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 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a
Delaware corporation. A list of our trademarks and patents can be found at
brands, products, or service names may be trademarks or service marks of their respective
owners.

2020-02-26 08:47
# Table of Contents

**About Device Classification** ........................................................................................................... 4  
Classification Enabled by Default ........................................................................................................ 4  
Upgrade from Earlier Versions ............................................................................................................. 4  
Groups Created by Primary Classification Policy ............................................................................. 5

**Prerequisites** ................................................................................................................................. 5

**Create a Primary Classification Policy** .......................................................................................... 5

**View Endpoints per Classification Type** ......................................................................................... 11

**View Classifications per Endpoint** ................................................................................................ 11

**Fine-Tune Device Classification** .................................................................................................. 12  
Improve Classification for Individual Endpoints ............................................................................. 12  
Improve Classification Using a Policy ............................................................................................... 14

**Additional Forescout Documentation** .......................................................................................... 17  
Documentation Downloads .............................................................................................................. 17  
Documentation Portal ....................................................................................................................... 18  
Forescout Help Tools ......................................................................................................................... 18
About Device Classification

The Forescout platform 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 create a policy that:

- Resolves several endpoint classification properties, including:
  - 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 Primary Classification policy template wizard to create a policy that fully leverages the Forescout 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.

After the policy runs, you can use Forescout platform 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 Forescout Administration Guide. See Additional Forescout Documentation for information on how to access this guide.

Classification Enabled by Default

Forescout eyeSight automatically discovers classification properties: Function, Operating System, and Vendor and Model, through Options > Discovery > Inventory, prior to the Primary Classification policy template being configured or run.

Data for classification properties is added to endpoints in the All Hosts pane and to the Classification folder of the Asset Inventory.

Upgrade from Earlier Versions

Upgraded versions of Forescout might include legacy Asset Classification policies that provide limited information about endpoints. To take advantage of more precise classification profiles, it is recommended to create and run Primary Classification policies.

The Primary Classification policy provides more comprehensive classification in your environment than legacy Asset Classification policies. To use it as your primary classification policy, ensure that the Add to Group actions are enabled in the Primary Classification policy, and use the Policy Manager to stop your Asset Classification policies.
Groups Created by Primary Classification Policy

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

- CounterACT Devices
- NAT Devices: Devices that may hide other devices
- Printers
- VoIP Devices
- Networking Equipment: Devices such as WLAN controllers, routers, switches, and wireless controllers
- Storage
- Windows
- Macintosh
- Linux/Unix
- Mobile Devices
- Approved Misc Devices
- Multiple Profile Matches
- Other Known Function
- Other Known Operating System
- Other Known Vendor
- Unclassified: If the Forescout platform does not know to which category an endpoint is associated, which may happen, for example, if network devices are new

Prerequisites

This solution requires the following:

- Forescout version 8.2
- Forescout Core Extensions Module version 1.2, including the Device Classification Engine

Create a Primary Classification Policy

Follow these steps to detect and classify profiles of connected devices using a policy template.
Select the Primary Classification Template

1. Log in to the Forescout Console.
2. In the Console toolbar, select Policy.
3. Select Add.
4. Under Templates, expand the Classification folder and select Primary Classification.
5. Select Next.
**Name the Policy**

In the Name pane, a default policy name is displayed.

6. Enter a name for the policy. Optionally, enter a description.
7. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.

**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.*

8. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:
Classify Devices How-to Guide

- **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 pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

9. Select **OK**. The added range is listed in the Scope pane.

10. To filter the specified ranges or add exceptions, select (Advanced).

11. Select **Next**.

**Finish Policy Creation**

The policy sub-rules instruct the Forescout platform 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 sort the detected endpoints into their respective device groups.

If a device does not meet the criteria for any group or if the Forescout platform 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 the Forescout platform does not classify, but that you know about and specifically do not want to fall into the Unclassified group.

12. Select Finish. The policy automatically is highlighted in the Policy Manager, where it can be activated.
Activate the Policy

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

The Forescout platform 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.

14. To see the created groups, in the Console toolbar, select **Home**, and in the Filters pane, expand the **Groups** folder and scroll to view the groups.
View Endpoints per Classification Type

To view the connected endpoints per classification type:

1. In the Console toolbar, select Asset Inventory.
2. In the Views pane, expand the Classification folder and select a classification type.

View Classifications per Endpoint

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

To evaluate devices:

1. In the Console toolbar, select Home.
2. In the Views pane, expand the Policies 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.
4. 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.

**Fine-Tune Device Classification**

To improve the classification of devices, you can use the procedures in this section or you can use the Reclassification policy template. Refer to the Policy Templates chapter in the Forescout Administration Guide for details on the Reclassification policy template.

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

- Improve Classification for Individual Endpoints
- Improve Classification Using a Policy

**Improve Classification for Individual Endpoints**

To reclassify devices:

1. In the Views pane of the Console Home, 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, Set OS Classification, or Set Vendor and Model 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 option to **Allow this classification change and its reason to be shared with Forescout**, 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 Options > Advanced > Data Sharing and select Share selected endpoint properties and plugin configuration and usage information with ForeScout. For more information about data sharing, refer to The Forescout Research and Intelligent Analytics Program section in the Forescout Administration Guide. See Additional Forescout Documentation for information on how to access this guide.

5. Select OK.

**Improve Classification Using a Policy**

To reclassify devices:

1. In the Console, select Policy, 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, Set OS Classification, or Set Vendor and Model 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 option to **Allow this classification change and its reason to be shared with Forescout**, 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 **Options > Advanced > Data Sharing** and select **Share selected endpoint properties and plugin configuration and usage information with Forescout**. For more information about data sharing, refer to The Forescout Research and Intelligent Analytics Program section in the Forescout Administration Guide. See Additional Forescout Documentation for information on how to access this guide.

9. Select **OK** and apply the policy.
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 Technical Documentation 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 Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:
- From the Console, select Help > About Forescout.

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:
- Go to https://www.Forescout.com/company/technical-documentation/

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 Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.
To access documentation on the Customer Support 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 quickly access information about the tasks and topics you are working with.

Forescout Administration Guide
- Select Administration Guide from the Help menu.

Plugin Help Files
- After the plugin is installed, select Tools > Options > Modules, select the plugin and then select Help.

Documentation Portal
- Select Documentation Portal from the Help menu to access the Documentation Portal.