ForeScout CounterACT®

Core Extensions Module: Advanced Tools Plugin

Configuration Guide

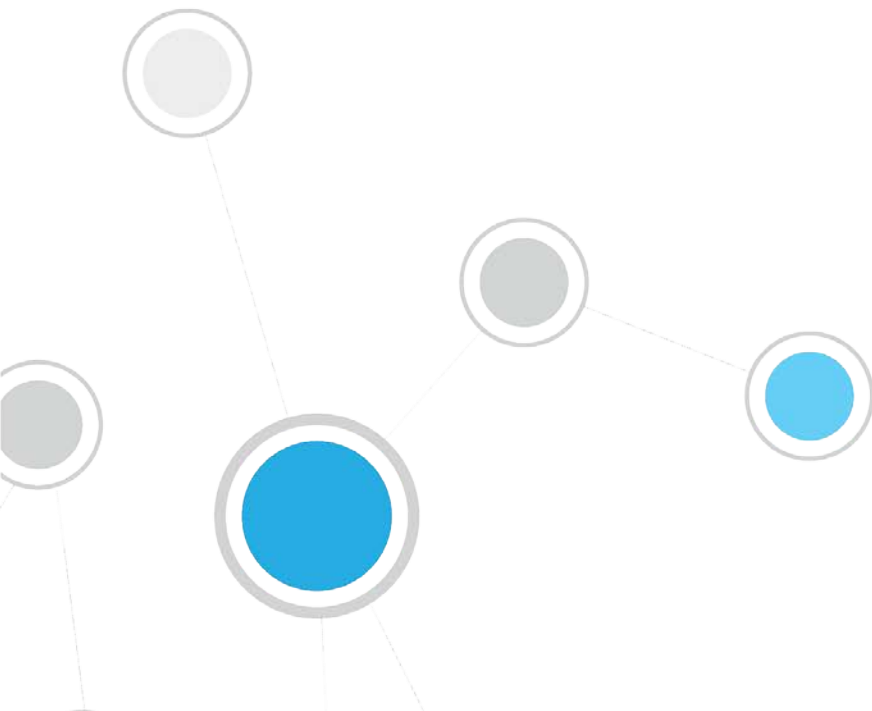**Version 2.2.4**

Table of Contents

About the CounterACT Advanced Tools Plugin

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

The Advanced Tools plugin provides host properties and actions in CounterACT 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)

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.

Requirements

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

- CounterACT version 8.0

- Endpoint Module version 1.0 with the HPS Inspection Engine running.

- An active Maintenance Contract for CounterACT devices is required.

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 CounterACT 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**.
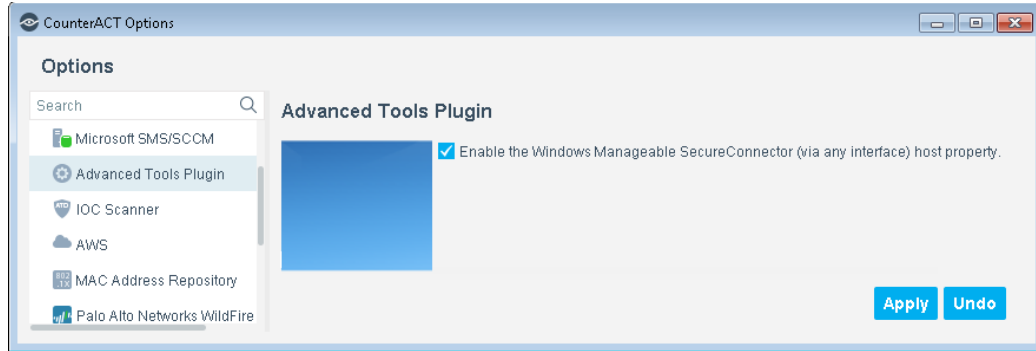
5. Select **Apply** to save configuration changes.

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

CounterACT *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.
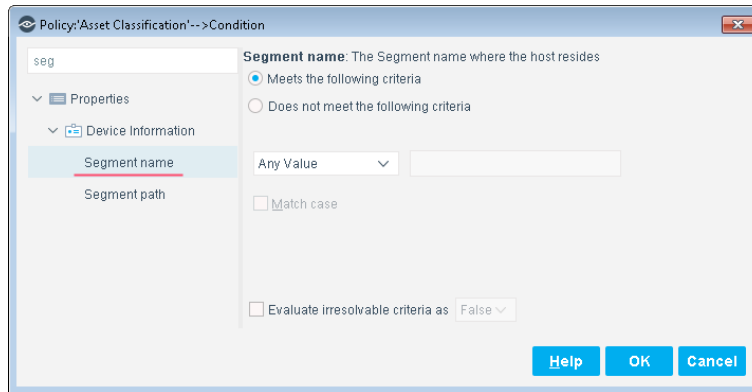
Segment Path Property

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.
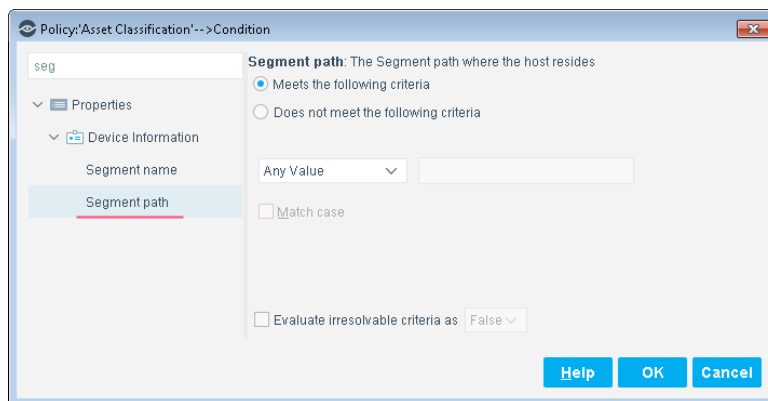
Evaluate Commands and Scripts

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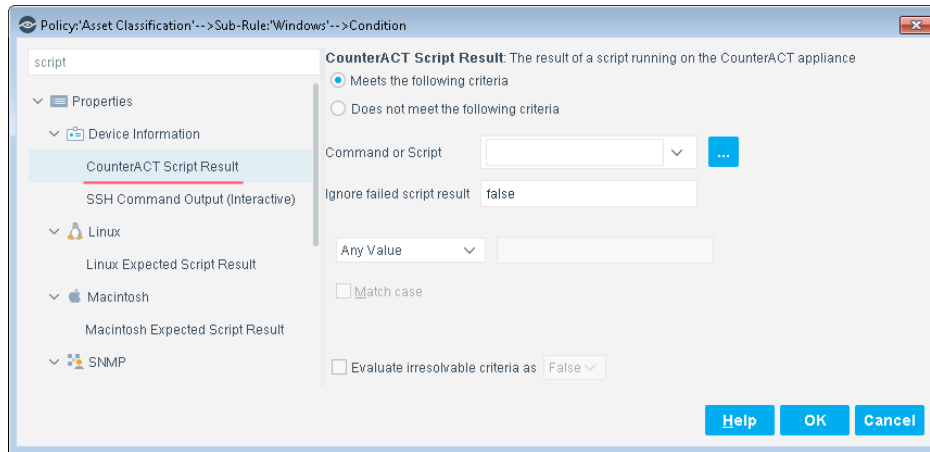
CounterACT evaluates the script or command for each endpoint that matches previous conditions of the policy. This result is compared to the specified values and matching logic of the condition.

> 📄 *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 CounterACT automatically appends the IP address to the list of arguments passed to the script.*

Ignore Failed Script Result	Enter *true* to ignore any partial output received by CounterACT 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

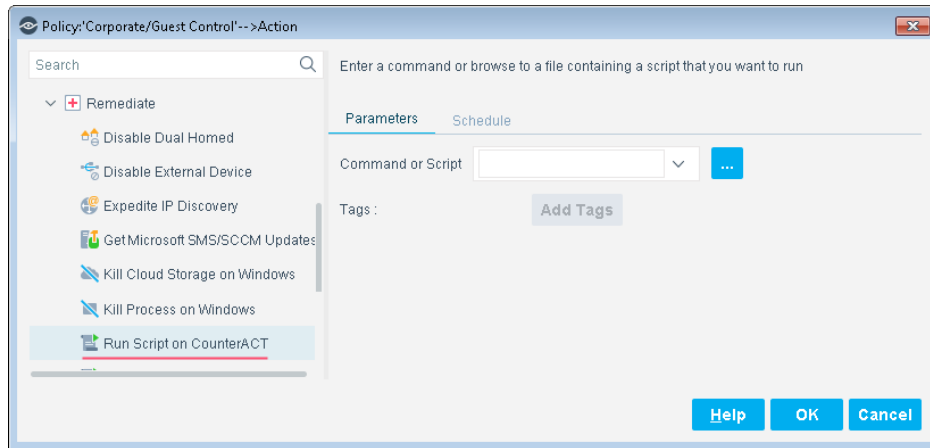This action runs a script or command for endpoints that match the conditions of the policy. This action is located in the Remediate group of the Actions tree.

CounterACT 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.
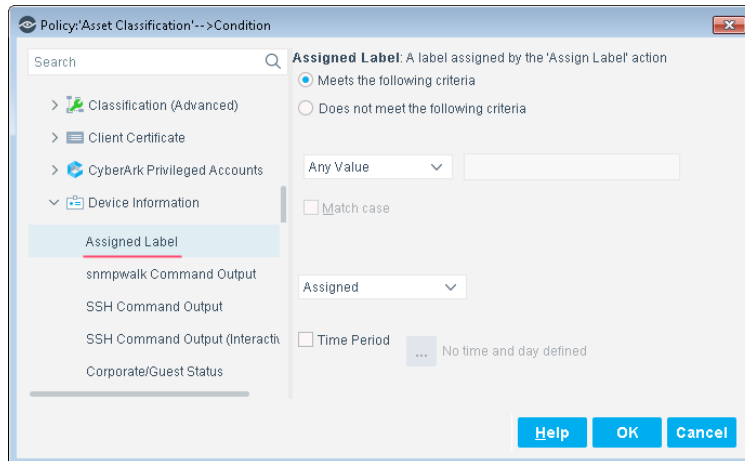
The text string you specify is compared to each of the labels assigned to the endpoint.

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

You can apply time constraints to the condition. CounterACT matches only endpoints that satisfy the matching condition during the specified time period.

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.
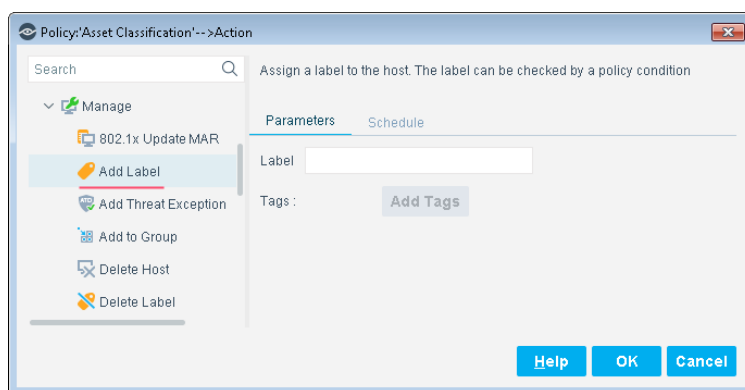
In the Label field, define the label text. The label can combine static text strings and endpoint-specific information. Select **Add Tags** to insert data tags that resolve to host property values. Labels are listed with other endpoint details in the Home and Asset Inventory views.

Delete Label Action

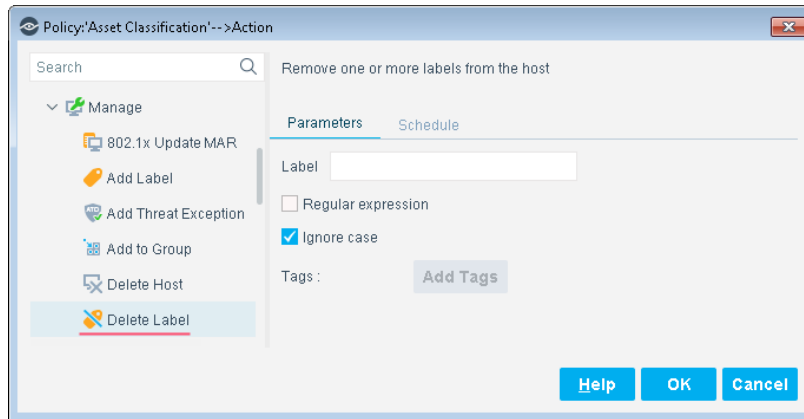This action removes a text label from endpoints that match the conditions of the policy. This action is located in the Manage group of the Actions tree.

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 CounterACT 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.
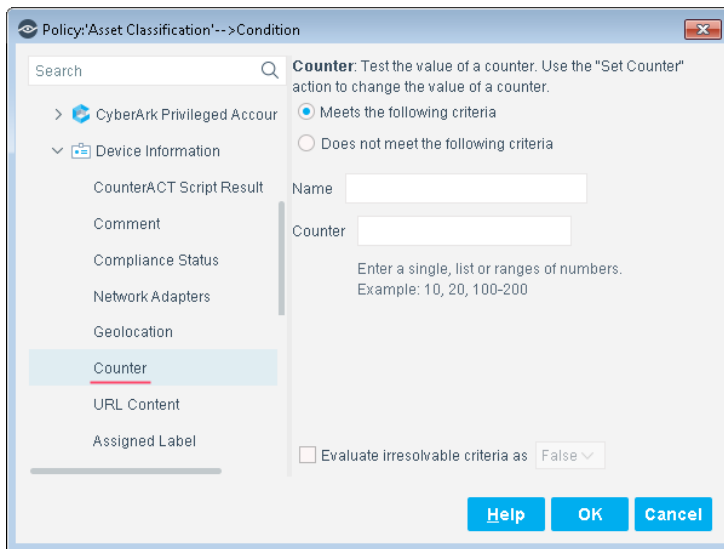

Enter the following values to create a condition based on a counter.

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.
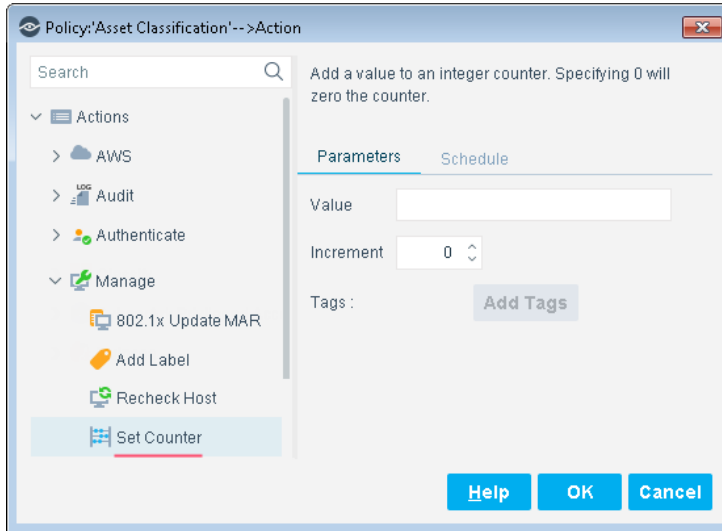
Use the following fields to define an action that creates a new counter, or increments an existing counter.

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 SSH Commands

- Retrieve Output using an Interactive SSH Session

These properties let you extend and refine CounterACT 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 CounterACT detects an endpoint 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 CounterACT detects a VoIP endpoint, 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 CounterACT host properties or discovery processes. For example: CounterACT detects networked manufacturing robots running a niche real time operating system which CounterACT cannot identify or query 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.
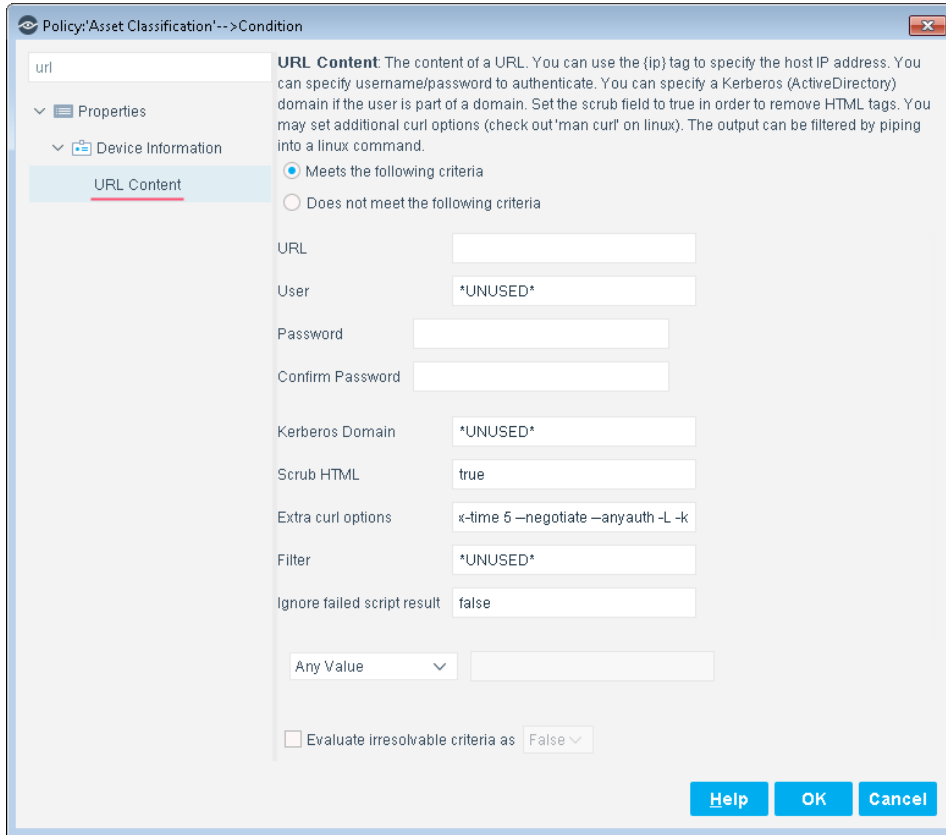
Use the following fields to define the URL target. Additional credentials can be added if required and additional customization options can be applied.
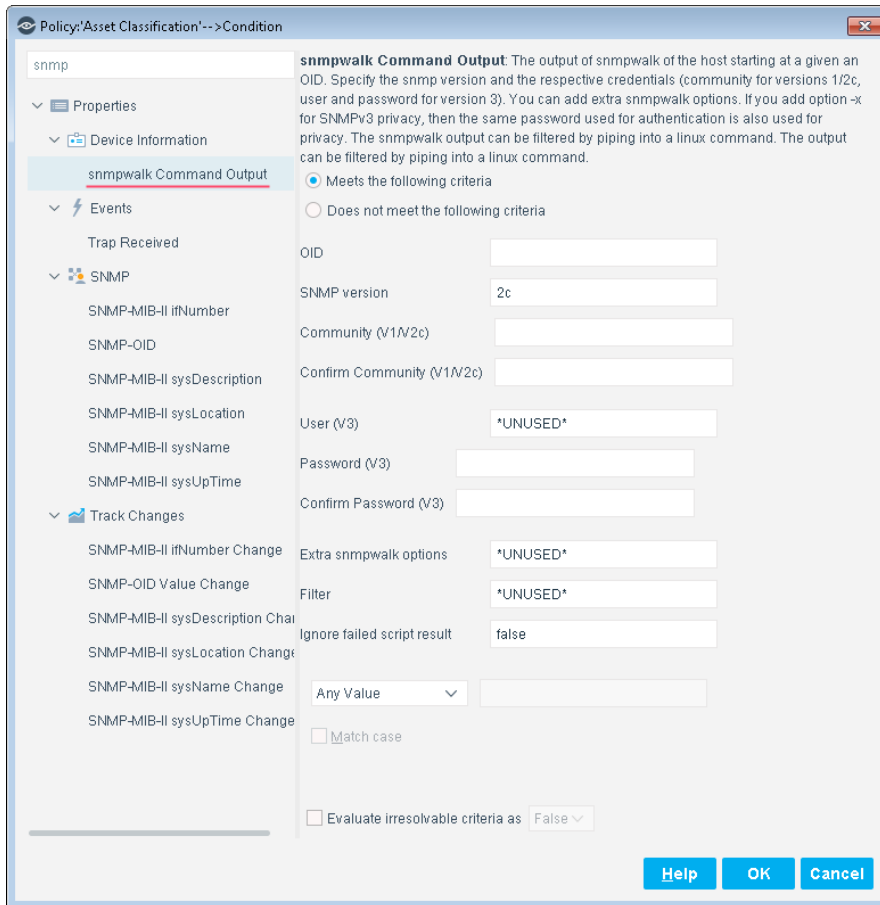
> 📄 *Enter *UNUSED* in a field if you want CounterACT to ignore the parameter.*

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 by CounterACT 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.
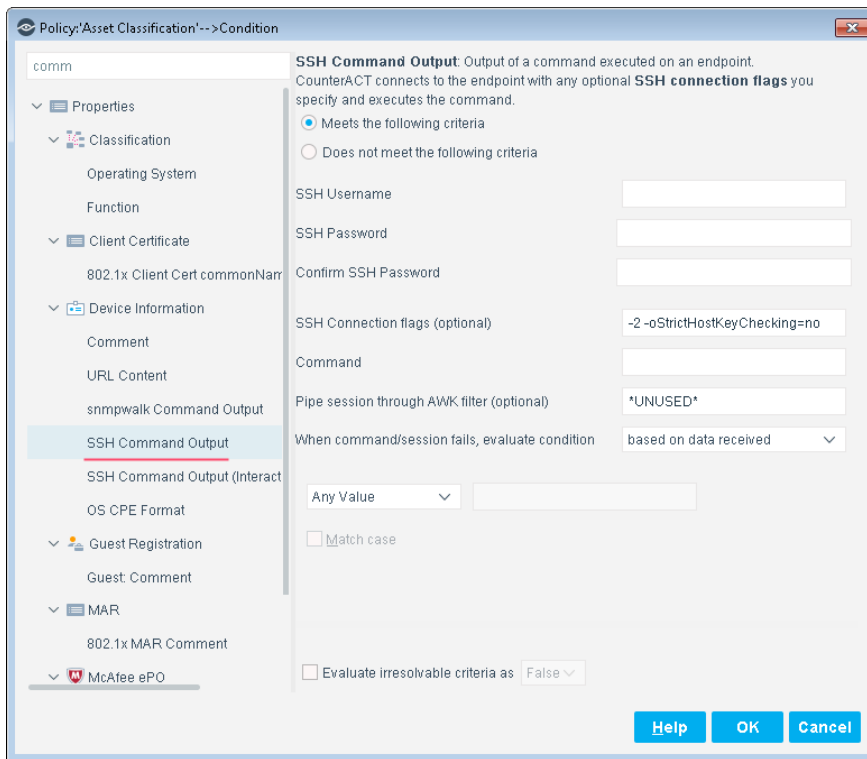
📄 *Enter *UNUSED* in a field if you want CounterACT to ignore the parameter.*

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 by CounterACT 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 CounterACT 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 CounterACT 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 CounterACT waits after submission of each command for an output response.
Login timeout	The maximum interval, in seconds, that CounterACT 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 CounterACT establishes an SSH session on the endpoint, it submits the first command listed in the **Interactive Session Script** field. CounterACT 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, CounterACT ends the interactive session.

- If the output matches the expected response, CounterACT submits the next command in the session script.

CounterACT ends the session 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 CounterACT through one NIC, only that host (NIC) is resolved as *Managed by SecureConnector*.

When CounterACT 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 CounterACT 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.
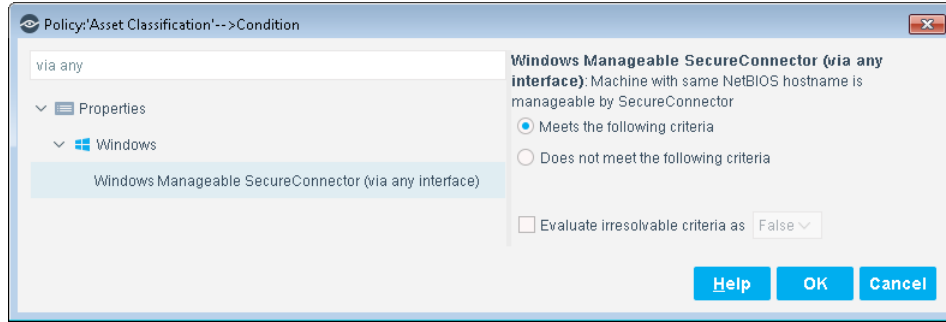
Windows Manageable SecureConnector (via any interface) Property

When CounterACT manages endpoints 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, CounterACT synchronizes endpoint identity information by resolving the NetBIOS name on each endpoint host. CounterACT 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
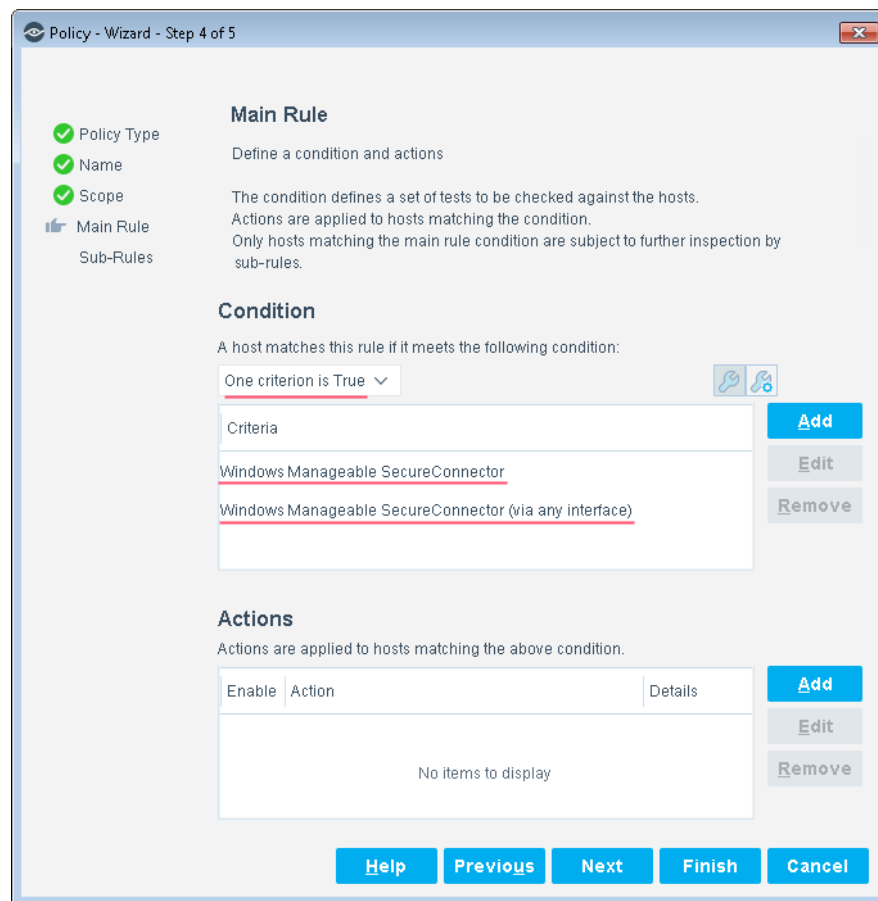
8. Save changes to the policy.

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

Core Extensions Module Information

The Advanced Tools plugin is installed with the CounterACT Core Extensions Module.

The Core Extensions Module provides an extensive range of capabilities that enhance the core CounterACT solution. These capabilities enhance detection, classification, reporting, troubleshooting and more, and include the following components:

- Advanced Tools Plugin
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
- IOC Scanner Plugin
- IoT Posture Assessment Engine
- NBT Scanner Plugin
- NetFlow Plugin
- Reports Plugin
- Syslog Plugin
- Technical Support Plugin
- Web GUI Plugin

The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are released and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Guide* for more module information, for example module requirements, upgrade and rollback instructions. See Additional CounterACT Documentation for information about how to access the module guide.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal

- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

  Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

  If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.

2. Select the plugin and then select **Help**.

Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21