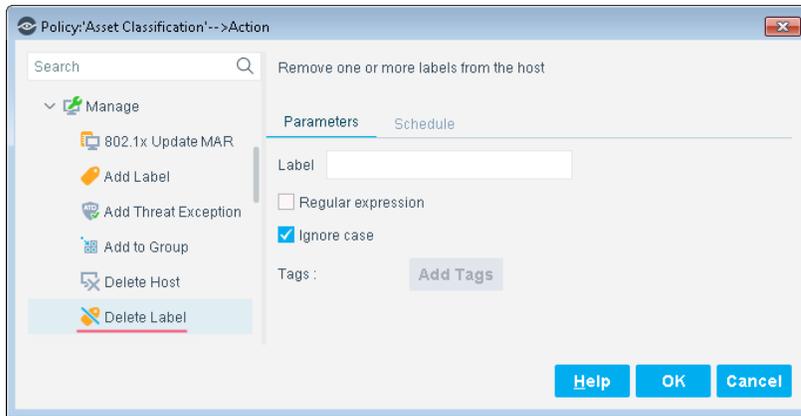This action removes a text label from endpoints that match the conditions of the policy. This action is located in the Manage group of the Actions tree.

In the Label field, define the label text. The label can combine static text strings and endpoint-specific information. Select **Add Tags** to insert data tags that resolve to host property values.

To delete several labels, enter a string using wildcard characters and then select **Regular expression**. All partially matched labels are deleted.

Select **Ignore case** to match labels only by spelling.

Setting and Incrementing Counters

This section describes properties and actions that let you set and evaluate counters in policies. Policies can trigger actions based on counters assigned and incremented previously by other policies. This allows you to use endpoint history in policies.

For example, if an endpoint repeatedly installs pluggable memory devices, you can invoke actions on the endpoint after this behavior is repeated a number of times. The use of counters lets you accommodate occasional use of hot-swappable memory and identify problematic repeat users.

When using counters in policies, note that:

▪ Counters are incremented each time an endpoint *returns* to the conditions of a policy, as follows:

   – The endpoint meets the conditions of the policy, and the counter is initialized.

   – Host properties change. The policy examines the endpoint and finds that it no longer satisfies the policy.

   – Host properties change again. The policy examines the endpoint again and finds that it satisfies the policy. The counter is incremented.

This is how the Forescout platform evaluates other policy conditions. However, counter values are *retained* even when the endpoint no longer satisfies the conditions of the policy.

> 📄 *Counters are maintained per endpoint – and like a host property, the same counter can have a different value for each endpoint.*

Using Counters in Policy Rules

Use properties and actions related to counters as follows:

- When you create a policy rule that defines a *new* counter, use only the Set Counter action.

- A policy rule that increments an *existing* counter must use both the Counter property and the Set Counter action:

  a. The rule contains a condition that uses the Counter property to verify the presence of the counter for an endpoint. Enable the **Evaluate irresolvable criteria as True** option when the Counter property is used to verify the presence of a newly created counter.

  b. Then the rule uses the Set Counter action to increment the counter on endpoints that match the condition.

Counter Property

This property compares the value of a counter to a numerical value. This condition is located in the Device Information group of the Properties tree.
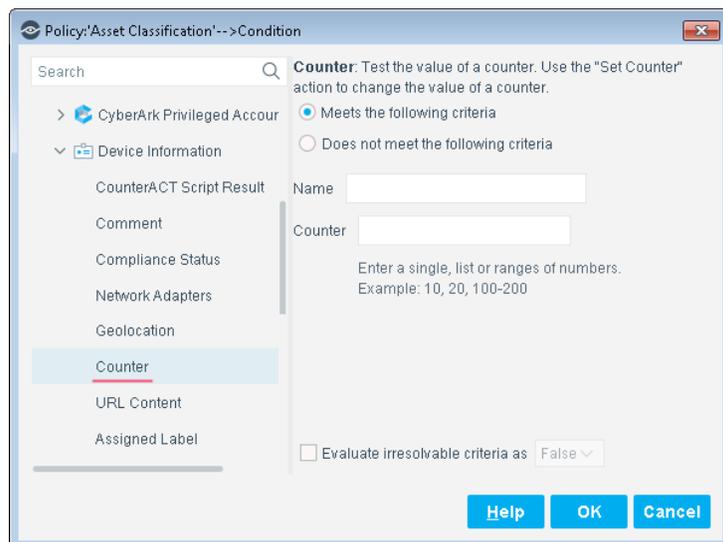
Enter the following values to create a condition based on a counter.

Name	The name of an existing counter.

Counter	Value(s) that the condition compares to the current value of the counter. You can specify a single value, a list of values, or a range of values.

> 📄 *Enable the **Evaluate irresolvable criteria as True** option when the Counter property is used to verify the presence of a newly created counter. See Using Counters in Policy Rules for more information.*

Set Counter Action

This action creates or increments a counter. This action is located in the Manage group of the Actions tree.
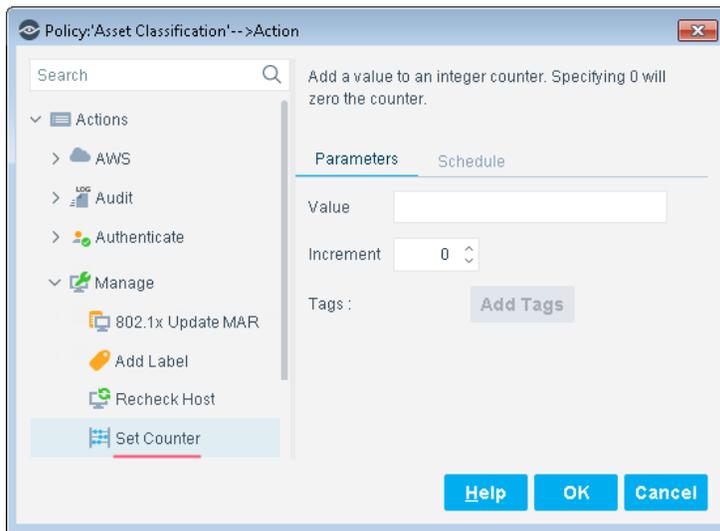
Use the following fields to define an action that creates a new counter or increments an existing counter.

Counter name	A text label for the counter. Because counters are maintained for each endpoint, this label can combine static text strings and endpoint-specific information to yield an endpoint-specific label. Select **Add Tags** to insert data tags that resolve to host property values.
Increment	The numerical value added to the existing value of the counter. The counter is incremented for an endpoint each time that endpoint matches the conditions of the rule. To reset an existing counter to zero, specify 0 in this field.

When you create a policy that defines a *new* counter, use only the Set Counter action. A policy that increments an *existing* counter must use both the Counter property and the Set Counter action. See Using Counters in Policy Rules for more information.

Retrieve Endpoint Information

The plugin provides the following *Device Information* properties to retrieve information from endpoints:

- Retrieve URL Content
- Retrieve snmpwalk Output
- Retrieve Output using an SSH Command
- Retrieve Output using an Interactive SSH Session

These properties let you extend and refine classification and compliance checking, supporting very fine-grained handling of non-standard endpoints. Use these properties to help you fine-tune or customize classification of endpoints. For example:

- When an endpoint is detected with a web interface, use the **URL Content** property to retrieve a known page on its web server. Policy conditions based on this property match web page content to further identify the endpoint.
- When a VoIP endpoint is detected, you may need to clarify the hardware model or firmware release of the device. Use the **SSH Command Output** properties to connect to the endpoint and run one or more commands on it. Policy conditions based on this property analyze the endpoint's responses to more accurately classify the device.

You can also extend and deepen policy-based management, creating policy conditions based on information not covered by other Forescout host properties or discovery processes. For example: the Forescout platform detects networked manufacturing robots running a niche real time operating system which cannot be identified or queried to check compliance. When these machines host an SSH server process, you can use the **SSH Command Output** properties to log in to the endpoints and verify correct configuration or other conditions for policy-based management.

Tracking Success and Failure of Retrieval Commands

You can track the success and failure of command(s) on endpoints by inspecting the last line of text in the property resolution. If there was a failure, the line will include the text *Exit Status:* followed by the numerical exit code provided by the endpoint's operating system. This information is presented the Console Detections Pane, in the Profile tab, All Polices tab, and other Console locations where property resolution details are available.

This option is available when you:

- Retrieve URL Content
- Retrieve snmpwalk Output
- Retrieve Output using an SSH Command
- Retrieve Output using an Interactive SSH Session

Retrieve URL Content

This property retrieves the content of a URL. You can create a condition that matches a regular expression or other text in the URL.

Use the following fields to define the URL target. Additional credentials can be added if required and additional customization options can be applied.
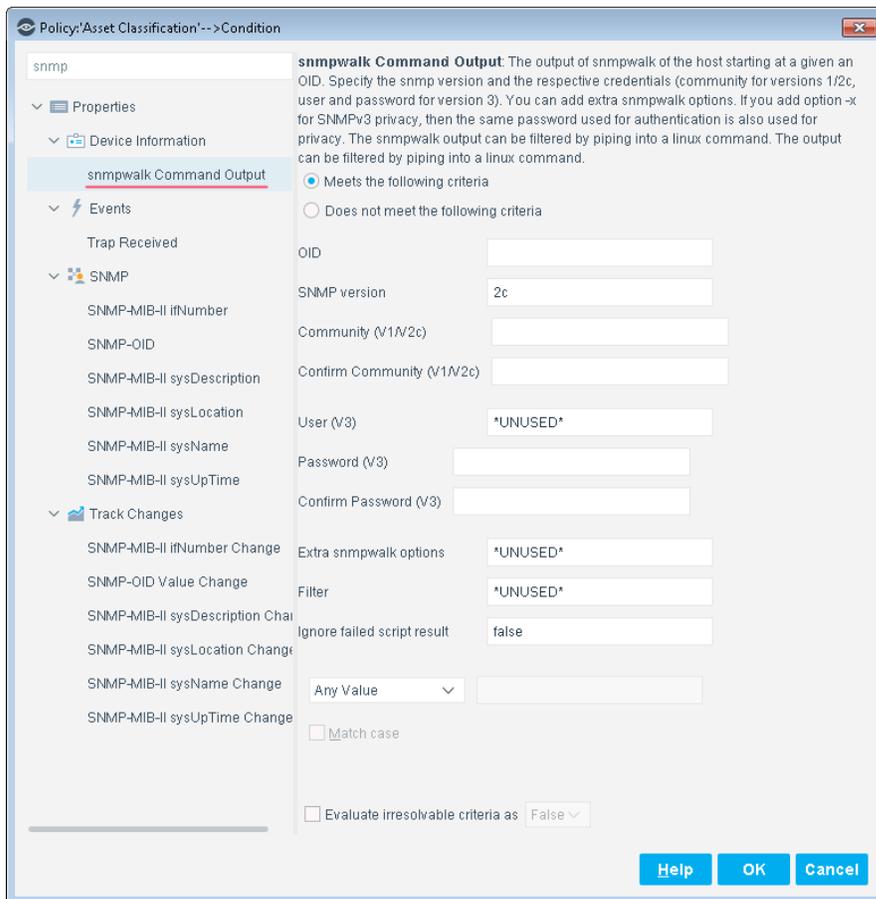
> 📄 *Enter *UNUSED* in a field if you want the Forescout platform to ignore the parameter.*

URL	Enter the path of the URL from which you want to retrieve information. You can use the {ip} tag to specify the endpoint IP address, for example http://{ip}/info.html
User/Password	Enter user credentials if access to the page requires authentication.
Kerberos Domain	Specify a Kerberos (ActiveDirectory) domain if the user is part of a domain.
Scrub HTML	Type *true* in order to remove HTML tags. Type *false* to display tags.
Extra curl options	Set additional curl options (check out 'man curl' on Linux)
Filter	Include only specific information in the output by piping into a Linux command. For example, to exclude the text XYZ use " grep –v "XYZ""

Ignore Failed Script Result	Enter *true* to ignore any partial output received before the session failed. The property is evaluated as *Irresolvable*.
	Enter *false* to preserve output from the failed session in the property and use that output to evaluate the condition.

Retrieve snmpwalk Output

This property retrieves snmpwalk output from a given OID. You can create a condition that matches a regular expression or other text in the output.

Use the following fields to define the snmpwalk to be retrieved. Filters and customization options can be applied.

> 📄 *Enter *UNUSED* in a field if you want the Forescout platform to ignore the parameter.*

OID	Enter the ID.
SNMP version	Enter the SNMP version.
Community	Enter the community for versions 1/2c.
User (V3)	Enter the user and password (version 3).

Password (V3)	Enter the user and password (version 3).
Extra snmpwalk options	Include additional snmpwalk options. If you include -x for SNMPv3 privacy, the same password used for authentication is used for privacy.
Filter	Include only specific information in the output by piping into a Linux command.
Ignore Failed Script Result	Enter *true* to ignore any partial output received before the session failed. The property is evaluated as *Irresolvable*. Enter *false* to preserve output from the failed session in the property, and use that output to evaluate the condition.

Retrieve Output using an SSH Command

Retrieve output of a command run on the endpoint using SSH. Filters and customization options can be applied.

Use the following fields to specify SSH session details and the command to be submitted on the endpoint. Filters and customization options can be applied.

> 📄 *Enter *UNUSED* in a field if you want the Forescout platform to ignore the parameter.*

SSH Username	Specify credentials used to log in and establish an SSH session on the endpoint. Note that these credentials are not encrypted.
SSH Password	

SSH Connection Flags (optional)	(Optional) Specify additional Open SSH option flags that are applied when the SSH session is established.
Command	Enter the command submitted on the endpoint.
Pipe session through AWK filter (optional)	(Optional) Specify a Linux filter command to filter output before evaluating the condition.
When command/session fails, evaluate condition	Select **as Irresolvable** to ignore any partial output when the session fails. The property is evaluated as Irresolvable. Select **Based on data received** to preserve output from the failed session in the property and use that output to evaluate the condition.

Retrieve Output using an Interactive SSH Session

This property captures the output of an interactive script run on the endpoint during an SSH session. The SSH session is established using OpenSSH.

Use the following fields to specify SSH session details and the commands to be submitted on the endpoint. Filters and customization options can be applied.

> 📄 *Enter* *UNUSED* *in a field if you want the Forescout platform to ignore the parameter.*

SSH Username	Specify credentials used to log in and establish an SSH session on the endpoint. Note that these credentials are not encrypted.
SSH Password	
SSH Connection Flags (optional)	(Optional) Specify additional Open SSH option flags that are applied when the SSH session is established.
Interactive Session Script	Enter an alternating series of commands and expected responses, beginning with a command. Each command is on an odd numbered line, each expected response is on an even line. Expected response lines contain regular expressions used to match actual output.
Response timeout	The maximum interval, in seconds, that the Forescout platform waits after submission of each command for an output response.
Login timeout	The maximum interval, in seconds, that the Forescout platform waits when it logs in to establish the SSH session.
Pipe session through AWK filter (optional)	(Optional) Specify a Linux filter command to filter session output before evaluating the condition.
When command/session fails, evaluate condition	Select **as Irresolvable** to ignore any partial output when the session fails. The property is evaluated as Irresolvable. Select **Based on data received** to preserve output from the failed session in the property and use that output to evaluate the condition.

After an SSH session is established on the endpoint, the first command listed in the **Interactive Session Script** field is submitted. The Forescout platform waits for a response and tests the response output against the expected response in the next line of the script.

- If the actual response output does not match the expected response, or if the session times out without a response, the interactive session is ended.

- If the output matches the expected response, the next command in the session script is submitted.

The session is ended after a response is received for the last command, or after the session times out.

The property contains a log of all submitted commands and complete actual responses.

Resolve Dual-homed Endpoints as Managed or Unmanaged by SecureConnector

The plugin provides an optional host property that lets you correctly resolve dual-homed endpoints as managed or unmanaged by SecureConnector.

When an endpoint with multiple interfaces connects to the Forescout platform through one NIC, only that host (NIC) is resolved as *Managed by SecureConnector*.

When Forescout policies apply actions to dual-homed endpoints that are not managed by SecureConnector, actions are applied to all interfaces of the endpoint, even if another host (NIC) on the same endpoint is managed by SecureConnector. As a result, the endpoint may lose access to network services it uses.

Use the **Windows Manageable SecureConnector (via any interface)** property to resolve a secondary (unmanaged) interface on the endpoint as managed if another host (NIC) on the endpoint is already managed by SecureConnector.

This property can be used in environments where Windows endpoints are ***solely*** managed by SecureConnector.

Sample Use Case

- Network Windows laptops utilize both wired and wireless connections (simultaneously and separately).

- Applications on the laptops require use of both network connections.

- Policies are deployed that remediate/restrict/block endpoints not managed by Secure Connector.

- SecureConnector is installed on endpoints and connects to the Forescout platform via the wired interface.

- When the wired endpoint is detected the Windows Manageable SecureConnector host property is evaluated as *True*. When the wireless endpoint is detected the Windows Manageable SecureConnector property is evaluated as *False* – and block/remediation actions will be performed on the wireless endpoint. This will also impact the endpoint.

- Applications accessed from the wireless connection are blocked if the policy performs a block action.

Windows Manageable SecureConnector (via any interface) Property

When endpoints are managed with SecureConnector, one host/interface may be managed by SecureConnector and another may not be managed. Use the optional **Windows Manageable SecureConnector (via any interface)** property to resolve a secondary (unmanaged) host on the endpoint as managed if another host (NIC) on the endpoint is already managed by SecureConnector.

This property can be used in environments where Windows endpoints are *solely* managed by SecureConnector.

To use this property, select the **Enable the Windows Manageable SecureConnector (via any interface) host property** option when you configure the plugin.

> 📄 *When this property is active, it requires significant processor and memory resources on CounterACT devices. Only enable and use this property if compliance policies in your environment require identification of managed and unmanaged interfaces on dual-homed devices.*
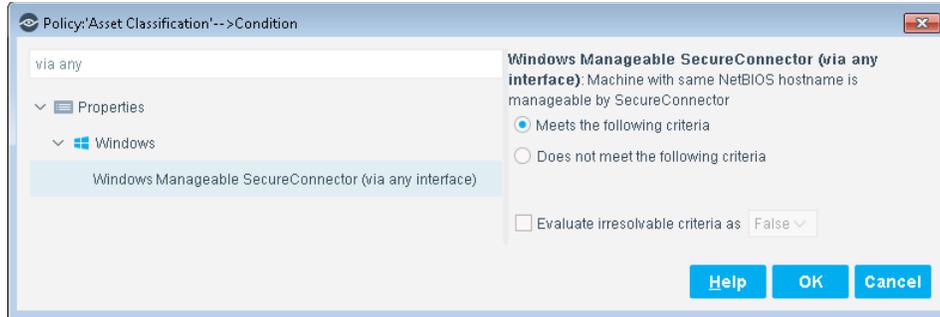
To resolve this property, endpoint identity information is synchronized by resolving the NetBIOS name on each endpoint host. The Forescout platform then examines the Windows Manageable SecureConnector host property to determine if any hosts on the endpoint are managed by SecureConnector.

- If NetBIOS names match, and *one* of the hosts is managed by SecureConnector (Windows Manageable SecureConnector = True) the Windows Manageable SecureConnector (via another interface) property is resolved as True, and the endpoint complies with policies that detect endpoints that have SecureConnector installed.

- If the NetBIOS names match and *neither* host on an endpoint is managed by SecureConnector (Windows Manageable SecureConnector = False), the Windows Manageable SecureConnector (via another interface) property is resolved as False, and the endpoint does not comply with policies that detect endpoints that have SecureConnector installed.

Windows Manageable SecureConnector	Windows Manageable SecureConnector (via another interface)	Evaluated as Managed by SecureConnector
True	True	**Yes**
False	True	**Yes**
False	False	**No**

Create a Policy that Detects Dual Homed Managed Endpoints

Use the procedure below to modify policies to detect dual-homed endpoints managed by SecureConnector through one host and not managed on the other. Endpoints that meet this criterion can be defined as compliant in policies that verify SecureConnector management. This means that the non-SecureConnector managed host will still be accessible to the network services it uses.

If you create new policies that verify SecureConnector manageability, use the rule definitions described below to detect dual-homed endpoints managed by SecureConnector through one host and not managed on the other.

To detect dual homed endpoints managed by SecureConnector:

1. Edit a policy that evaluates the *Windows Manageable SecureConnector* property.

2. Navigate to the rule that references the *Windows Manageable SecureConnector* property and select **Edit**.

3. In the Conditions section of the Policy dialog box select **Add**.

4. In the Properties tree, select the *Windows Manageable SecureConnector (via any interface)*. Select **Meets the following criteria**.

5. Select **OK**. The property appears as a criterion of the condition.

6. In the Condition section of the Policy dialog box, select **One criterion is true**.

7. Verify that the condition is defined as follows:

   One of the following criteria is True:

   – *Windows Manageable SecureConnector* property
   – *Windows Manageable SecureConnector (via any interface)* property
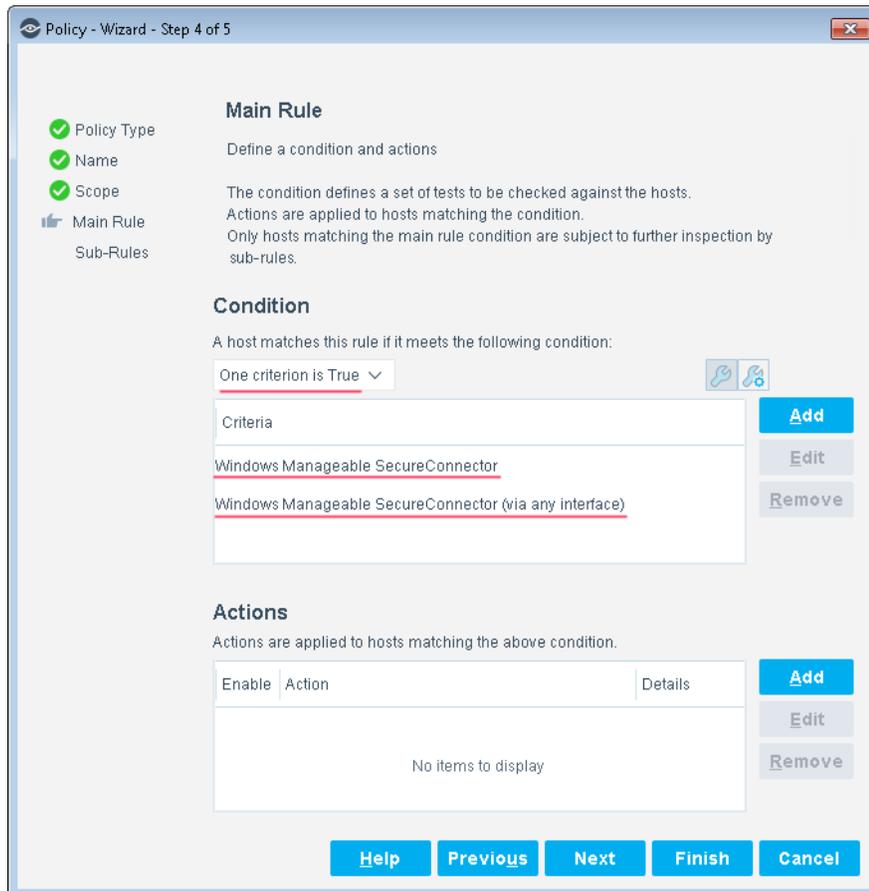
8. Save changes to the policy.

9. Repeat this procedure for all relevant policies that evaluate the *Windows Manageable SecureConnector* property.

Add Property Values to a List

This section describes an action that helps you work with property values and lists in policies. Lists contain endpoint properties and related values that are referenced by policy conditions. For example, a list of domain user names or a list of DNS names, or of processes that you want to prohibit on your network. Each List is associated with a single endpoint property and can contain multiple related values. Using lists speeds up and streamlines the policy creation and endpoint management process.

Add Value to List Action

Use the Add Value to List action to place property values that match a policy condition into a list. For example, place all logged-in users of hosts at which a malicious event was detected by Forescout eyeSight into a 'Malicious Users' list. You can then use this list to define a policy that performs a restrict action on other hosts where the user logged-in to.
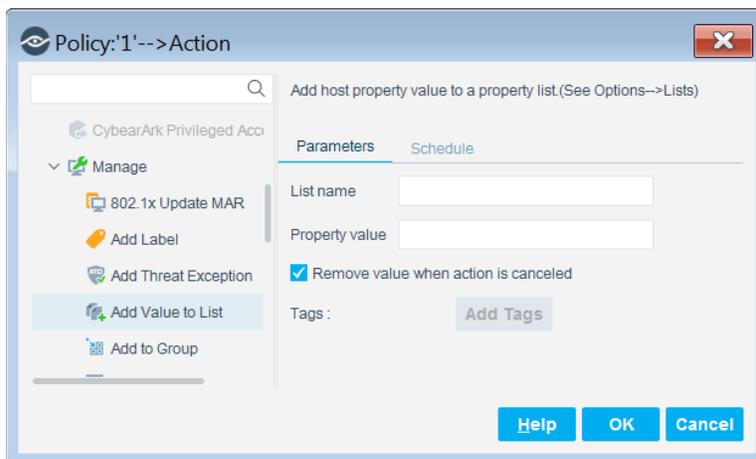
In the **List name** field, enter the name of the list that you want to add the property value to. The list name you enter must match the name of a previously defined list.

In the **Property value** field, use tags to define endpoint-specific property values. Select **Add Tags** to insert data tags that resolve to host property values.

Select the **Remove value when action is cancelled** option to remove the value from the list when the action is cancelled (i.e. when the host no longer matches the policy rule).

Core Extensions Module Information

The Advanced Tools 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).