



ForeScout CounterACT[®]

Classify Devices

How-to Guide

Version 8.0

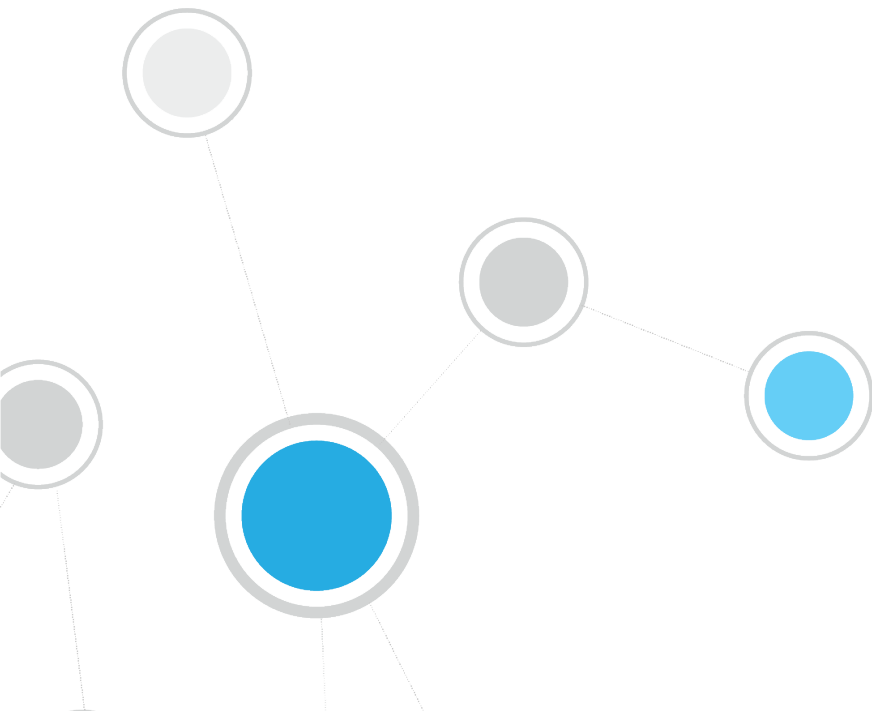




Table of Contents

About Device Classification	3
Groups That Can Be Created by the Policy	3
Prerequisites	4
Create a Primary Classification Policy	5
View Endpoints per Classification Metric	10
View Classifications per Endpoint.....	11
Replace an Asset Classification Policy	12
Fine-Tune Device Classification	12
Improve Classification for Individual Endpoints	13
Improve Classification Using a Policy	14
Additional CounterACT Documentation	16
Documentation Downloads	16
Documentation Portal	17
CounterACT Help Tools.....	17



About Device Classification

ForeScout CounterACT[®] provides powerful tools that let you continuously track, control and profile devices connected to your network.


Follow the step-by-step procedures in this guide to use a wizard-based policy template that:

- Resolves several endpoint classification properties, including the following:
 - Function
 - Operating System
 - Vendor and Model
- Demonstrates a broad policy-based classification of the devices according to the device types commonly found in many environments.

It is recommended to use the wizard-based *Primary Classification* policy template to create a policy that fully leverages the CounterACT classification technology, and then enhance the policy to meet your needs. For example, if your environment contains many IP-connected security cameras from a particular vendor, you may want to create an additional sub-rule to group those devices.

If you currently use an *Asset Classification* policy, the *Primary Classification* policy may provide more comprehensive classification in your environment. For more information, see [Replace an Asset Classification Policy](#).

After the policy is run, you can use CounterACT tools to review an extensive range of information about each device and about the users connected to them.

 *This How-to guide provides basic configuration instructions designed for a quick setup. For more information on the extended configuration options, refer to the CounterACT Administration Guide.*

Groups That Can Be Created by the Policy

Organizing all the connected devices into CounterACT groups makes it easier to create and manage other policies and track policy results. If the *Add to Group* actions are enabled in the *Primary Classification* policy, the following groups are created and populated:

- CounterACT Devices
- Storage
- NAT devices: Devices that may hide other devices.
- Mobile devices
- Windows
- Printers
- Linux/Unix
- Macintosh
- VoIP devices



- Network devices: Networking equipment, such as WLAN controllers, routers, switches, and wireless controllers.
- Unclassified: If CounterACT does not know to which category an endpoint is associated. This may happen, for example, if network devices are new.

Prerequisites

This solution requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0.
- Device Profile Library. This is a Content Module that delivers a library of pre-defined device classification *profiles*, each composed of properties and corresponding values that match a specific device type. The Device Profile Library is upgraded periodically to improve the accuracy and breadth of classification. Install the latest version of the Device Profile Library to take advantage of the most current classifications.
- CounterACT Core Extensions Module version 1.0, including the Device Classification Engine.
- An active Maintenance Contract for CounterACT devices.

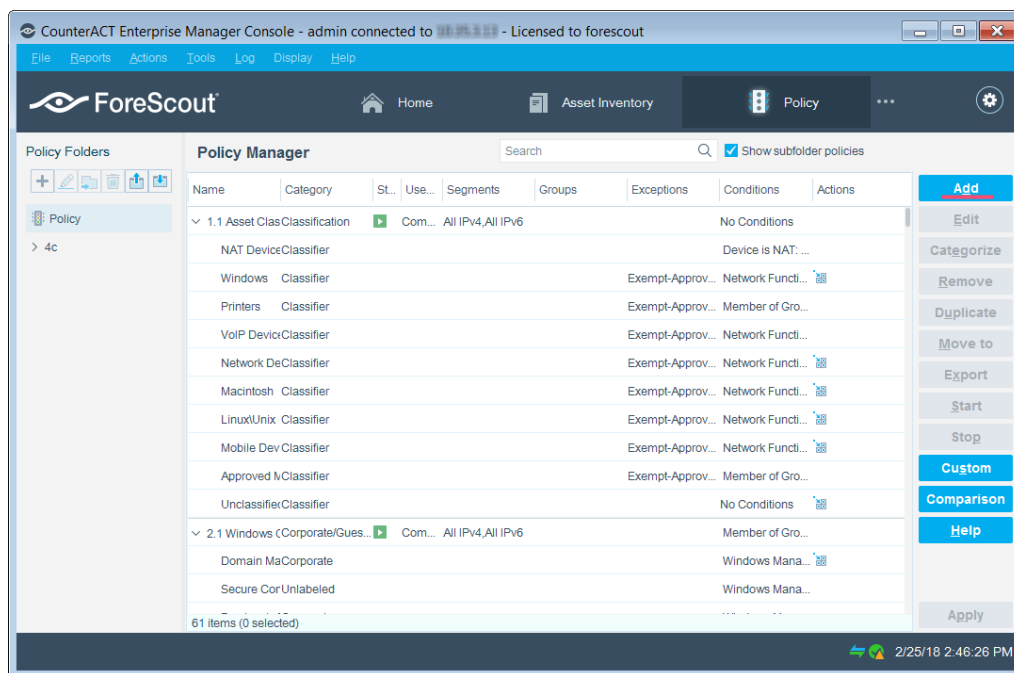


Create a Primary Classification Policy

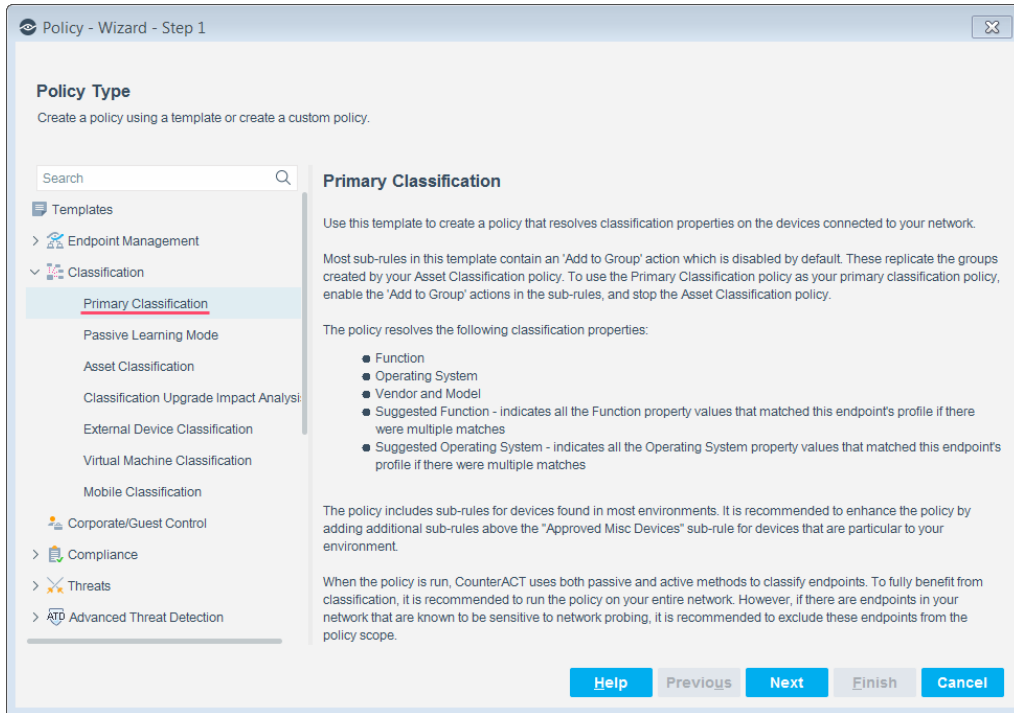
Follow these steps to detect and classify profiles of connected devices using a policy template.

1 Select the Primary Classification Template

1. Log into the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.



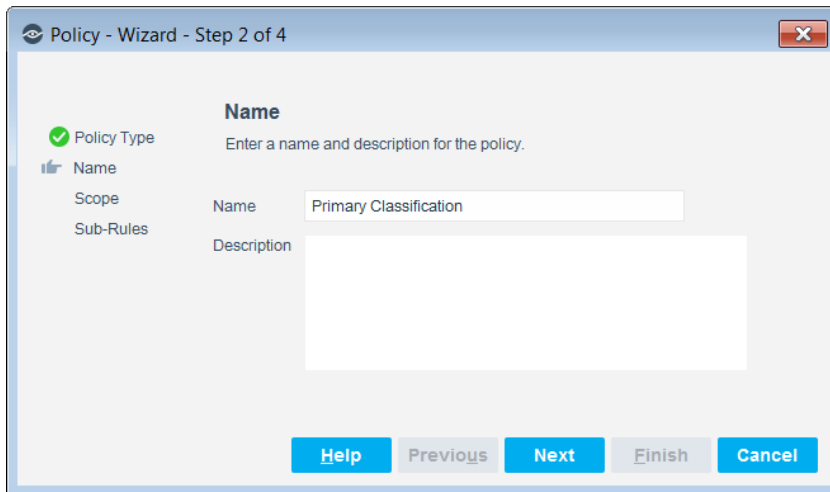
3. Select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Classification** folder and select **Primary Classification**.



5. Select **Next**. The Name pane opens.

2 Name the Policy

1. In the Name pane, a default policy name appears in the **Name** field.



2. Accept the default name or create a new unique name, and add a description.

3. Select **Next**. The Scope pane and the IP Address Range dialog box open.

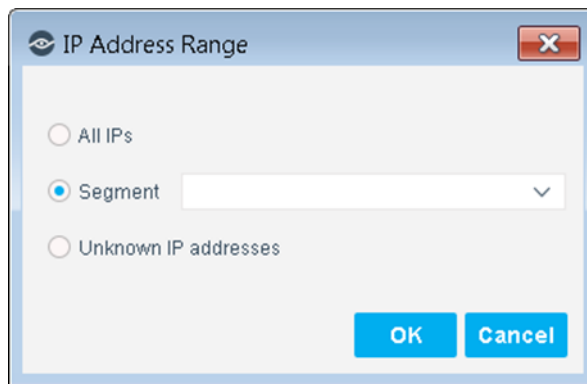


3 Choose the Endpoints to Inspect


To fully benefit from classification, it is recommended to run a classification policy on your entire network.

*If there are endpoints in your network that are known to be sensitive to network probing, it is recommended to the **Properties - Passive Learning** group.*

1. Use The IP Address Range dialog box to define which endpoints are inspected.

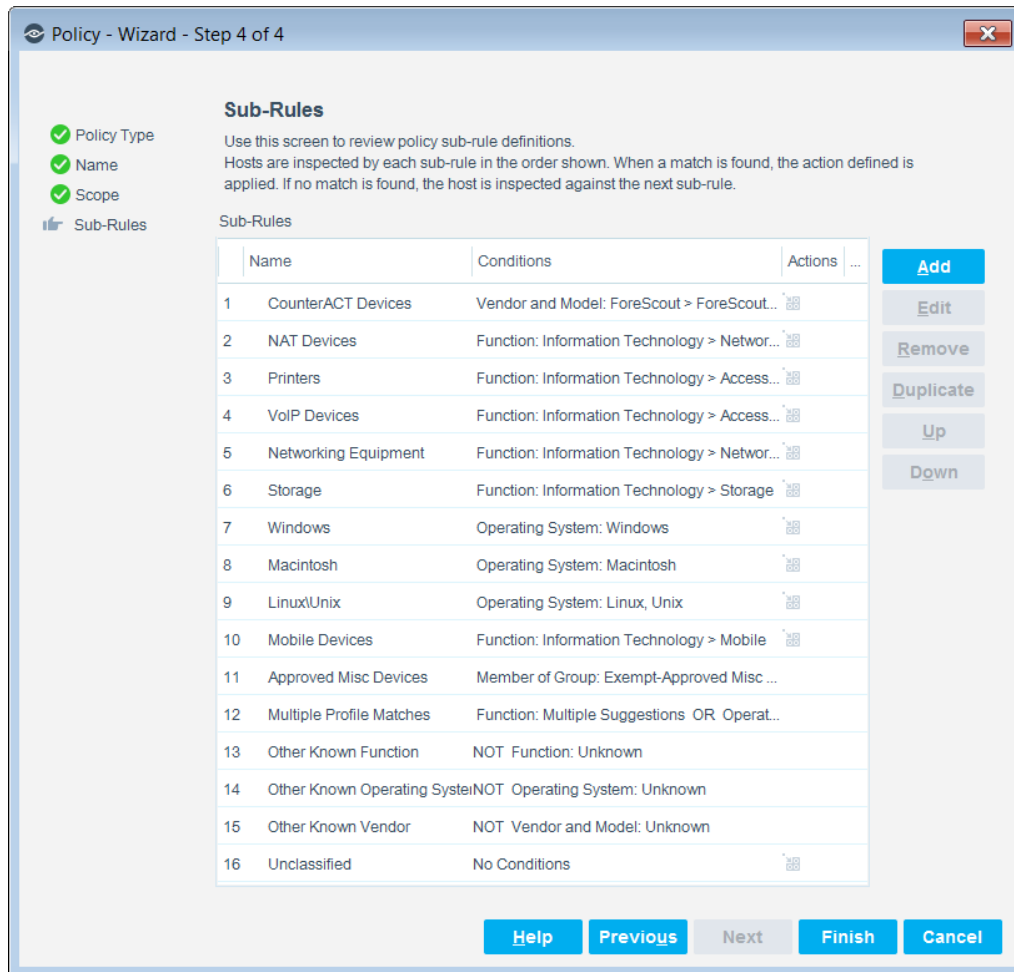


The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
2. Select **OK**. The added range appears in the Scope list.
 3. To filter the specified ranges or add exceptions, select  (**Advanced**).
 4. Select **Next**. The Sub-Rules pane opens.


4 Finish Policy Creation

The policy sub-rules instruct CounterACT how to detect endpoints (Conditions) and handle endpoints (Actions). Sub-rules are performed in order until a match is found.



The sub-rule conditions of these policies detect endpoints of the specific device type. The actions are disabled by default. When the actions are enabled, they sort the detected endpoints into their respective device groups.

If a device does not meet the criteria for any group or if CounterACT cannot evaluate the endpoint, it is Unclassified.

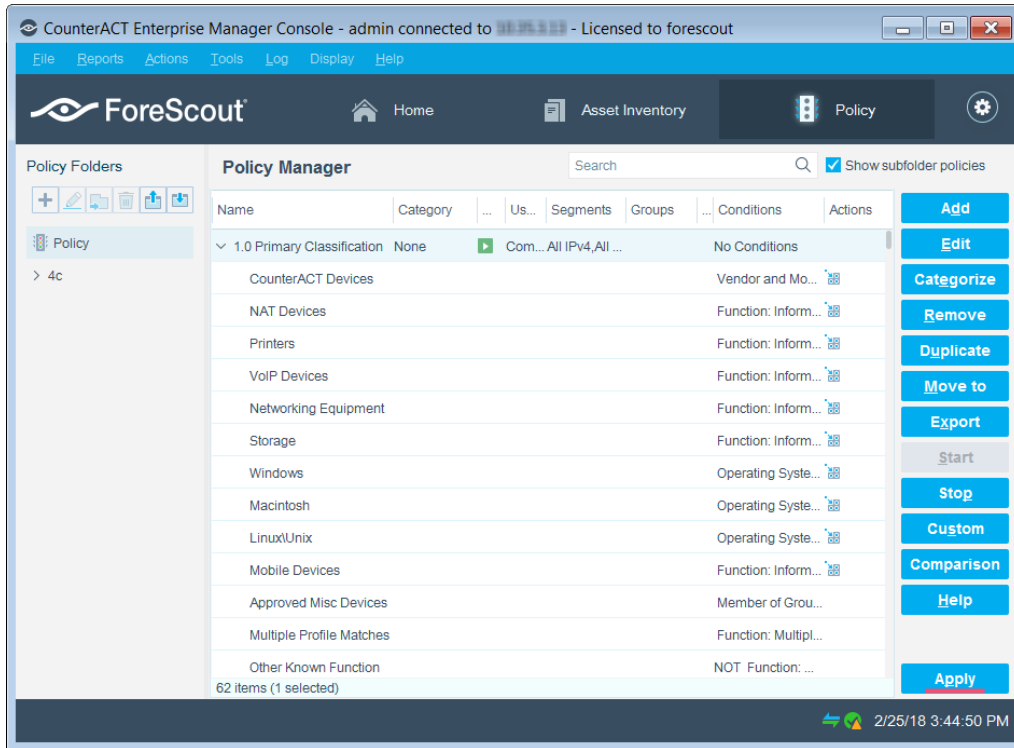
 *The Primary Classification template includes a sub-rule that indicates if a member of the Exempt-Approved Misc Devices group does not meet the criteria for a classification category. It is recommended to add to this group all the endpoints that CounterACT does not classify, but that you know about and specifically do not want to fall into the Unclassified group.*

1. Select **Finish**. The policy automatically appears highlighted in the Policy Manager, where it can be activated.



5 Activate the Policy

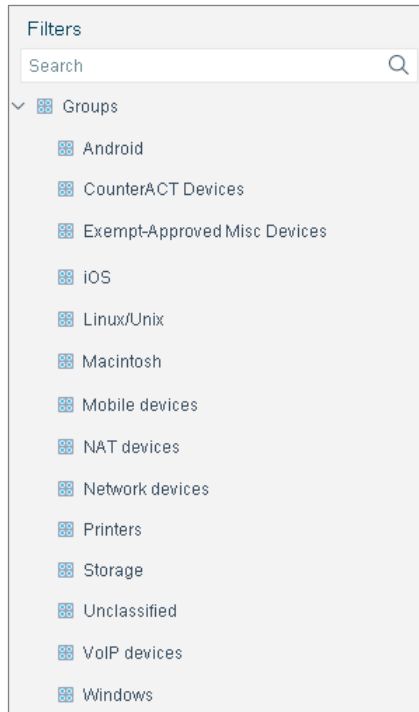
1. Select **Apply**. The policy is activated.



CounterACT detects the connected devices at the addresses you specified in the Scope pane and resolves their classification properties. It also adds them to their appropriate groups if the Add to Group actions are enabled.



2. To see the created groups, on the Console toolbar, select the Home tab, and in the Filters pane, expand the **Groups** folder and scroll to view the groups.



View Endpoints per Classification Metric

To view the connected endpoints per classification metric:

1. On the Console toolbar, select the Asset Inventory tab.
2. In the Views pane, expand the Classification node and select a metric.



CounterACT Enterprise Manager Console - admin connected to [redacted] - Licensed to ForeScout

File Reports Actions Tools Log Display Help

ForeScout Home Asset Inventory Policy

Views

Search

Classification

- Function
 - Information Technology
 - Accessory
 - Computer
 - Mobile
 - Networking

Filters

Search

All

- Segments (462)
- Organizational Units
- Default Groups

Mobile

Search

Function	No. of Hosts	Last Update	Full Classification Path	Last Host	Lists
Mobile	2	2/25/18 4:02:29 ...	Information Technology > Mobile	10.44.2.1...	
SmartPhone	2	2/25/18 3:28:23 ...	Information Technology > Mobile > SmartPhone	10.44.2.1...	

Hosts

Function: SmartPhone Search 2 OF 710 HOSTS

Host	IPv4 ...	Segm...	MAC A...	Com...	Displa...	Switch...	Sw...	Function	Actions	S...
galaxy-s8.pm...	10.44.2...	PM Net...	30074d...					SmartPhone		
10.44.2.105	10.44.2...	PM Net...	4c6641...					SmartPhone		

2/25/18 4:19:17 PM

View Classifications per Endpoint

After activating a classification policy, you can view an extensive range of details about connected endpoints.

To evaluate devices:

1. On the Console toolbar, select the Home tab.
2. In the Views pane, expand the **Policy** folder and select the policy containing your device classification policy.
3. In the Detections pane, select a host. Host information is displayed in the Details pane.



- To customize the information displayed about hosts and users connected to assets, right-click a column heading, select **Add/Remove Columns**, and select the information of interest to you. You can also reorder the columns.

Replace an Asset Classification Policy

If you find that the *Primary Classification* policy provides more comprehensive classification in your environment than an existing *Asset Classification* policy, it is recommended to use it as your primary classification policy. To do this, enable the *Add to Group* actions in the *Primary Classification* policy to replicate the groups created by the *Asset Classification* policy, and use the Policy Manager to stop the *Asset Classification* policy.

Fine-Tune Device Classification

After policies are run, you can manually fine-tune the device classification when a *Function* or *Operating System* property value set by the Device Classification Engine is not the optimal classification for your compliance and control policies.

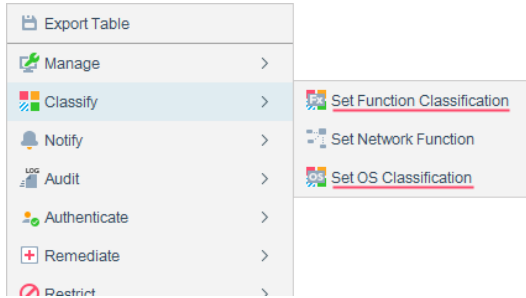
- [Improve Classification for Individual Endpoints](#)
- [Improve Classification Using a Policy](#)



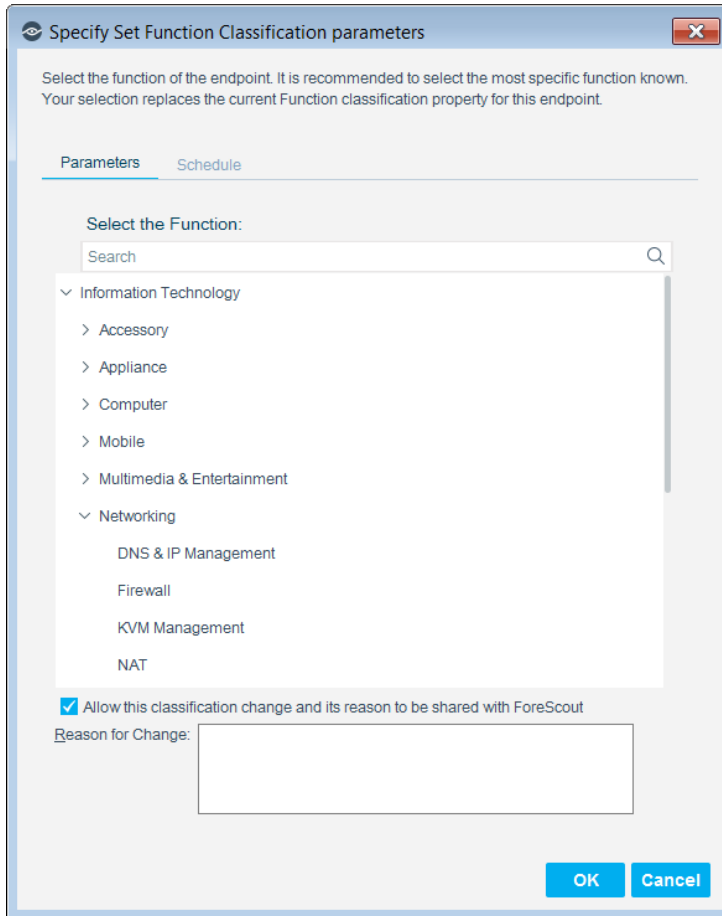
Improve Classification for Individual Endpoints

To re-classify devices:

1. In the Views pane of the Console Home tab, expand the Policies folder and select your device classification policy.
2. In the Detections pane, right-click one or more devices to be re-classified to a common value, and select **Classify > Set Function Classification** or **Set OS Classification**.




3. In the Parameters tab, select the most detailed correct function or operating system classification from the list.





4. If you agree to provide ForeScout with information regarding the change, select the checkbox, and enter:
 - the reason why the selected classification is appropriate for this endpoint
 - the ideal classification for this endpoint, if it is not in the classification list


The feedback that you enter in this field will be sent to ForeScout to help provide better classification services.

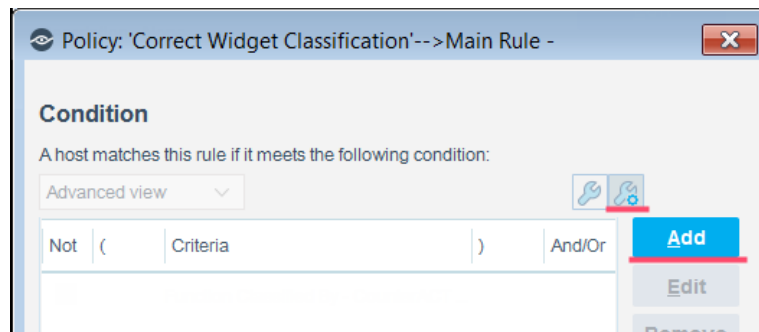
 *To ensure that your changes are shared with ForeScout, first go to Tools > Options > Advanced > Data Sharing, and select **Allow selected endpoint properties to be shared with ForeScout**. For more information about data sharing, refer to The ForeScout Research and Intelligent Analytics Program section in the CounterACT Administration Guide. See [Additional CounterACT Documentation](#) for information on how to access the guide.*

5. Select **OK**.

Improve Classification Using a Policy

To re-classify devices:

1. In the Console Policy tab, add a custom policy, and define the endpoint scope.
2. In the policy rule Condition area, select  (**Advanced**).



3. In Condition area, create the following condition and enclose it within parentheses:
 - a. The **Classification (Advanced) > Function Classified By** or **Classification (Advanced) > Operating System Classified By** property equals **CounterACT Device Classification Engine**.
 - b. The **Classification > Function** or **Classification > Operating System** property equals the specific classification that needs to be changed.
 - c. If necessary, other conditions that ensure that only the intended devices match the policy rule.
4. In Condition area, create another condition and enclose it within parentheses:
 - a. The **Classification (Advanced) > Function Classified By** or **Classification (Advanced) > Operating System Classified By** property equals **Policy or manual action**.



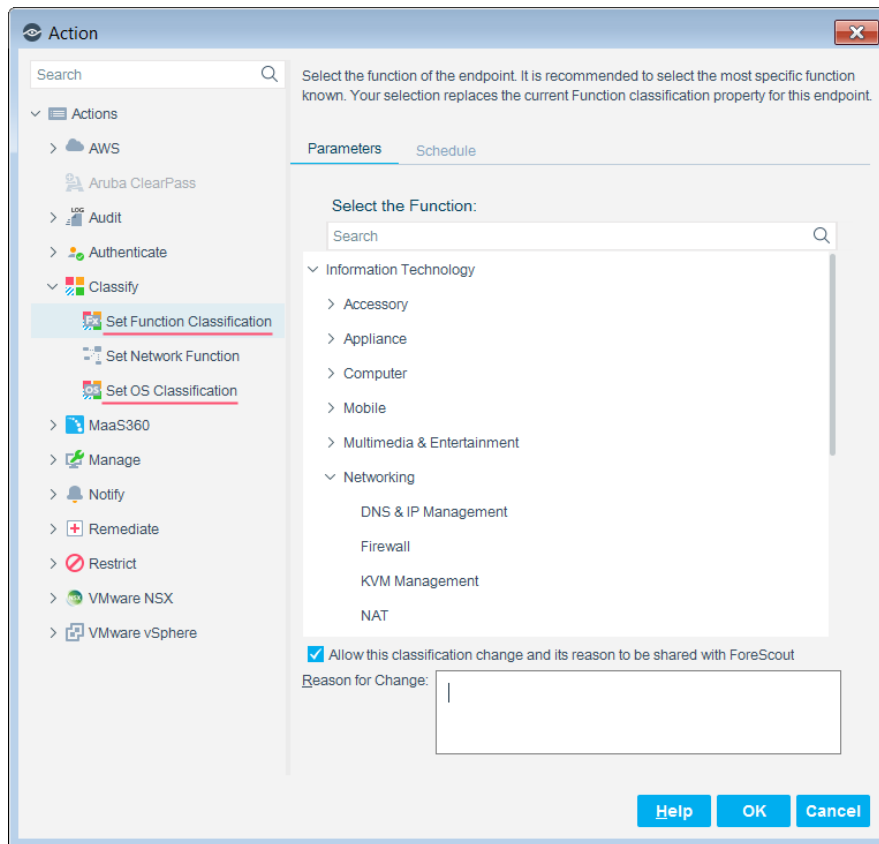
- b. The **Classification > Function** or **Classification > Operating System** property equals the correct classification for devices that match the first condition.

The second condition ensures that the policy does not undo classification changes already applied by this policy.

- 5. Between the two conditions, change **AND** to **OR**.




- 6. In the Actions area, add **Classify > Set Function Classification** or **Set OS Classification**.





7. In the Parameters tab, select the most detailed correct function or operating system classification for devices that match the first condition.
8. If you agree to provide ForeScout with information regarding the change, select the checkbox, and enter:
 - the reason why the selected classification is appropriate for this endpoint
 - the ideal classification for this endpoint, if it is not in the classification list

The feedback that you enter in this field will be sent to ForeScout to help provide better classification services.

 *To ensure that your changes are shared with ForeScout, first go to Tools > Options > Advanced > Data Sharing, and select **Allow selected endpoint properties to be shared with ForeScout**. For more information about data sharing, refer to The ForeScout Research and Intelligent Analytics Program section in the CounterACT Administration Guide. See [Additional CounterACT Documentation](#) for information on how to access the guide.*

9. Select **OK** and apply the policy.

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.

Options

Search

- VPN
- General
- Discovery
- NAC
- Licenses**
- Lists
- Map
- Internal Network

Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Search

Name ^	Status	Type
<u>ForeScout CounterACT See</u>	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

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



Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-15 14:07