Forescout

Core Extensions Module: Device Classification Engine

Configuration Guide

Version 1.3

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 Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-03-19 14:27

Table of Contents

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.

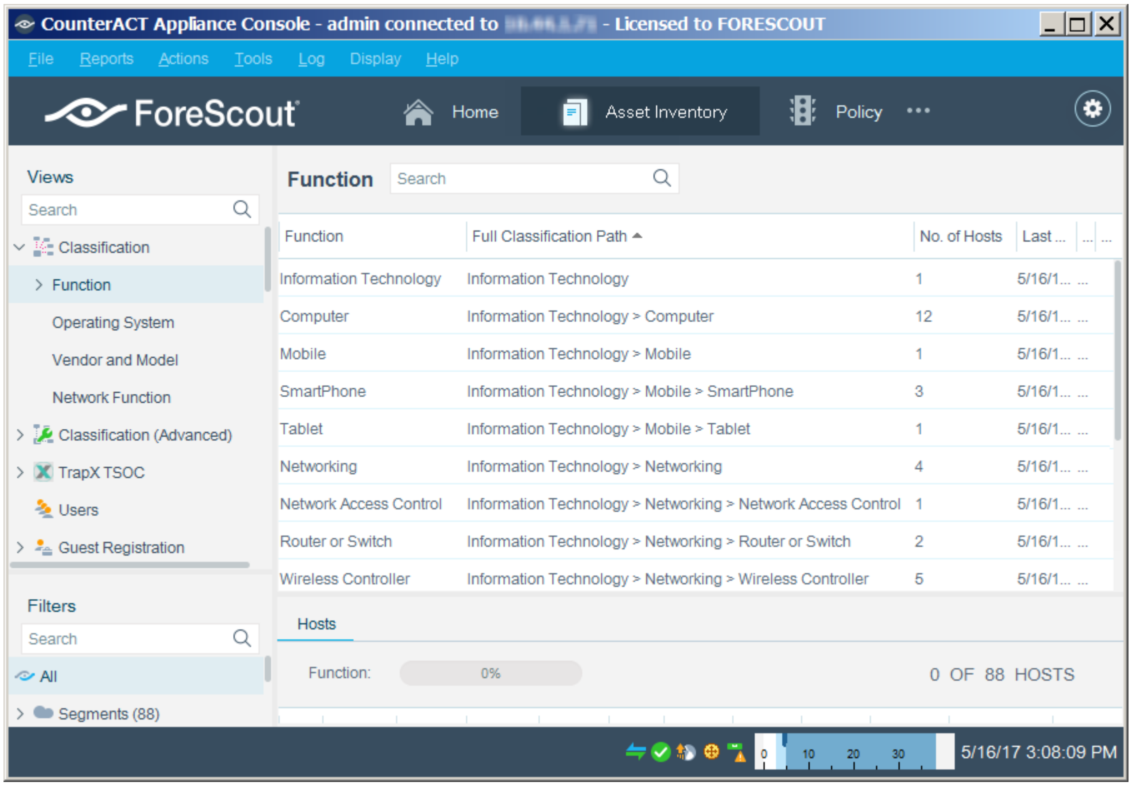
The Device Classification Engine is a core feature of Forescout 8.1 that resolves classification-related properties for comprehensive classification of each endpoint.

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 new classification metrics. See Inventory All Detected Endpoints.
- High level of 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 allows you to ensure complete classification coverage within your environment.

Inventory All Detected Endpoints

The Device Classification Engine classifies traditional IT as well as IoT devices connected to your network. After a Forescout 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 metric in the Asset Inventory view.



CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT

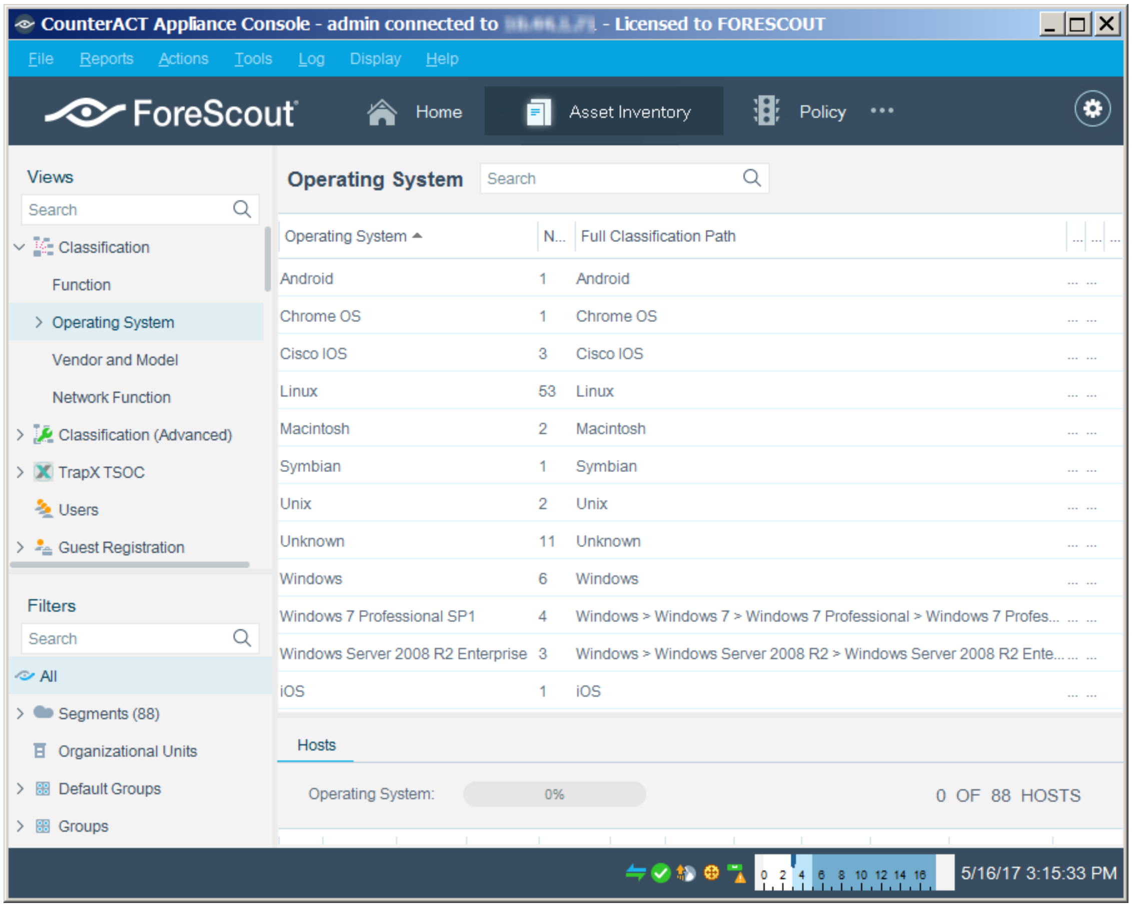
Function

Function	Full Classification Path	No. of Hosts	Last ...	...	...
Information Technology	Information Technology	1	5/16/1...	...	
Computer	Information Technology > Computer	12	5/16/1...	...	
Mobile	Information Technology > Mobile	1	5/16/1...	...	
SmartPhone	Information Technology > Mobile > SmartPhone	3	5/16/1...	...	
Tablet	Information Technology > Mobile > Tablet	1	5/16/1...	...	
Networking	Information Technology > Networking	4	5/16/1...	...	
Network Access Control	Information Technology > Networking > Network Access Control	1	5/16/1...	...	
Router or Switch	Information Technology > Networking > Router or Switch	2	5/16/1...	...	
Wireless Controller	Information Technology > Networking > Wireless Controller	5	5/16/1...	...	

Function: 0%

0 OF 88 HOSTS

5/16/17 3:08:09 PM



CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT

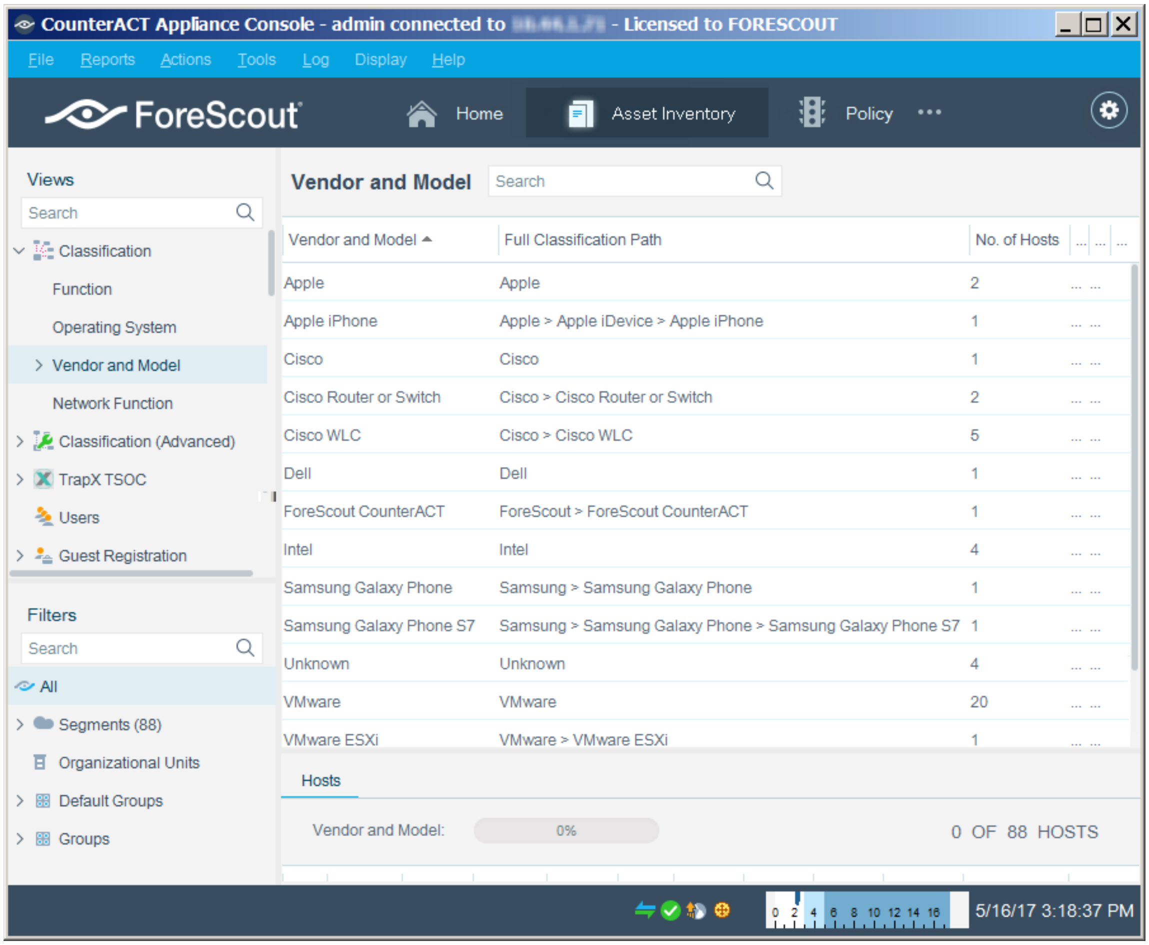
Operating System

Operating System	N...	Full Classification Path	...	...	...
Android	1	Android	...	...	
Chrome OS	1	Chrome OS	...	...	
Cisco IOS	3	Cisco IOS	...	...	
Linux	53	Linux	...	...	
Macintosh	2	Macintosh	...	...	
Symbian	1	Symbian	...	...	
Unix	2	Unix	...	...	
Unknown	11	Unknown	...	...	
Windows	6	Windows	...	...	
Windows 7 Professional SP1	4	Windows > Windows 7 > Windows 7 Professional > Windows 7 Profes...	...	...	
Windows Server 2008 R2 Enterprise	3	Windows > Windows Server 2008 R2 > Windows Server 2008 R2 Ente...	...	...	
iOS	1	iOS	...	...	

Operating System: 0%

0 OF 88 HOSTS

5/16/17 3:15:33 PM



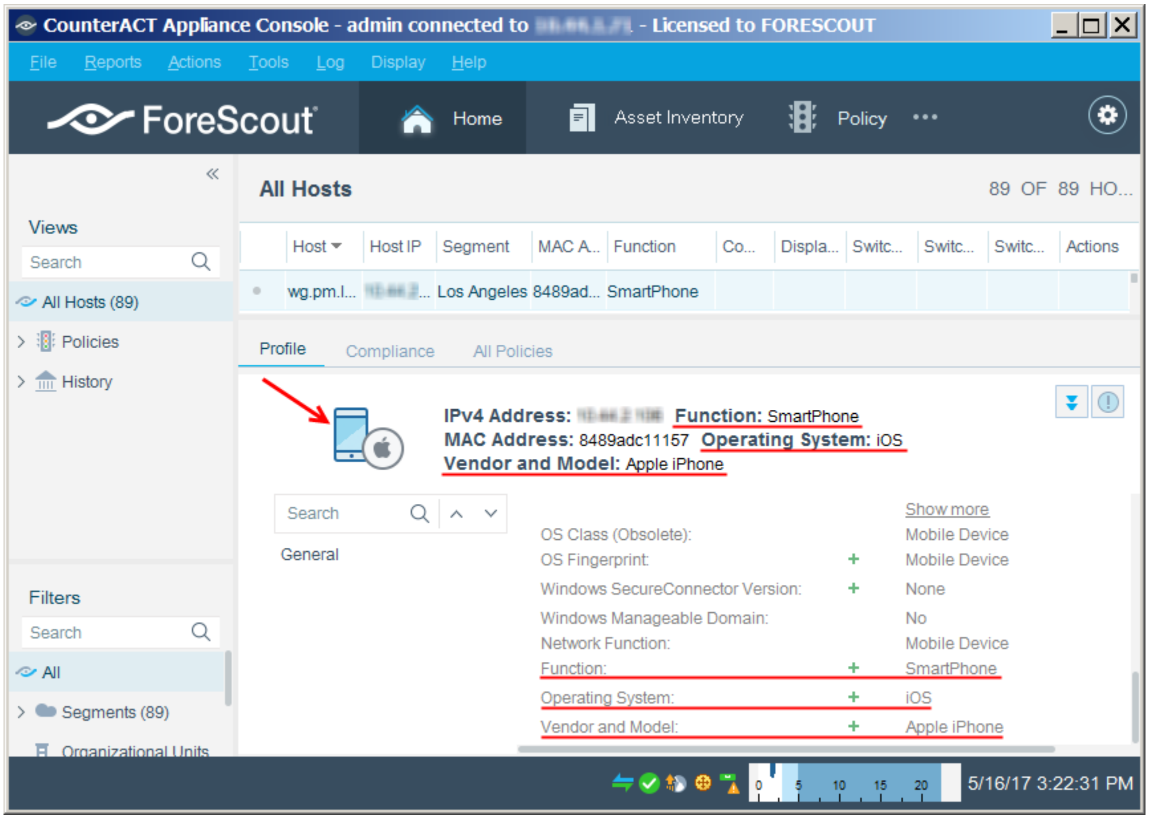
Vendor and Model

Vendor and Model ▲	Full Classification Path	No. of Hosts	...	...	...
Apple	Apple	2	...	...	
Apple iPhone	Apple > Apple iDevice > Apple iPhone	1	...	...	
Cisco	Cisco	1	...	...	
Cisco Router or Switch	Cisco > Cisco Router or Switch	2	...	...	
Cisco WLC	Cisco > Cisco WLC	5	...	...	
Dell	Dell	1	...	...	
ForeScout CounterACT	ForeScout > ForeScout CounterACT	1	...	...	
Intel	Intel	4	...	...	
Samsung Galaxy Phone	Samsung > Samsung Galaxy Phone	1	...	...	
Samsung Galaxy Phone S7	Samsung > Samsung Galaxy Phone > Samsung Galaxy Phone S7	1	...	...	
Unknown	Unknown	4	...	...	
VMware	VMware	20	...	...	
VMware ESXi	VMware > VMware ESXi	1	...	...	

Vendor and Model: 0% 0 OF 88 HOSTS

Endpoint Classification Details

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



	Host	Host IP	Segment	MAC A...	Function	Co...	Displa...	Switc...	Switc...	Switc...	Actions
	wg.pm.l...	[redacted]...	Los Angeles	8489ad...	SmartPhone						

IPv4 Address: [redacted] **Function:** SmartPhone
MAC Address: 8489adc11157 **Operating System:** iOS
Vendor and Model: Apple iPhone

OS Class (Obsolete):		Mobile Device
OS Fingerprint:	+	Mobile Device
Windows SecureConnector Version:	+	None
Windows Manageable Domain:		No
Network Function:		Mobile Device
Function:	+	SmartPhone
Operating System:	+	iOS
Vendor and Model:	+	Apple iPhone

🗎 *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 versions of CounterACT 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 the guide.

How It Works

The Device Profile Library contains classification profiles which 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 Forescout 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 the guide.
5. Install the Core Extensions Module whenever a new version is available.

🗎 *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 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 the guide.*

Forescout Requirements

The Device Classification Engine requires the following:

- Forescout version 8.1.
- 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.

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.

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

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.

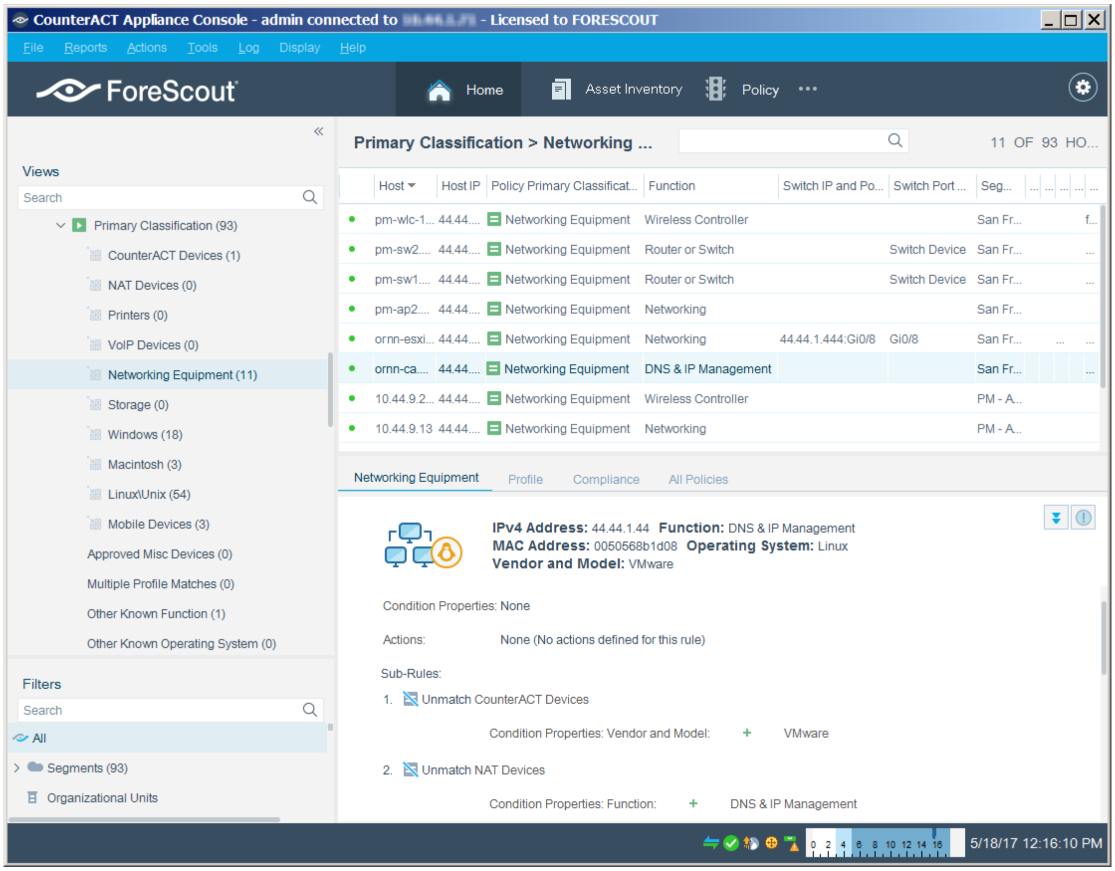
🗎 *If some endpoints in your network are known to be sensitive to network probing, see Handling Sensitive Endpoints.*

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

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

To see an overview of your policy:

1. In the Console Home tab, Views pane, expand the Policies folder.
2. 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.
3. Select a sub-rule. The endpoints that matched the rule are displayed.



CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT

Views

Search

- Primary Classification (93)
  - CounterACT Devices (1)
  - NAT Devices (0)
  - Printers (0)
  - VoIP Devices (0)
  - Networking Equipment (11)
  - Storage (0)
  - Windows (18)
  - Macintosh (3)
  - Linux\Unix (54)
  - Mobile Devices (3)
  - Approved Misc Devices (0)
  - Multiple Profile Matches (0)
  - Other Known Function (1)
  - Other Known Operating System (0)

Filters

Search

- All
- Segments (93)
- Organizational Units

Primary Classification > Networking ... 11 OF 93 HO...

	Host	Host IP	Policy Primary Classificat...	Function	Switch IP and Po...	Switch Port ...	Seg...	...	...	...	...	...
●	pm-wlc-1...	44.44....	Networking Equipment	Wireless Controller			San Fr...					f...
●	pm-sw2....	44.44....	Networking Equipment	Router or Switch		Switch Device	San Fr...					...
●	pm-sw1....	44.44....	Networking Equipment	Router or Switch		Switch Device	San Fr...					...
●	pm-ap2....	44.44....	Networking Equipment	Networking			San Fr...					
●	ornn-esxi...	44.44....	Networking Equipment	Networking	44.44.1.444:Gi0/8	Gi0/8	San Fr...			...		...
●	ornn-ca....	44.44....	Networking Equipment	DNS & IP Management			San Fr...					...
●	10.44.9.2...	44.44....	Networking Equipment	Wireless Controller			PM - A...					
●	10.44.9.13	44.44....	Networking Equipment	Networking			PM - A...					

IPv4 Address: 44.44.1.44 **Function:** DNS & IP Management
MAC Address: 0050568b1d08 **Operating System:** Linux
Vendor and Model: VMware

Condition Properties: None

Actions: None (No actions defined for this rule)

Sub-Rules:

1. Unmatch CounterACT Devices

   Condition Properties: Vendor and Model: + VMware

2. Unmatch NAT Devices

   Condition Properties: Function: + DNS & IP Management

5/18/17 12:16:10 PM

Custom Policies

Forescout policy tools provide an extensive range of options for detecting and handling endpoints. You can use a policy to instruct Forescout 8.1 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 Handling 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 on. 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.

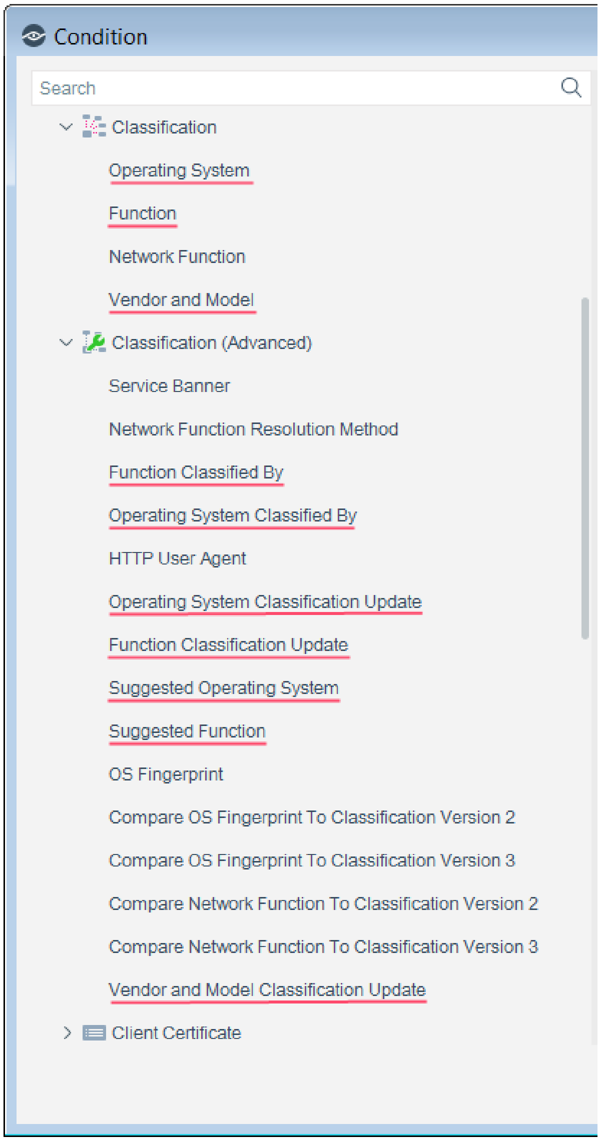
Handling Sensitive Endpoints

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). 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 the guide.

Policy Properties

To access classification-related properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Device classification properties are available in the following Properties nodes:
   - Classification Properties
   - Classification (Advanced) Properties


Condition
Search
Classification
Operating System
Function
Network Function
Vendor and Model
Classification (Advanced)
Service Banner
Network Function Resolution Method
Function Classified By
Operating System Classified By
HTTP User Agent
Operating System Classification Update
Function Classification Update
Suggested Operating System
Suggested Function
OS Fingerprint
Compare OS Fingerprint To Classification Version 2
Compare OS Fingerprint To Classification Version 3
Compare Network Function To Classification Version 2
Compare Network Function To Classification Version 3
Vendor and Model Classification Update
Client Certificate

Classification Properties

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

- 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 node.

Property	Description
Function Classified By	Indicates if the *Function* classification property was determined by the Device Classification Engine or set by an action.
Operating System Classified By	Indicates if the *Operating System* classification property was determined by the Device Classification Engine or set by an action.
Function Classification Update	Indicates if a *Function* classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the Options > Classification > Pending Updates window.
Operating System Classification Update	Indicates if an *Operating System* classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the Options > Classification > Pending Updates window.
Vendor and Model Classification Update	Indicates if a *Vendor and Model* classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the Options > Classification > Pending Updates window.
Suggested Function	If there are multiple candidates for the endpoint's *Function* 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 *Function* property value, possibly due to conflicting choices. If the *Function* property has been changed by a policy or manual action, this property indicates the endpoint's *Function* classification set by the Device Classification Engine. See Classify Actions.
Suggested Operating System	If there are multiple candidates for the endpoint's *Operating System* 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 *Operating System* property value, possibly due to conflicting choices. If the *Operating System* property has been changed by a policy or manual action, this property indicates the endpoint's *Operating System* classification set by the Device Classification Engine. See Classify Actions.

Classify Actions

If a *Function* or *Operating System* property value set by the Device Classification Engine is not the optimal classification for your compliance and control policies, you can override the value.

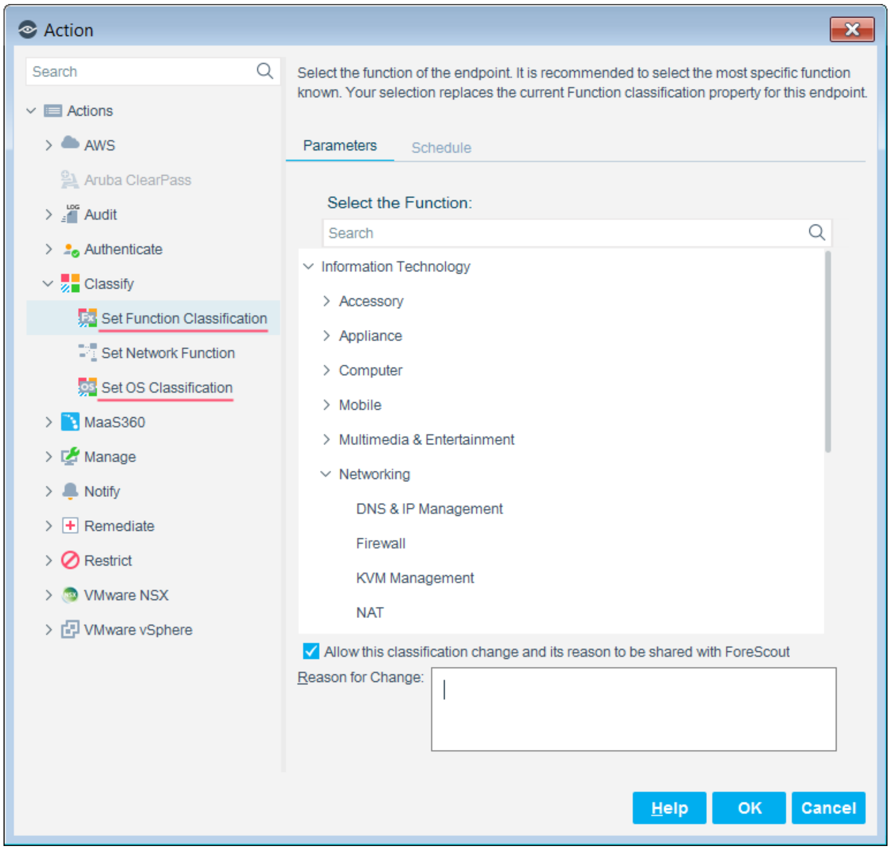
This is useful when:

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



Select the function of the endpoint. It is recommended to select the most specific function known. Your selection replaces the current Function classification property for this endpoint.

☑ Allow this classification change and its reason to be shared with ForeScout

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 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 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 Tools > Options > Advanced > Data Sharing, and select* ***Allow selected endpoint properties to be shared 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. In the Home tab, right-click the endpoint.
2. Expand the Cancel Actions node and select one of the following actions:

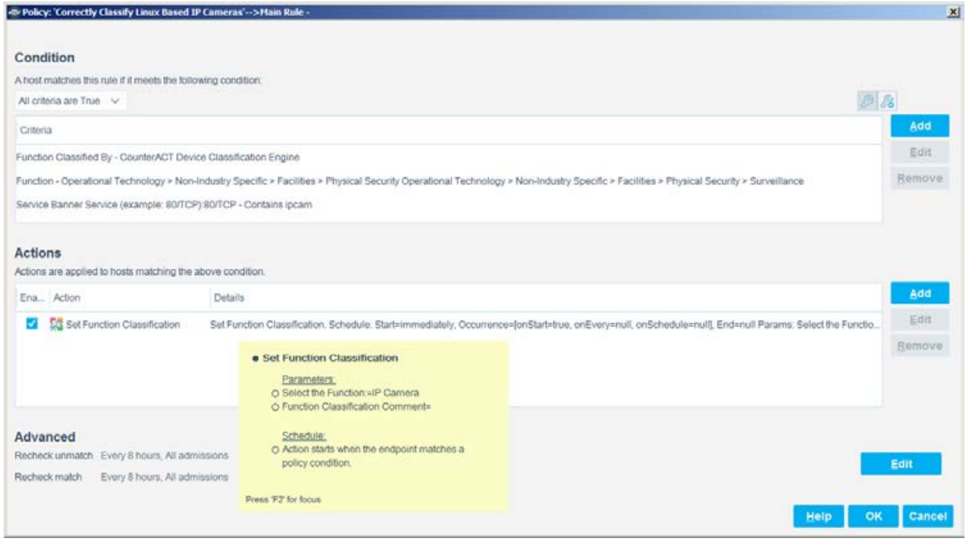
- Revert to Suggested Function Classification
- Revert to Suggested Operating System Classification

Classification Property Fine Tuning

Forescout 8.1 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.

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.



Policy: 'Correctly Classify Linux Based IP Cameras'-->Main Rule -

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
Function Classified By - CounterACT Device Classification Engine
Function - Operational Technology > Non-Industry Specific > Facilities > Physical Security Operational Technology > Non-Industry Specific > Facilities > Physical Security > Surveillance
Service Banner Service (example: 80/TCP):80/TCP - Contains ipcam

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
☑	Set Function Classification	Set Function Classification. Schedule: Start=immediately, Occurrence=[onStart=true, onEvery=null, onSchedule=null], End=null Params: Select the Functio...

● Set Function Classification

Parameters:
○ Select the Function:=IP Camera
○ Function Classification Comment=

Schedule:
○ Action starts when the endpoint matches a policy condition.

Press 'F2' for focus

Advanced

Recheck unmatch Every 8 hours, All admissions

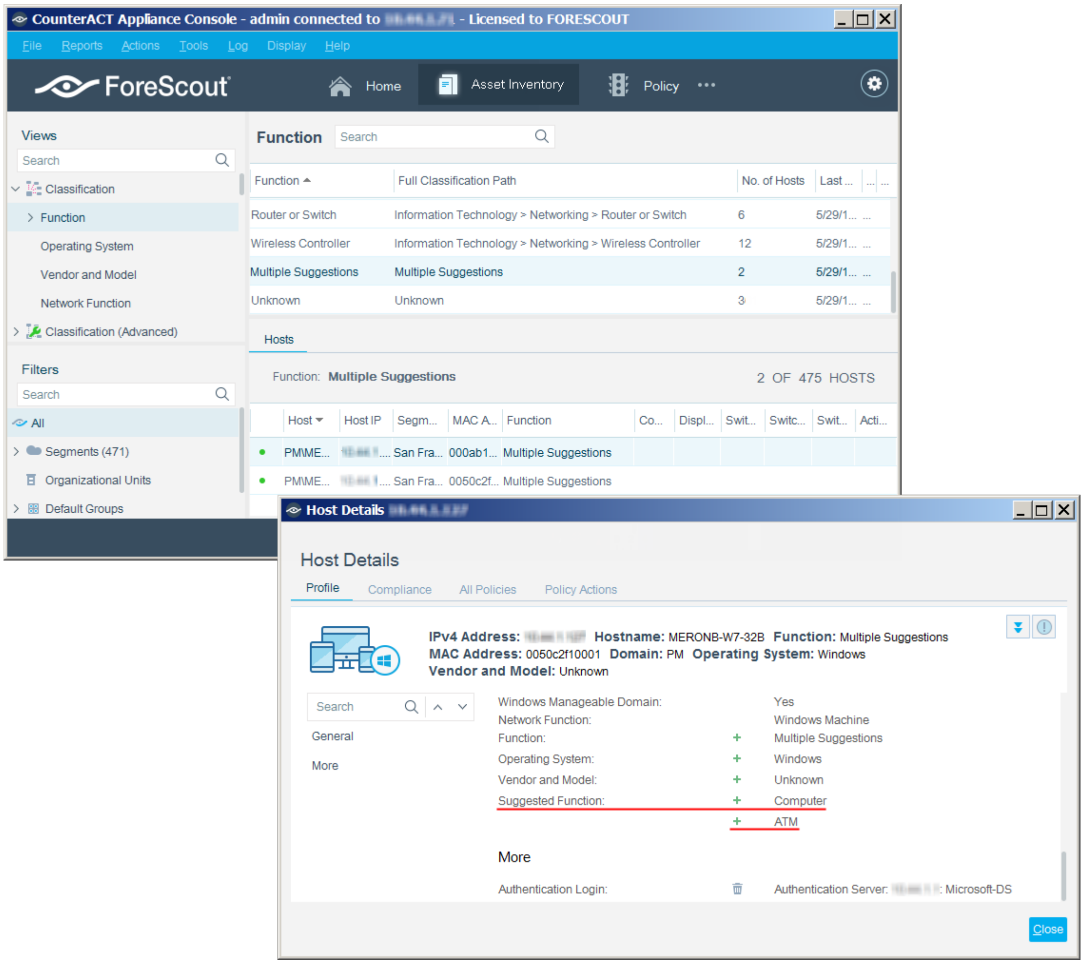
Recheck match Every 8 hours, All admissions

To fine-tune the classification results:

1. Navigate to each of the *Function* and *Operating System* results in the Classification node of the Asset Inventory view.
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.



Function

Function	Full Classification Path	No. of Hosts	Last ...	...	...
Router or Switch	Information Technology > Networking > Router or Switch	6	5/29/1...	...	
Wireless Controller	Information Technology > Networking > Wireless Controller	12	5/29/1...	...	
Multiple Suggestions	Multiple Suggestions	2	5/29/1...	...	
Unknown	Unknown	3	5/29/1...	...	

Hosts

Function: **Multiple Suggestions** 2 OF 475 HOSTS

	Host	Host IP	Segm...	MAC A...	Function	Co...	Displ...	Swit...	Switc...	Swit...	Acti...
●	PM\ME...	[redacted]....	San Fra...	000ab1...	Multiple Suggestions						
●	PM\ME...	[redacted]....	San Fra...	0050c2f...	Multiple Suggestions						

Host Details [redacted]

Host Details

IPv4 Address: [redacted] **Hostname:** MERONB-W7-32B **Function:** Multiple Suggestions
MAC Address: 0050c2f10001 **Domain:** PM **Operating System:** Windows
Vendor and Model: Unknown

Windows Manageable Domain:		Yes
Network Function:		Windows Machine
Function:	+	Multiple Suggestions
Operating System:	+	Windows
Vendor and Model:	+	Unknown
Suggested Function:	+	Computer
	+	ATM

More

Authentication Login: Authentication Server: [redacted]: Microsoft-DS

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. For example, you might create a policy that uses the *Set Function Classification* action to classify any endpoint that has Suggested Functions of *Computer* and *ATM* ***and*** an Operating System of *Windows*, with the Function of *Computer*.
- 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, Forescout upgrades the Device Profile Library 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

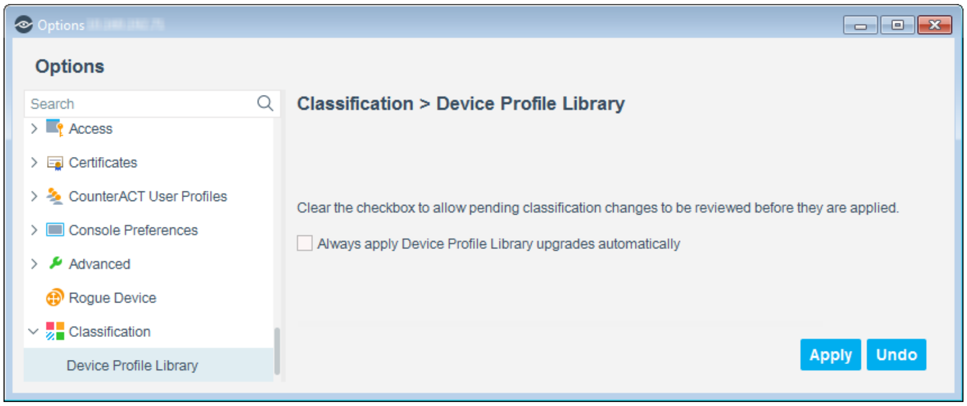
It is not recommended to perform Set Classification actions after a new Device Profile Library version is installed and before it is applied or rolled back. If these actions are performed:

- 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 Tools > Options > Classification > Device Profile Library.



Classification > Device Profile Library

Clear the checkbox to allow pending classification changes to be reviewed before they are applied.

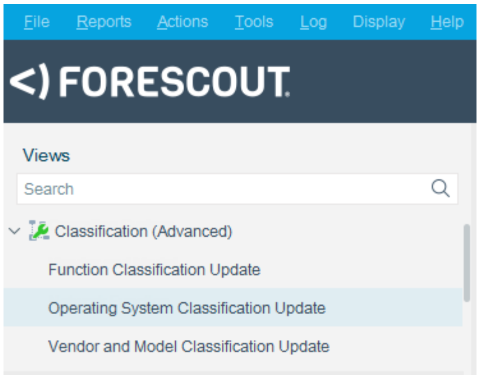
□ Always apply Device Profile Library upgrades automatically

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

Review Pending Profile Changes

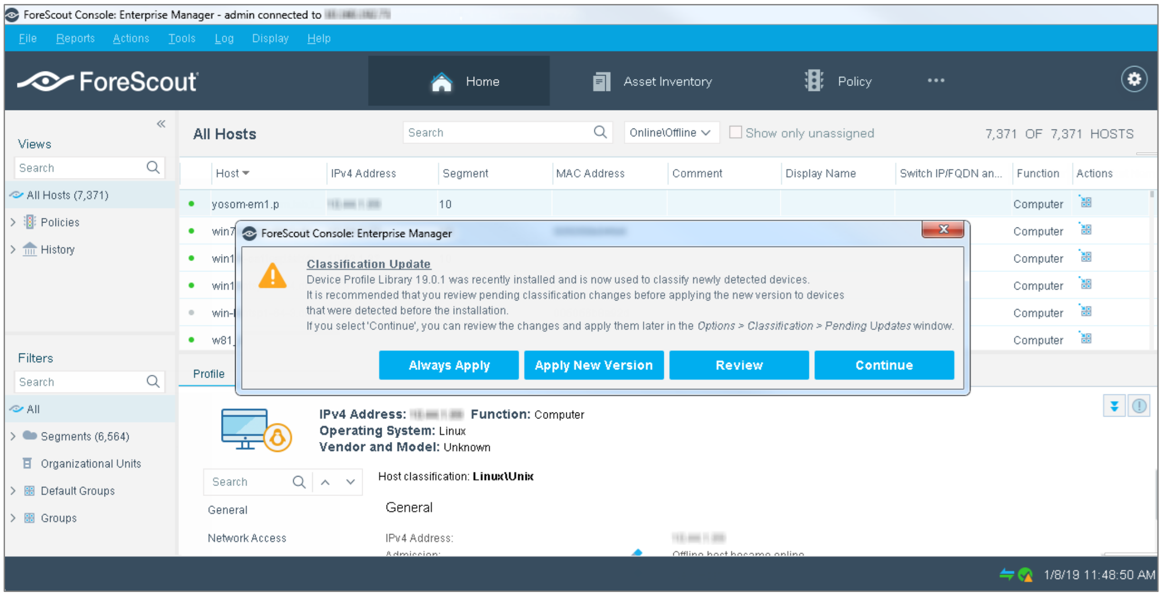
To view pending change requests without applying them:

- In the Asset Inventory tab Views pane, expand Classification (Advanced), and select the appropriate classification property.


File
Reports
Actions
Tools
Log
Display
Help
<) FORESCOUT
Views
Search
Classification (Advanced)
Function Classification Update
Operating System Classification Update
Vendor and Model Classification Update

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 pops up. To review the changes, select **Review**.



Host	IPv4 Address	Segment	MAC Address	Comment	Display Name	Switch IP/FQDN an...	Function	Actions
yosom-em1.p	[redacted]	10					Computer	
win7							Computer	
win1							Computer	
win1							Computer	
win-							Computer	
w81							Computer	

ForeScout Console: Enterprise Manager

Classification Update

Device Profile Library 19.0.1 was recently installed and is now used to classify newly detected devices.
It is recommended that you review pending classification changes before applying the new version to devices that were detected before the installation.
If you select 'Continue', you can review the changes and apply them later in the *Options > Classification > Pending Updates* window.

Always Apply | Apply New Version | Review | Continue

IPv4 Address: [redacted] **Function:** Computer
Operating System: Linux
Vendor and Model: Unknown

Host classification: **Linux\Unix**

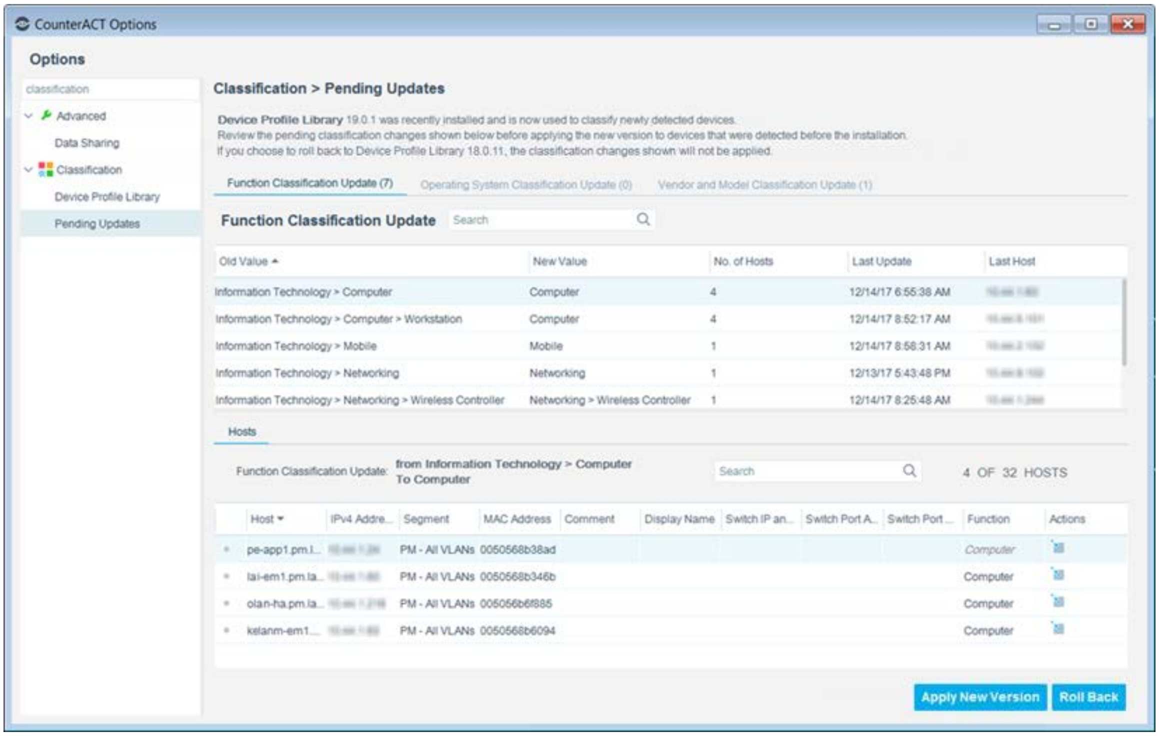
General

IPv4 Address: [redacted]

– After a Device Profile Library is installed, an icon appears 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 Tools > Options > Classification > Pending Updates.



Classification > Pending Updates

Device Profile Library 19.0.1 was recently installed and is now used to classify newly detected devices.
Review the pending classification changes shown below before applying the new version to devices that were detected before the installation.
If you choose to roll back to Device Profile Library 18.0.11, the classification changes shown will not be applied.

Function Classification Update

Old Value	New Value	No. of Hosts	Last Update	Last Host
Information Technology > Computer	Computer	4	12/14/17 6:55:38 AM	[redacted]
Information Technology > Computer > Workstation	Computer	4	12/14/17 8:52:17 AM	[redacted]
Information Technology > Mobile	Mobile	1	12/14/17 8:58:31 AM	[redacted]
Information Technology > Networking	Networking	1	12/13/17 5:43:48 PM	[redacted]
Information Technology > Networking > Wireless Controller	Networking > Wireless Controller	1	12/14/17 8:25:48 AM	[redacted]

Function Classification Update: **from Information Technology > Computer To Computer**

4 OF 32 HOSTS

Host	IPv4 Addre...	Segment	MAC Address	Comment	Display Name	Switch IP an...	Switch Port A...	Switch Port ...	Function	Actions
pe-app1.pm.l...	[redacted]	PM - All VLANs	0050568b38ad						*Computer*	
lai-em1.pm.la...	[redacted]	PM - All VLANs	0050568b346b						Computer	
olan-ha.pm.la...	[redacted]	PM - All VLANs	005056b6f885						Computer	
kelanm-em1...	[redacted]	PM - All VLANs	0050568b6094						Computer	

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 window. Then return to this window 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 window and select **Apply New Version**.
   - If the changes are not acceptable, select **Roll Back**, and then select the Device Profile Library version to revert to. 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 allows you to 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 Tools > Options > Advanced > Data Sharing, and select **Allow selected endpoint properties to be shared 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 the 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
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Dashboard Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
- Flow Collector
- IOC Scanner Plugin
- IoT Posture Assessment Engine
- NBT Scanner Plugin
- Packet Engine
- Reports Plugin
- Syslog Plugin
- Technical Support Plugin
- Web Client Plugin

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation.

Additional Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

🗎 *Software downloads are also available from these portals.*

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

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

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

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

🗎 *If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.*

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

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 **Forescout Help** from the **Help** menu.

Plugin Help Files

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

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).