



# Forescout

## Core Extensions Module: Device Classification Engine

### Configuration Guide

**Version 1.4.1**



## 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](mailto: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 <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.

2020-06-17 11:12

# Table of Contents

<b>About the Device Classification Engine.....</b>	<b>4</b>
Classification Enabled by Default .....	4
Inventory All Detected Endpoints .....	4
Endpoint Classification Details.....	6
Optimal Classification Policies .....	7
<b>How It Works .....</b>	<b>7</b>
<b>What to Do .....</b>	<b>8</b>
<b>Device Classification Engine Requirements .....</b>	<b>8</b>
<b>Configuration .....</b>	<b>9</b>
Ensure That the Device Classification Engine Plugin Is Running .....	9
<b>Primary Classification Policy Template.....</b>	<b>9</b>
<b>Custom Policies .....</b>	<b>11</b>
Use Case Examples .....	11
<b>Handle Sensitive Endpoints .....</b>	<b>12</b>
<b>Policy Properties .....</b>	<b>12</b>
Classification Properties .....	13
Function .....	14
Operating System .....	14
Vendor and Model .....	15
Classification (Advanced) Properties .....	15
<b>Classify Actions .....</b>	<b>16</b>
Cancel Classify Actions.....	17
<b>Classification Property Fine Tuning .....</b>	<b>18</b>
<b>Update Classification Profiles.....</b>	<b>20</b>
Manual Changes.....	21
Enable Pending Profile Changes to Be Reviewed .....	21
Review Pending Profile Changes .....	22
<b>Share Data with Forescout .....</b>	<b>24</b>
<b>Core Extensions Module Information .....</b>	<b>24</b>
<b>Additional Forescout Documentation.....</b>	<b>25</b>
Documentation Downloads .....	25
Documentation Portal .....	26
Forescout Help Tools.....	26

## About the Device Classification Engine

The Device Classification Engine is a component of the Forescout Core Extensions Module. See [Core Extensions Module Information](#) for details about the module.

The Device Classification Engine is a core feature of the Forescout platform. It resolves classification-related properties for comprehensive classification of each endpoint.

The key benefits of the Device Classification Engine are:

- Out-of-the-box precise classification of traditional IT devices as well as IoT, OT, mobile, and virtual endpoints connected to your network.
- Comprehensive view of all endpoints in the inventory across three classification types. See [Inventory All Detected Endpoints](#).
- High-level, granular classification of function, operating system, and vendor. See [Endpoint Classification Details](#).
- Broad and extensible Primary Classification policy template for device classification. See [Optimal Classification Policies](#).
- Content updates that allow rapid accommodation of new endpoint categories and finer granularity in classification.
- Display of pending classification changes for evaluating the impact of Device Profile Library upgrades.
- Flexible classification paradigm that lets you ensure complete classification coverage within your environment.

## 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.

## Inventory All Detected Endpoints

The Device Classification Engine classifies traditional IT as well as IoT devices connected to your network. After a Forescout platform policy is run that resolves any of the *Function*, *Operating System*, or *Vendor and Model* classification properties, you can see all the connected endpoints per classification type in the Asset Inventory view.

The following graphic shows the Asset Inventory for the Function classification type:

The screenshot displays the ForeScout Console Enterprise Manager interface. The 'Asset Inventory' tab is selected, and the 'Function' classification type is chosen from the left-hand menu. The main table lists various device functions with their full classification paths, the number of hosts, and the last update time. Below the table, there are sections for 'Field' and 'Hosts'.

Function	Full Classification Path	No. of Hosts	Last Update	Last Host	Links
Mobile	Information Technology > Mobile	4	8/20/19 8:52:30 AM		
Network Access Control	Information Technology > Networking > Network Access Control	4	8/20/19 11:05:35 AM		
Networking	Information Technology > Networking	11	8/20/19 10:47:44 AM		
Out Of Band Controller	Information Technology > Accessory > Out Of Band Controller	1	8/20/19 5:44:50 AM		
Printer	Information Technology > Accessory > Printer	17	8/20/19 11:22:51 AM		
Router or Switch	Information Technology > Networking > Router or Switch	3	8/20/19 8:55:39 AM		
Server	Information Technology > Computer > Server	29	8/20/19 11:18:47 AM		
Smartphone	Information Technology > Mobile > Smartphone	1	8/20/19 11:25:44 AM		
Tablet	Information Technology > Mobile > Tablet	1	8/20/19 3:52:25 AM		

Field: Function

Hosts: 0 OF 2,026 HOSTS

Host: [Search] [0%]

Host \* IPv4 Address Segment Comment MAC Address Display Name Switch-IPFQDN and... Switch Port Alias Switch Port Name Function Actions

The following graphic shows the Asset Inventory for the Operating System classification type:

The screenshot displays the ForeScout Console Enterprise Manager interface. The 'Asset Inventory' tab is selected, and the 'Operating System' classification type is chosen from the left-hand menu. The main table lists various operating systems with their full classification paths, the number of hosts, and the last update time. Below the table, there are sections for 'Field' and 'Hosts'.

Operating System	Full Classification Path	No. of Hosts	Last Update	Last Host	Links
CentOS	Linux > CentOS	1	8/20/19 10:10:19 AM		
Cisco IOS	Cisco > Cisco IOS	1	8/20/19 4:26:12 AM		
Cisco IOS-XE 03.03	Cisco > Cisco IOS-XE > Cisco IOS-XE 03.03	1	8/20/19 8:55:39 AM		
Contiki OS	Contiki OS	1	8/20/19 8:19:49 AM		
Debian	Linux > Debian	30	8/20/19 11:35:35 AM		
Fedora	Linux > Fedora	2	8/20/19 9:18:53 AM		
FreeBSD	Unix > FreeBSD	9	8/20/19 10:31:48 AM		
Linux	Linux	332	8/20/19 11:35:14 AM		

Field: Operating System

Hosts: 0 OF 2,025 HOSTS

Operating System: [Search]

Host \* IPv4 Address Segment Comment MAC Address Display Name Switch-IPFQDN and... Switch Port Alias Switch Port Name Function Actions

The following graphic shows the Asset Inventory for the Vendor and Model classification type:

The screenshot shows the ForeScout Console Enterprise Manager interface. The 'Asset Inventory' tab is selected, and the 'Vendor and Model' classification type is chosen. The table displays the following data:

Vendor and Model	Full Classification Path	No. of Hosts	Last Update	Last Host	Link
3Com	3Com	633	8/20/19 11:39:09 AM		
Action Star	Action Star	1	8/20/19 8:00:25 AM		
Apple iPad	Apple > Apple Device > Apple iPad	1	8/20/19 3:52:25 AM		
Apple iPhone	Apple > Apple Device > Apple iPhone	1	8/20/19 11:25:44 AM		
Cisco	Cisco	5	8/20/19 11:04:18 AM		
Cisco Router or Switch	Cisco > Cisco Router or Switch	2	8/20/19 5:14:34 AM		
Cisco Switch 3000 Series	Cisco > Cisco Router or Switch > Cisco Switch 3000 Series	1	8/20/19 6:56:39 AM		
Dell	Dell	14	8/20/19 10:45:58 AM		
ForeScout Appliance	ForeScout > ForeScout Platform > ForeScout Appliance	3	8/20/19 11:05:36 AM		

Below the table, there is a 'Hosts' section showing 0 OF 2,025 HOSTS.

## Endpoint Classification Details

You can see all the device classification details for each endpoint in the **Home** tab. The icon displayed for each endpoint combines its function classification and its operating system classification, if known.

The screenshot shows the 'All Hosts' tab in the ForeScout Console Enterprise Manager. A list of hosts is displayed, and one host is selected, showing its details in the 'Profile' section. The details include:

- IPV4 Address:** [Redacted]
- Operating System:** iOS
- MAC Address:** [Redacted]
- Function:** Network > Mobile > Tablet
- Vendor and Model:** Apple > Apple Device > Apple iPad

The 'Profile' section also lists various system properties and their values, such as DHCP Domain Name, DHCP Hostname, DHCP Options, DNS Name, MAC Address, NIC Vendor, Open Ports, OS Class, OS Fingerprint, Windows SecureConnector Deployment Type, Windows SecureConnector Display, Windows SecureConnector Version, Windows ManageGate SecureConnector, Network Function, Function, Operating System, Vendor and Model, Vendor Classified By, and Operating System Classified By.


*If the endpoint function has not been classified, then the Network Function property determines the icon.*

## Optimal Classification Policies

The Device Classification Engine provides a Primary Classification policy template to create a policy that:

- Resolves the *Function*, *Operating System*, and *Vendor and Model* classification properties on all the devices connected to your network
- 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 template to create a policy that fully leverages the Device Classification Engine technology, and then enhance the policy to meet your needs. For example, if in your environment, you have many IP-connected security cameras from a particular vendor, you may want to create an additional sub-rule to group those devices.

 *Environments upgraded from earlier CounterACT versions might be running a less comprehensive Asset Classification policy. It is recommended to create a Primary Classification policy in its place and then use the Policy Manager to stop the Asset Classification policy.*

For more information about the Primary Classification policy, refer to the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

## How It Works

The Device Profile Library contains classification profiles that are composed of various properties and corresponding values. To classify an endpoint, the Device Classification Engine compares the properties of the endpoint with the profiles in the library to find the best match. The endpoint is then classified accordingly.

For example, the profile defined for *Apple iPad* considers a set of properties that includes the hostname of the device revealed by DHCP traffic, the HTTP banner, the NIC vendor, and Nmap scan results. The Device Classification Engine classifies any endpoint with property values matching those specified in the *Apple iPad* classification profile as:


- *Function*: Information Technology/Mobile/Tablet
- *Operating System*: iOS
- *Vendor and Model*: Apple/Apple iDevice/Apple iPad

As a general rule, the more properties the Forescout platform detects for an endpoint, the greater the potential for an accurate and granular classification. To increase the number of detected properties, the Forescout platform integrates with third-party components and network devices, such as switches, wireless controllers, and hypervisors, enabling the endpoint to match the most appropriate classification profile.

# What to Do

## To work with the Device Classification Engine:

1. Verify that you have met system requirements. See [Device Classification Engine Requirements](#).
2. Resolve the classification properties on your endpoints in either of these ways:
  - Create and run a policy based on the Primary Classification policy template
  - Use the classification properties in other policies
3. Review and fine-tune the classification results. See [Classification Property Fine Tuning](#).
4. Install the Device Profile Library whenever a new version is available. Refer to the *Forescout Device Profile Library Configuration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.
5. Install the Core Extensions Module whenever a new version is available.

 *To help the Forescout platform provide better classification and posture assessment services, opt in to the Forescout Research and Intelligent Analytics Program. This voluntary program uploads anonymous host information from your environment to be used by Forescout researchers to improve the product. Refer to The Forescout Research and Intelligent Analytics Program section in the Forescout Administration Guide for more information about this program. See [Additional Forescout Documentation](#) for information on how to access this guide.*

## Device Classification Engine Requirements

The following Forescout platform and component version must be running in your Enterprise Manager and your appliances:

- Forescout interim release 8.2.1
- Core Extensions Module 1.2.1 with the Device Classification Engine Plugin
- 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.



# Configuration

The Device Classification Engine does not require any configuration. For endpoints to be classified, the [Classification Properties](#) must be used in a policy, such as a policy created by a *Primary Classification* policy template.

See [Primary Classification Policy Template](#) and [Custom Policies](#).




## Ensure That the Device Classification Engine Plugin Is Running

After installing the Device Classification Engine Plugin (and configuring it, if necessary), ensure that it is running.

### To verify:

1. Select **Tools > Options > Modules**.
2. In the *Modules* pane, hover over the Device Classification Engine Plugin name to view a tooltip indicating if it is running on Forescout devices in your deployment.

The name is preceded by one of the following icons:

-  - The Device Classification Engine Plugin is stopped on all Forescout devices.
  -  - The Device Classification Engine Plugin is stopped on some Forescout devices.
  -  - The Device Classification Engine Plugin is running on all Forescout devices.
3. If the Device Classification Engine Plugin is not running, select **Start**, and then select the relevant Forescout devices.
  4. Select **OK**.

## Primary Classification Policy Template

The Classification Engine provides a Primary Classification policy template that can be used to:


- Resolve classification properties on all connected endpoints.
- Group endpoints matching each sub-rule to display a granular summary of the different device types detected in your network. Most sub-rules in the template contain an *Add to Group* action that is enabled by default.

Run the policy to resolve the following properties:

- [Classification Properties](#):
  - [Function](#)
  - [Operating System](#)

- [Vendor and Model](#)
- [Classification \(Advanced\) Properties](#):
  - Function Classified By
  - Operating System Classified By
  - Function Classification Update
  - Operating System Classification Update
  - Vendor and Model Classification Update
  - Suggested Function
  - Suggested Operating System
  - Suggested Vendor and Model

It is recommended to enhance the policy by adding sub-rules for non-traditional devices found in your environment above the *Approved Misc Devices* sub-rule. For example, if you have many IP-enabled cameras in your network and you want to group them, add a sub-rule for these devices.

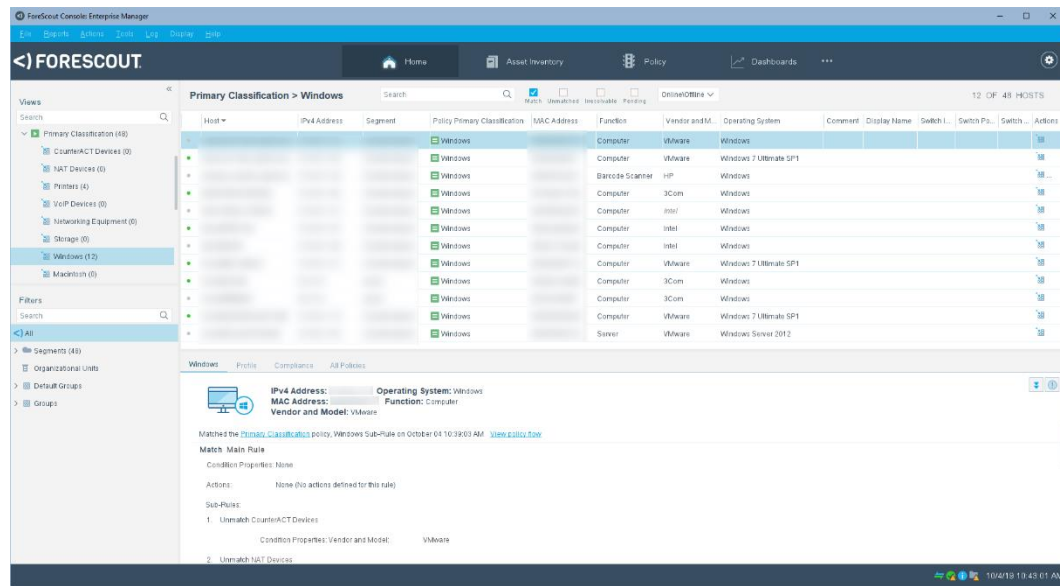
 *If some endpoints in your network are known to be sensitive to network probing, see [Handle Sensitive Endpoints](#).*

For more information about the Primary Classification policy template, refer to the *Policy Management* and *Policy Templates* chapters of the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

After the policy is run, you can see the endpoints that the policy detected.


**To see an overview of your policy:**

- 1.** Select **Home**.
- 2.** In the Views pane, expand the Policies folder.
- 3.** Expand the folder of the Primary Classification policy that you created. Each policy sub-rule name is displayed, followed by the number of endpoints that matched it.
- 4.** Select a sub-rule. The endpoints that matched the rule are displayed.



## Custom Policies

Forescout platform policy tools provide an extensive range of options for detecting and handling endpoints. You can use a policy to instruct the Forescout platform to apply actions to endpoints that match conditions based on classification-related properties.

 *If some endpoints in your network are known to be sensitive to network probing, see [Handle Sensitive Endpoints](#).*


It is helpful to create a set of policies that classify your endpoints into additional groups so that you can reference these groups later. This enables you to work with groups of endpoints based on different classification properties. For example, in some of your compliance and control policies, you may want to apply one action on all Samsung devices running Linux, and apply a different action on all tablets running Android. Grouping the devices in your classification policies makes this easy. Or, you can use the classification properties as conditions in custom policies.

## Use Case Examples

- Due to an MRI manufacturer's requirement to run an old version of Windows on a particular type of medical equipment, you want to enforce strict network controls on those devices. Create a policy that detects MRI machines running Windows XP and ensures that only the necessary ports are open, the devices are in a secure VLAN, and any suspicious activity results in immediate quarantine.
- You discover that an embedded Linux vulnerability is affecting several IP cameras from certain manufacturers. Use a simple condition to find IP cameras from those manufacturers, confirm the vulnerability, and quarantine if necessary.

## Handle Sensitive Endpoints

The Forescout platform uses both passive and active methods to classify endpoints. Active methods include probing the endpoint to check for a small range of open ports, running Nmap against the endpoint, and attempting to connect using WMI, SMB and/or RRP (depending on your HPS Inspection Engine configuration).

 *Forescout eyesight uses Nmap OS scans for classification. Sometimes Nmap selects random ports, specifically ports in the high range.*

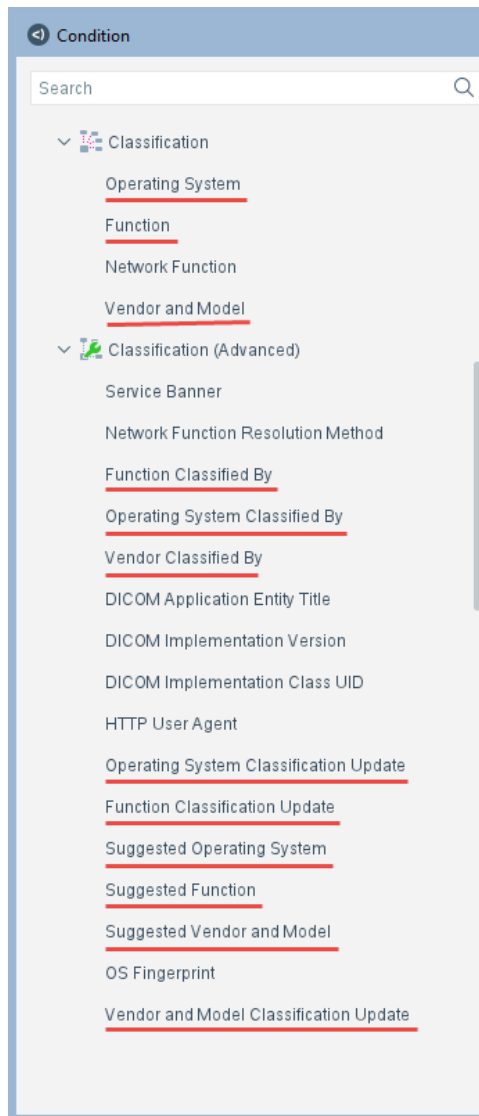
To fully benefit from classification, it is recommended to run a classification policy on your entire network. However, if there are endpoints in your network that are known to be sensitive to network probing, it is recommended to exclude these endpoints from the policy scope.

Alternatively, you can run a Passive Learning Mode policy to add the sensitive endpoints to the **Default Groups > Properties - Passive Learning** group. For more information, refer to the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

## Policy Properties

### To access classification-related properties:

1. Go to the Properties tree from the Policy Conditions dialog box.
2. Device classification properties are available in the following Properties folders:
  - [Classification Properties](#)
  - [Classification \(Advanced\) Properties](#)



## Classification Properties

The Device Classification Engine resolves three properties in the Classification condition folder:

- [Function](#)
- [Operating System](#)
- [Vendor and Model](#)

## Unmatched Endpoints

For each of the three properties, if the Classification Engine cannot definitively match the endpoint to a specific classification profile in the Device Profile Library, the property is resolved as follows:

- If multiple profiles match the endpoint, the property is resolved as the most specific value in the Device Profile Library that is common to all the matching profiles. For example, if *Windows Server 2008 Enterprise RTM* and *Windows Server 2008 Enterprise SP2* operating system profiles both match the endpoint, the Operating System property is resolved as *Windows Server 2008 Enterprise*.
  - 📄 *For a Function or Operating System classification, the other matching profile values are written to the Suggested Function or Suggested Operating System property.*
- If there is no common value among all the matching profiles, the property is resolved as *Multiple Suggestions*. This is indicative of highly conflicting information being received by the classification engine and should be investigated on a case-by-case basis, as it could indicate one device trying to impersonate another device type.
  - 📄 *For a Function or Operating System classification, all the matching profile values are written to the Suggested Function or Suggested Operating System property.*
- If no profiles in the Device Profile Library match the endpoint, the property is resolved as *Unknown*.

## Function

The *Function* property indicates the most detailed device function that can be resolved. For example:

- Information Technology/Accessory/Printer
- Operational Technology/Healthcare/Patient Monitor
- Operational Technology/Non-Industry Specific/Facilities/Physical Security/Surveillance/IP Camera

## Operating System

The *Operating System* property indicates the most detailed operating system information that can be resolved. For example:

- Windows/Windows Server 2012/Windows Server 2012 Essentials
- Macintosh/OS X 10.8 - MountainLion
- Chrome OS

## Vendor and Model

The *Vendor and Model* property indicates the vendor and the model, if known. For example:

- Samsung/Samsung Galaxy Tablet/Samsung Galaxy Tablet 10
- Cisco/Cisco Access Point/Cisco AP Aironet 3600

Some models are grouped by device type. For example:

- GE/GE Healthcare

## Classification (Advanced) Properties

The Device Classification Engine resolves several properties in the Classification (Advanced) condition folder.

Property	Description
<b>Function Classified By</b>	Indicates if the <i>Function</i> classification property was determined by the Device Classification Engine or set by an action.
<b>Operating System Classified By</b>	Indicates if the <i>Operating System</i> classification property was determined by the Device Classification Engine or set by an action.
<b>Vendor Classified By</b>	Indicates if the <i>Vendor and Model</i> classification property was determined by the Device Classification Engine or set by an action.
<b>Function Classification Update</b>	Indicates if a <i>Function</i> classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the <b>Options &gt; Classification &gt; Pending Updates</b> pane.
<b>Operating System Classification Update</b>	Indicates if an <i>Operating System</i> classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the <b>Options &gt; Classification &gt; Pending Updates</b> pane.
<b>Vendor and Model Classification Update</b>	Indicates if a <i>Vendor and Model</i> classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the <b>Options &gt; Classification &gt; Pending Updates</b> pane.
<b>Suggested Function</b>	If there are multiple candidates for the endpoint's <i>Function</i> classification, this property indicates all profiles in the Forescout Device Profile Library that match this endpoint. These values are considered less accurate than the resolved <i>Function</i> property value, possibly due to conflicting choices. If the <i>Function</i> property has been changed by a policy or manual action, this property indicates the endpoint's <i>Function</i> classification set by the Device Classification Engine. See <a href="#">Classify Actions</a> .

Property	Description
<b>Suggested Operating System</b>	If there are multiple candidates for the endpoint's <i>Operating System</i> classification, this property indicates all profiles in the Forescout Device Profile Library that match this endpoint. These values are considered less accurate than the resolved <i>Operating System</i> property value, possibly due to conflicting choices. If the <i>Operating System</i> property has been changed by a policy or manual action, this property indicates the endpoint's <i>Operating System</i> classification set by the Device Classification Engine. See <a href="#">Classify Actions</a> .
<b>Suggested Vendor and Model</b>	If there are multiple candidates for the endpoint's <i>Vendor and Model</i> classification, this property indicates all profiles in the Forescout Device Profile Library that match this endpoint. These values are considered less accurate than the resolved <i>Vendor and Model</i> property value, possibly due to conflicting choices. If the <i>Vendor and Model</i> property has been changed by a policy or manual action, this property indicates the endpoint's <i>Vendor and Model</i> classification set by the Device Classification Engine. See <a href="#">Classify Actions</a> .

## Classify Actions

If 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, you can override the value.

This is useful when:

- The classification resolved is not correct or the Forescout platform is unable to classify an endpoint.
- You are able to refine the classification resolved by the Forescout platform. For example, the device was classified as Healthcare, but it is actually an X-Ray device.
- The endpoint is excluded from the range of endpoints to be classified due to its sensitivity to probing.

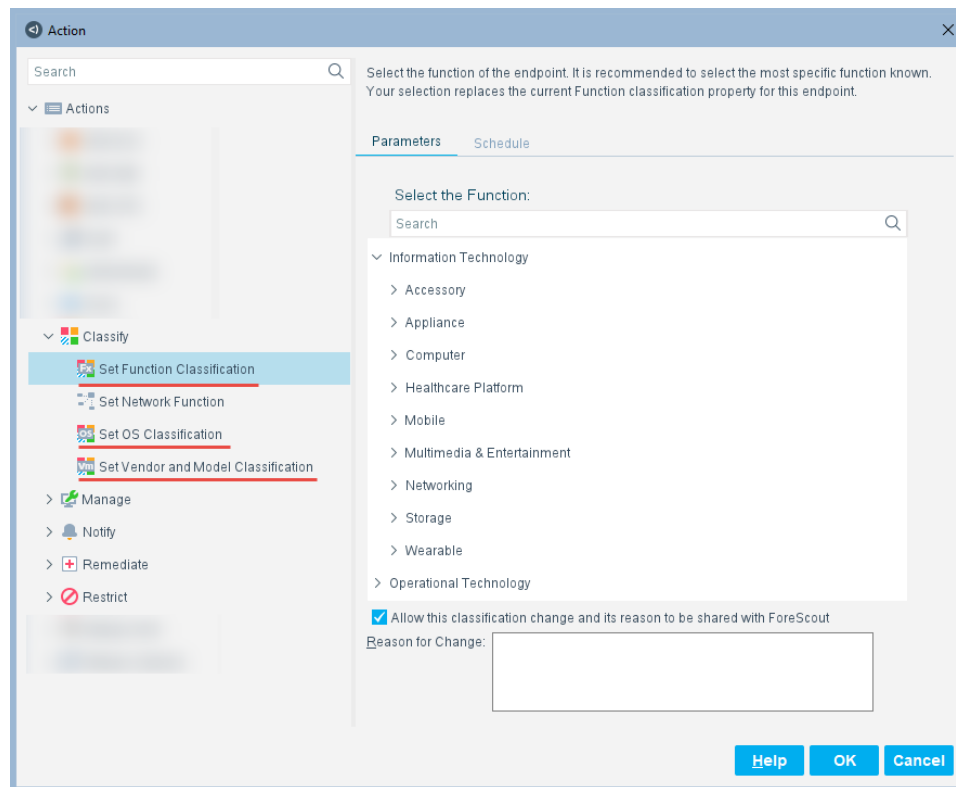
You can undo your manual classification assignment and revert to the classification set by the Device Classification Engine. See [Cancel Classify Actions](#) for details.

### To access device classification-related actions:

1. Do one of the following:
  - Go to the Actions tree from the Policy Actions dialog box
  - Right-click individual endpoints to classify them manually
2. Expand the Classify folder.
3. To override a classification property set by the Device Classification Engine, set one of the following actions:
  - Set Function Classification
  - Set OS Classification




## – Set Vendor and Model Classification



4. If you have opted in to data sharing, the classification change is uploaded to Forescout. If you agree to also provide Forescout with additional information regarding the change, select the option **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 you enter in this field is 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**. See [Share Data with Forescout](#).*

## Cancel Classify Actions

If you override an endpoint's classification property, you can undo your classification assignment and reset the property value to the one set by the Device Classification Engine.

**To cancel a device classification-related action after it was run:**

1. Select **Home**.

2. Right-click the endpoint.
3. Expand **Cancel Actions** and select one of the following actions:
  - Revert to Suggested Function Classification
  - Revert to Suggested Operating System Classification
  - Revert to Suggested Vendor and Model Classification



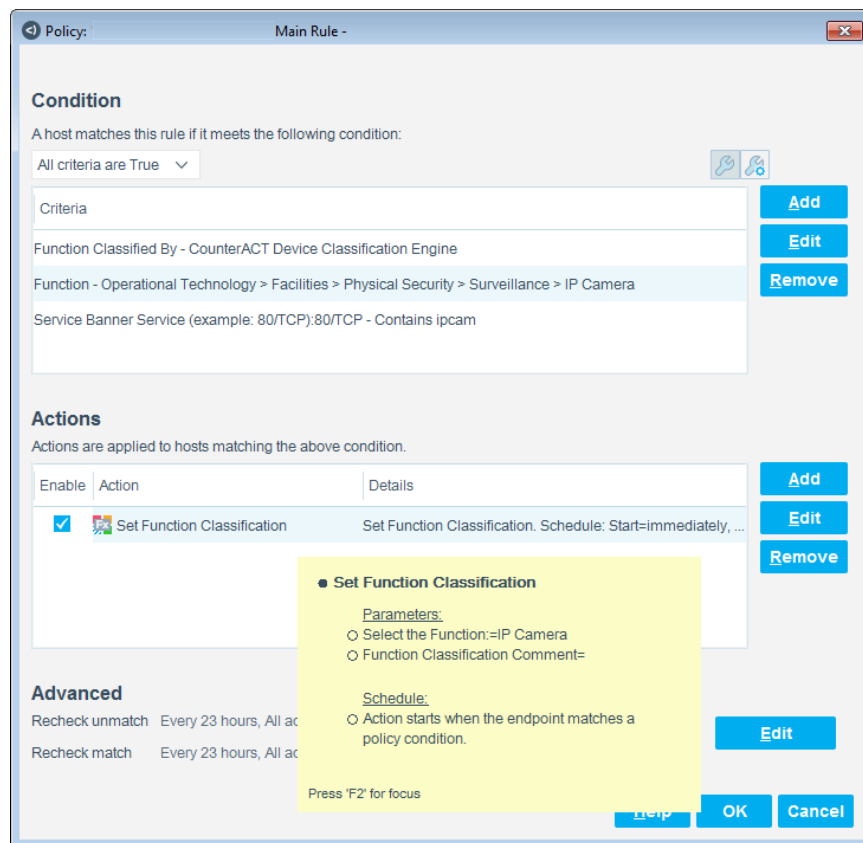
## Classification Property Fine Tuning

The Forescout platform classifies your endpoints with a high degree of accuracy. Nonetheless, some endpoints might not be classified as precisely as possible. It is recommended to fine-tune your device classification results if you can improve them.

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. See [Additional Forescout Documentation](#) for information on how to access this guide.

For example:

1. Create a condition that includes the following criteria:
  - The device was classified by the Forescout platform.
  - It was classified as a specific Function.
  - One or more properties indicate that the device has a more specific, or different, Function.
2. When this condition is met, set the Function to a different value.

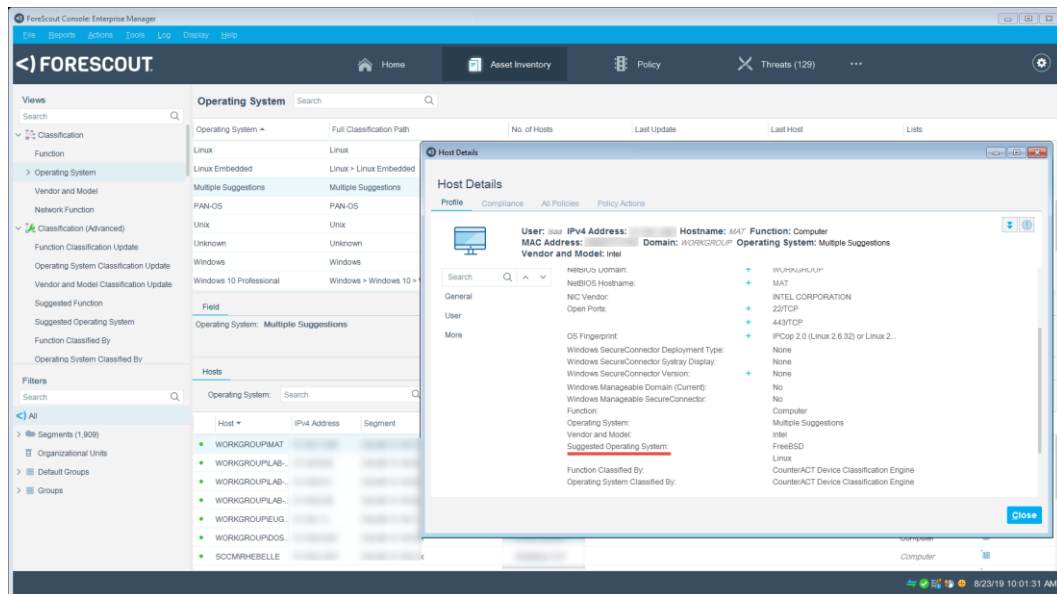


### To fine-tune the classification results:

1. Go to each of the *Function*, *Operating System*, and *Vendor and Model* results in the Classification folder of the **Asset Inventory**.
2. To improve the classification of endpoints classified as *Multiple Suggestions*, select the *Multiple Suggestions* entry. In the Hosts pane, all the endpoints that matched conflicting profiles are listed.

For each endpoint in the Hosts pane:

- a. Double-click the endpoint to open the Host Details.



- b. In the Profile tab, view the suggested classification matches.
  - c. Based on your familiarity with the endpoint, try to understand why inaccurate matches occurred. If possible, do one of the following:
    - Create a new policy with the correct [Classify Actions](#) for this endpoint and similar endpoints. The policy could include an additional property of the endpoints.
    - Use the [Classify Actions](#) to manually set the correct classification for this endpoint.
    - Change the sub-rules of your Primary Classification policy so that the correct match is made for this endpoint and similar endpoints.
3. To improve the classification of endpoints classified as *Unknown*, select the *Unknown* entry. All the endpoints that did not match any profile are listed in the Hosts pane.

If you know the classification of an endpoint, do one of the following:

- Create a new policy using the correct [Classify Actions](#) for this endpoint and similar endpoints.
- Use the [Classify Actions](#) to manually set the correct endpoint classification.
- Change the sub-rules of your Primary Classification policy so that the correct match is made for this endpoint and similar endpoints.

## Update Classification Profiles

Periodically, the Device Profile Library is upgraded to improve classification accuracy and to provide better coverage.

Due to classification profile changes in each library version, some device classifications may change when a new library version is applied to the endpoints.

Each time a new Device Profile Library version is installed, the following endpoint properties are resolved and used to indicate pending classification changes:

- Function Classification Update
- Operating System Classification Update
- Vendor and Model Classification Update

For more information about these properties, see [Classification \(Advanced\) Properties](#).

By default, you can review all the pending changes before they are applied. See [Review Pending Profile Changes](#). Then decide if you want to:

- Immediately apply the profile changes
- Modify existing policies and then apply the changes
- Cancel the changes and roll back to a previous Device Profile Library version

After a new Device Profile Library version is applied, it is recommended to run a policy that resolves classification properties.

## Manual Changes

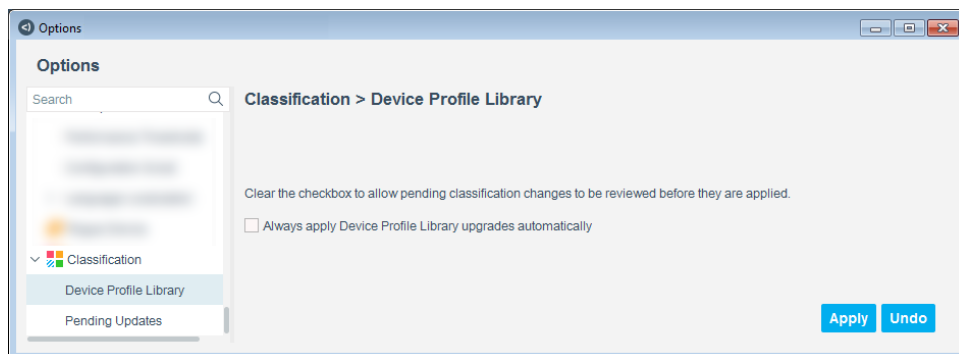
It is not recommended to perform Set Classification actions after a new Device Profile Library version is installed and before it is applied or rolled back. If these actions are performed:

- They are displayed together with the pending classification changes
- Their Set Classification action status is listed as **Success**
- They will not take effect until the new library version is applied or rolled back

## Enable Pending Profile Changes to Be Reviewed

**To ensure that you can review pending classification changes before they are applied:**

1. Go to **Options > Classification > Device Profile Library**.

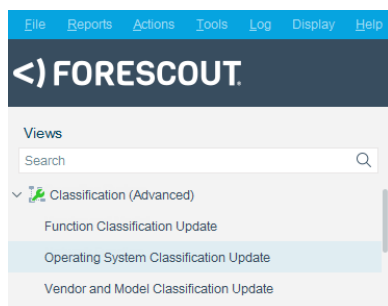


2. Clear the option **Always apply Device Profile Library upgrades automatically**.

## Review Pending Profile Changes

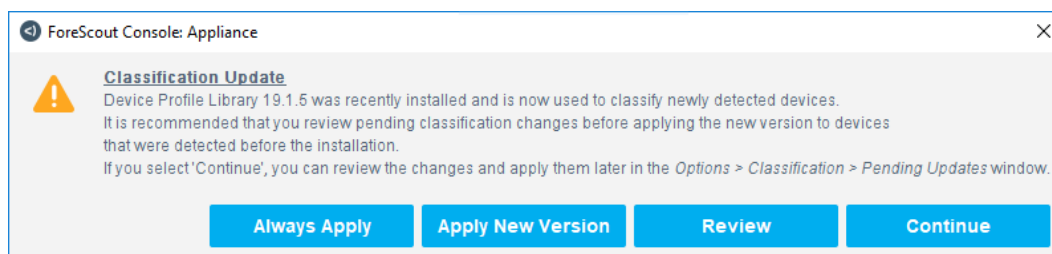
**To view pending change requests without applying them:**

1. Select **Asset Inventory**.
2. In the Views pane, expand Classification (Advanced), and select the appropriate classification property.

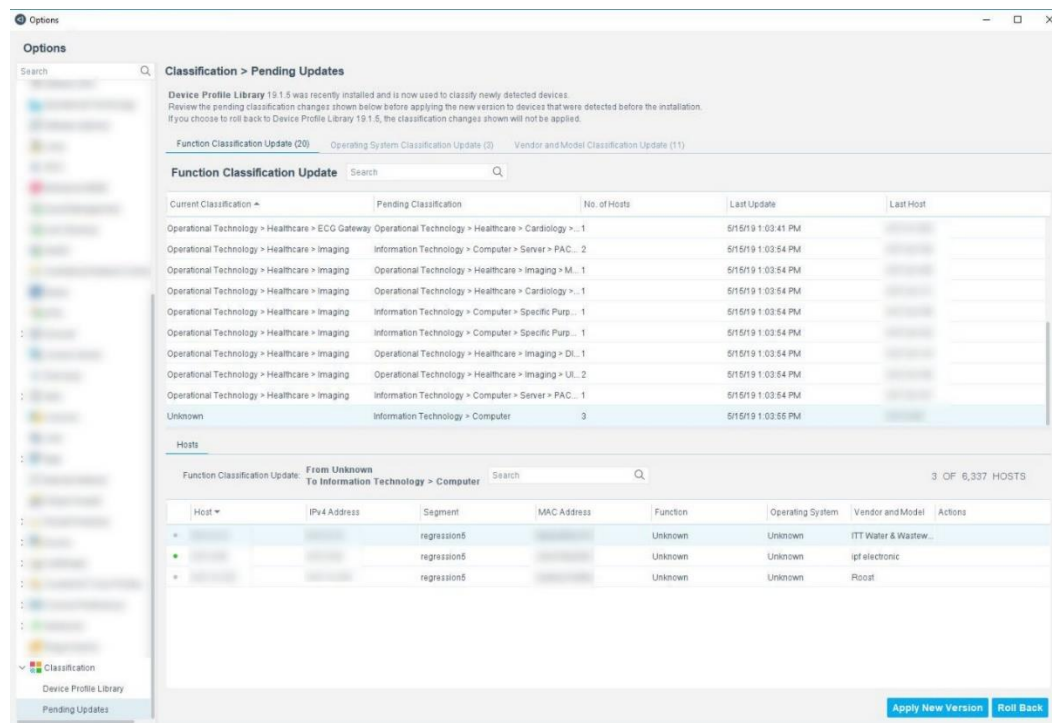


**To manage pending classification changes:**

1. Access the pending classification changes in one of the following ways:
  - Eight hours after the Device Profile Library is installed, a Classification Update message is displayed. To review the changes, select **Review**.



- After a Device Profile Library is installed, an icon is displayed on the task bar. Double-click the icon.
- *If you do not review the pending classification changes within a reasonable amount of time, the icon flashes.*
- At any time, go to **Options > Classification > Pending Updates**.



The pending classification changes are displayed in their respective tabs:

- Function Classification Update
  - Operating System Classification Update
  - Vendor and Model Classification Update
2. Review all the pending updates to verify that the new classifications are correct based on your knowledge of your environment, and that your existing control policies will continue to work as expected. Specifically pay attention to enforcement policies that rely on either old or new classification values.
  3. Do one of the following:
    - If the new classifications are satisfactory and your policies would all work correctly with the pending updates, select **Apply New Version**. All classification changes take effect.
    - If you need to modify policies before applying the changes, do so before selecting anything in this pane. Then return to this pane and select **Apply New Version**.
    - If only a few changes are not acceptable, you can write policies to fine-tune the classification and work around these changes. Then return to this pane and select **Apply New Version**.
    - If the changes are not acceptable, select **Roll Back**, and then select the Device Profile Library version to which to revert. All pending changes are discarded.

## Share Data with Forescout

To help Forescout provide better classification and posture assessment services, opt in to the Forescout Research and Intelligent Analytics Program. This voluntary program uploads anonymous information from your environment, such as policy-based or manual endpoint classification, to be used by Forescout researchers to improve the product. It also lets you share with Forescout additional information regarding your classification changes to aid Forescout in capturing your requirements in future content updates.

### To opt in to the program:

- Go to **Options > Advanced > Data Sharing** and select **Share selected endpoint properties and plugin configuration and usage information with Forescout**.

For more information about this program, 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.

## Core Extensions Module Information

The Device Classification Engine 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	Device Data Publisher	IoT Posture Assessment Engine
CEF Plugin	DNS Client Plugin	
Cloud Uploader	DNS Enforce Plugin	NBT Scanner Plugin
DHCP Classifier Plugin	DNS Query Extension Plugin	Packet Engine
Dashboards Plugin	External Classifier Plugin	Reports Plugin
Data Publisher	Flow Analyzer Plugin	Syslog Plugin
Data Receiver	Flow Collector	Technical Support Plugin
Device Classification Engine	IOC Scanner Plugin	Web Client Plugin

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 [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**.

### Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

#### To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

### Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend products. The portal also provides 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 product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend products. Software and related documentation 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/](https://updates.forescout.com/support/files/counteract/docs_portal/)

## Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), 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 in the Console.

**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**.

**Content Module, eyeSegment Module, and eyeExtend Product Help Files**

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

**Documentation Portal**

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