ForeScout CounterACT®

Core Extensions Module: Device Classification Engine

Configuration Guide

Version 1.1

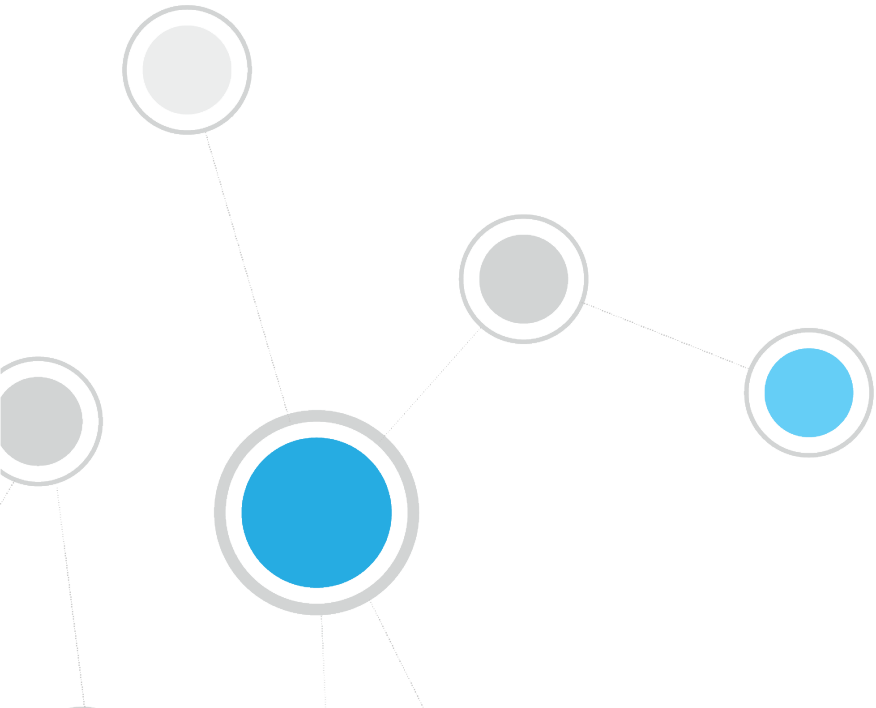


Table of Contents

About the Device Classification Engine

The Device Classification Engine is a component of the ForeScout CounterACT® Core Extensions Module. See Core Extensions Module Information for details about the module.

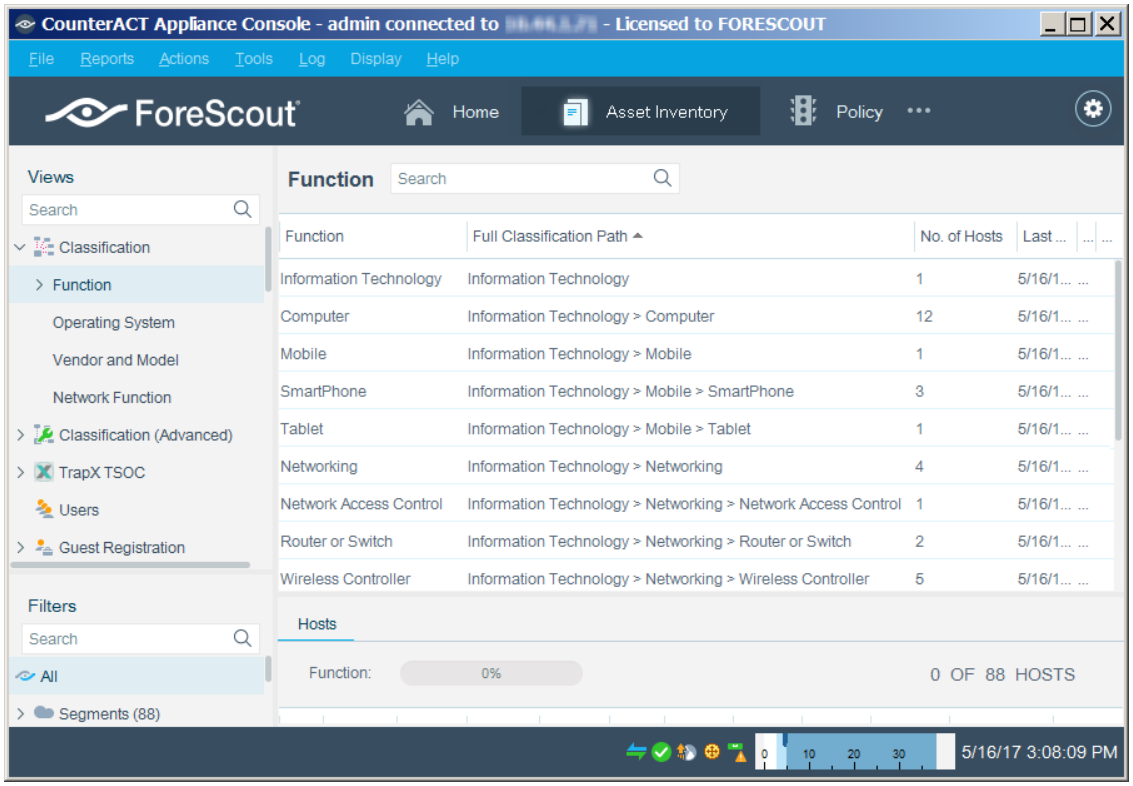
The Device Classification Engine is a core feature of CounterACT that resolves classification-related properties for comprehensive classification of each endpoint.

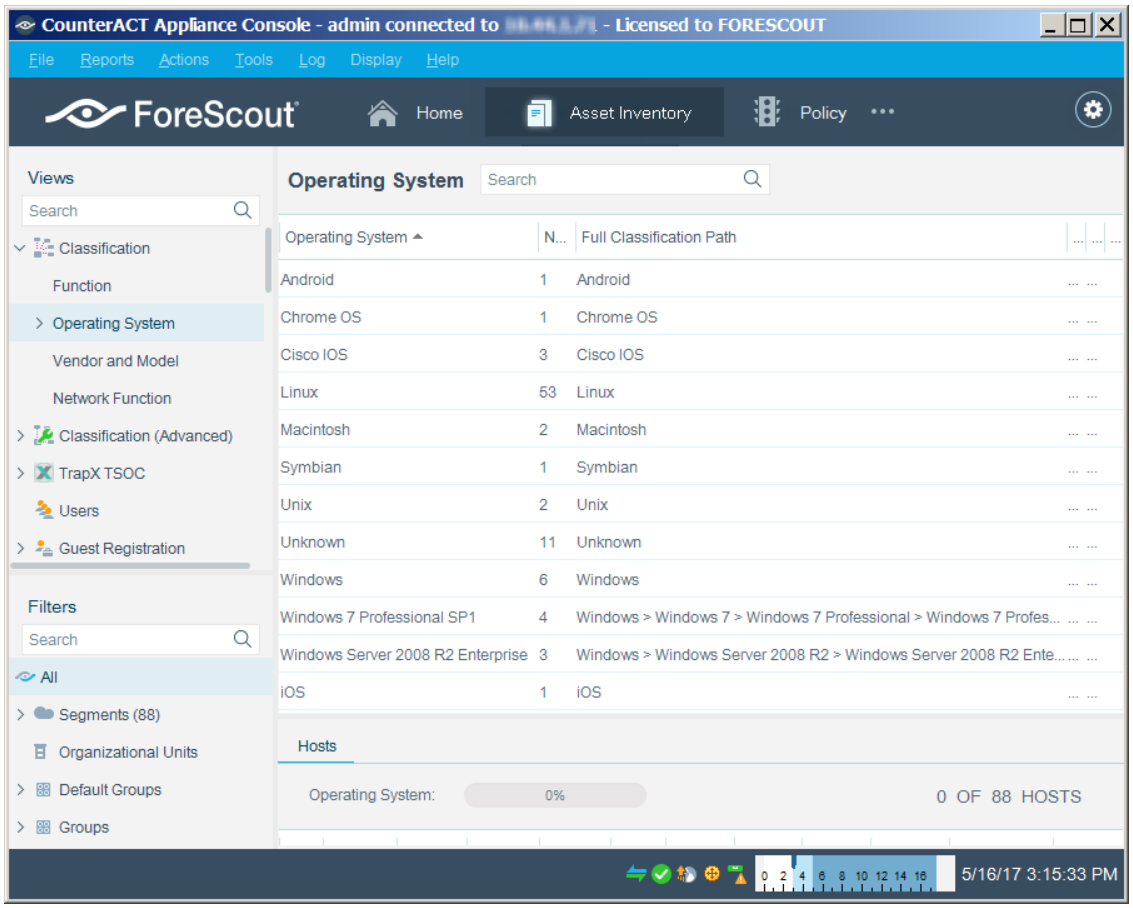
The key benefits of the Device Classification Engine are:

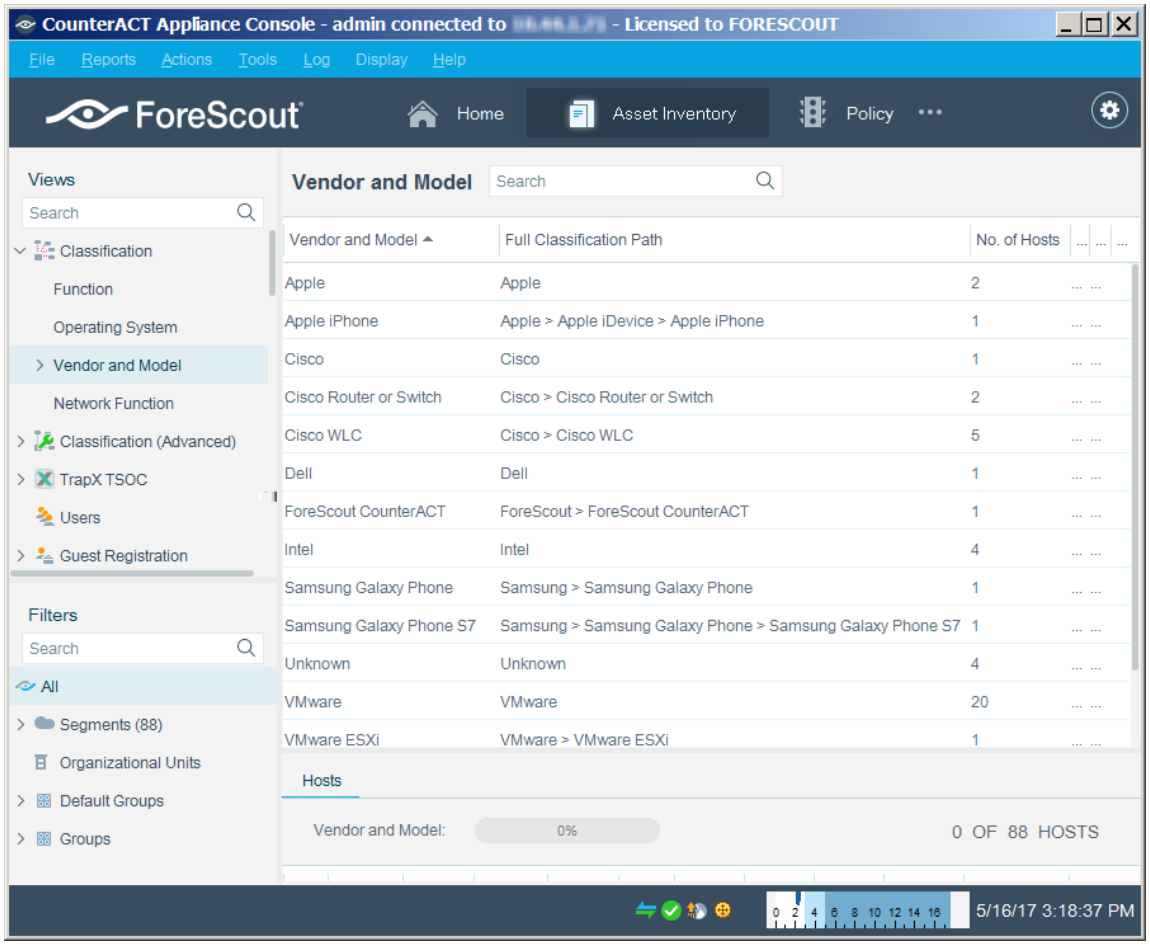
- 'Out obile, and virtual endpoints connected to your network.
- Comprf the box' precise classification of traditional IT devices as well as IoT, OT, moehensive view of all endpoints in the inventory across three new classification metrics. See Inventory All Detected Endpoints.
- High level of granular 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 CounterACT runs a policy 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.

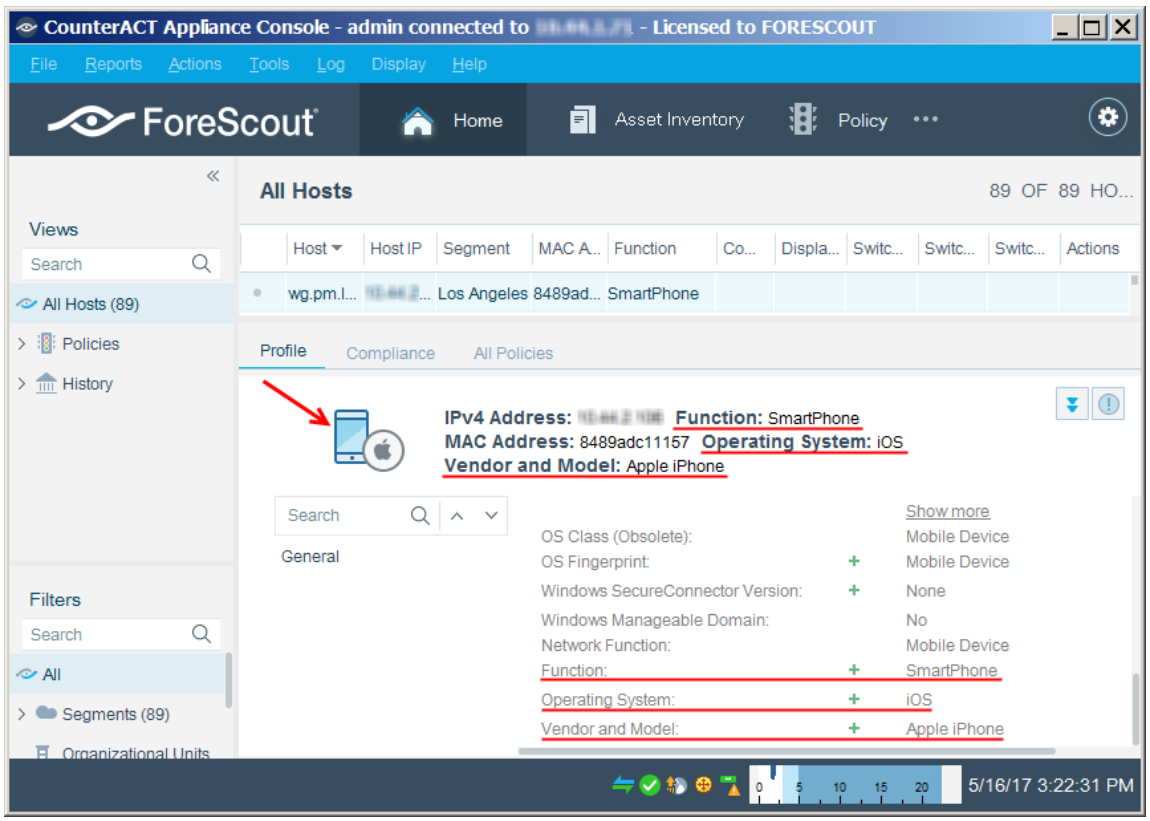

CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT
File Reports Actions Tools Log Display Help
ForeScout
Home
Asset Inventory
Policy
Views
Search
Classification
Function
Operating System
Vendor and Model
Network Function
Classification (Advanced)
TrapX TSOC
Users
Guest Registration
Filters
Search
All
Segments (88)
Function
Search
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...
Hosts
Function:
0%
0 OF 88 HOSTS
5/16/17 3:08:09 PM


CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT
File Reports Actions Tools Log Display Help
ForeScout
Home
Asset Inventory
Policy
Views
Search
Classification
Function
Operating System
Vendor and Model
Network Function
Classification (Advanced)
TrapX TSOC
Users
Guest Registration
Filters
Search
All
Segments (88)
Organizational Units
Default Groups
Groups
Operating System
Search
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
Hosts
Operating System:
0%
0 OF 88 HOSTS
5/16/17 3:15:33 PM


CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT
File Reports Actions Tools Log Display Help
ForeScout
Home
Asset Inventory
Policy
Views
Search
Classification
Function
Operating System
Vendor and Model
Network Function
Classification (Advanced)
TrapX TSOC
Users
Guest Registration
Filters
Search
All
Segments (88)
Organizational Units
Default Groups
Groups
Vendor and Model
Search
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
Hosts
Vendor and Model: 0%
0 OF 88 HOSTS
0 2 4 6 8 10 12 14 16
5/16/17 3:18:37 PM

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.



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.

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

For more information about the *Primary Classification* and *Asset Classification* policies, refer to the *CounterACT Administration Guide*. See Additional CounterACT Documentation for information on how to access the guide.

How It Works

The Device Profile Library contains classification profiles which are composed of various CounterACT 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 the set of properties which 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 CounterACT detects for an endpoint, the greater the potential for an accurate and granular classification. CounterACT integration with third party components and network devices, such as switches, wireless controllers and hypervisors, increases the number of endpoint properties that can be detected for endpoints and therefore aids in detecting the most appropriate classification profile.

What to Do

Perform the following to work with the Device Classification Engine:

1. Verify that you have met system requirements. See CounterACT Software Requirements.
2. Do one of the following to resolve the classification properties on your endpoints:
   - 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 *CounterACT Device Profile Library Configuration Guide*. See Additional CounterACT 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* CounterACT Administration Guide *for more information about this program. See Additional CounterACT Documentation for information on how to access the guide.*

CounterACT Software Requirements

The Device Classification Engine requires the following CounterACT releases and other CounterACT components:

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

Configure the Device Classification Engine

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 About the Primary Classification Policy Template and About 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.

About the 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 coarse grained summary of the different device types detected in your network. Most sub-rules in the template contain an *Add to Group* action that is disabled by default. These replicate the groups created by an Asset Classification policy.

  To use a policy created by the Primary Classification template as your main classification policy, enable the Add to Group *actions in the sub-rules, and stop any Asset Classification policies that may be running.*

Run the policy to resolve:

- the following Classification Properties:
  - Function
  - Operating System
  - Vendor and Model
- the following 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 additional 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 there are endpoints in your network that are known to be sensitive to network probing, see Handling Sensitive Endpoints.

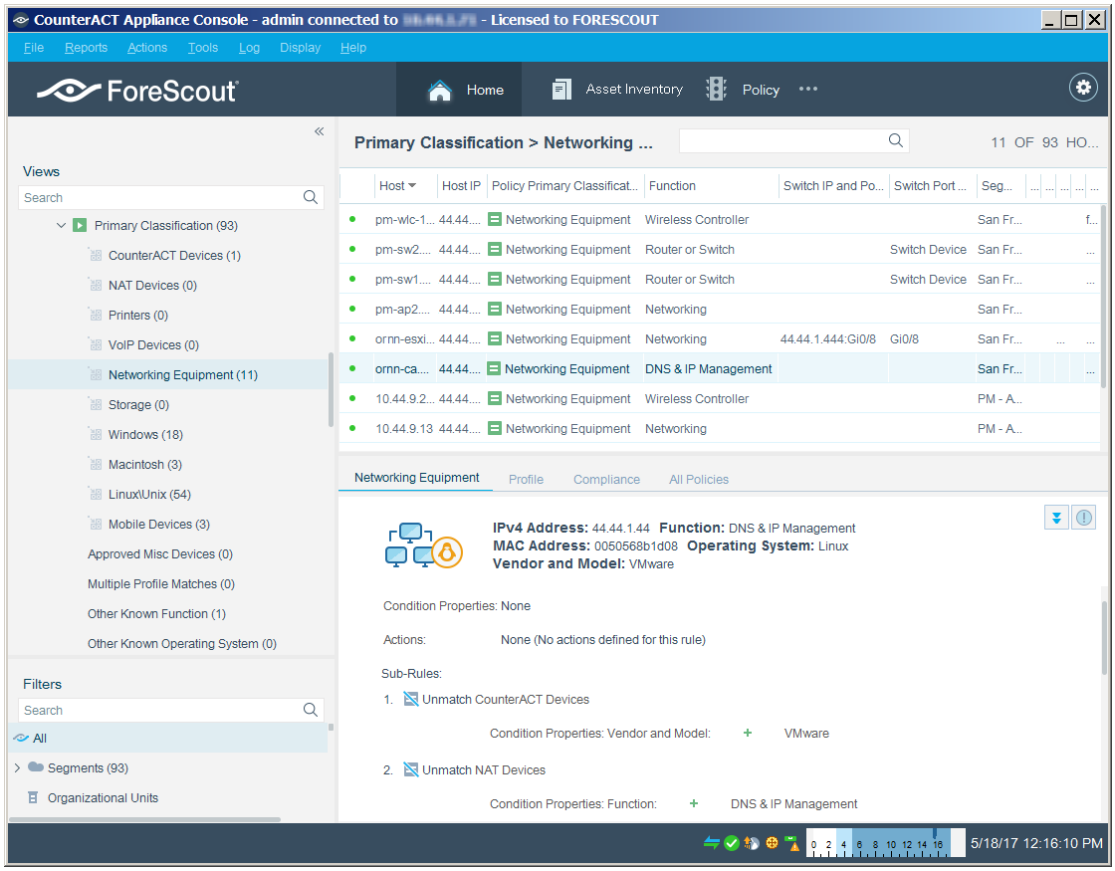
For more information about the CounterACT Primary Classification policy template, refer to the *CounterACT Templates* and *Policy Management* chapters of the *CounterACT Administration Guide*. See Additional CounterACT Documentation for information on how to access the guide.

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 in the Detections pane.



About Custom Policies

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

> *If there are endpoints in your network that 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.

Examples of Custom Policies

- 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 that 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.

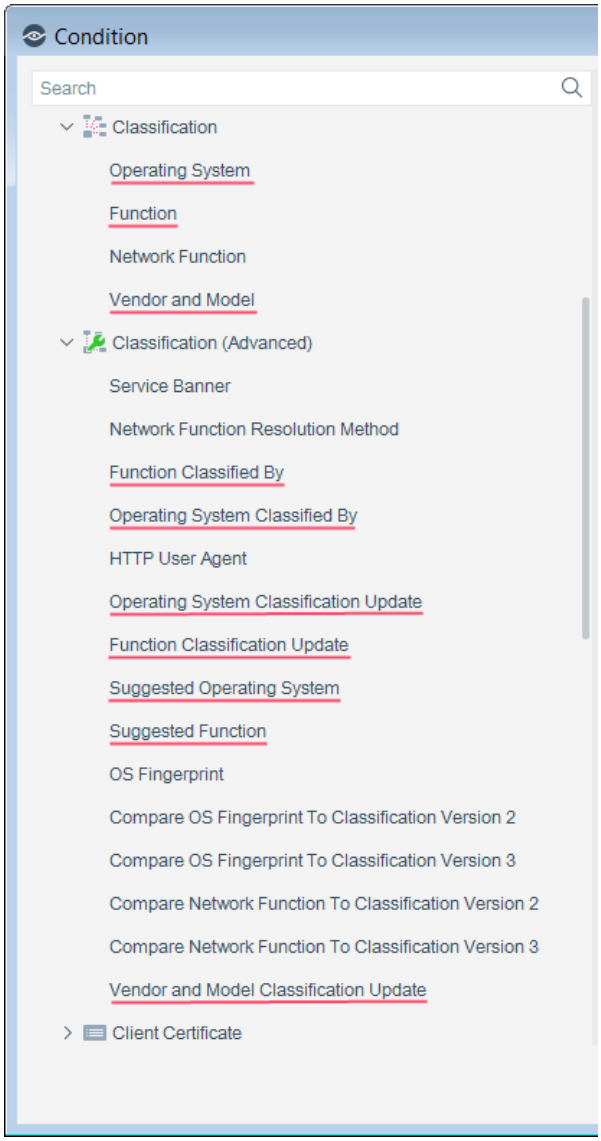
Handling Sensitive Endpoints

CounterACT 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 *CounterACT Administration Guide*. See Additional CounterACT 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



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, the following describes what happens when the Classification Engine cannot definitively match the endpoint to a specific classification profile in the Device Profile Library:

- 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 also 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 was set by an action.
Operating System Classified By	Indicates if the *Operating System* classification property was determined by the Device Classification Engine, or was 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 > Device Profile Library 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 > Device Profile Library 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 > Device Profile Library window.
Suggested Function	If there are multiple candidates for the endpoint's *Function* classification, then this property indicates all the profiles in the CounterACT Device Profile Library that match this endpoint. These values were 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, then this property indicates all the profiles in the CounterACT Device Profile Library that match this endpoint. These values were 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.

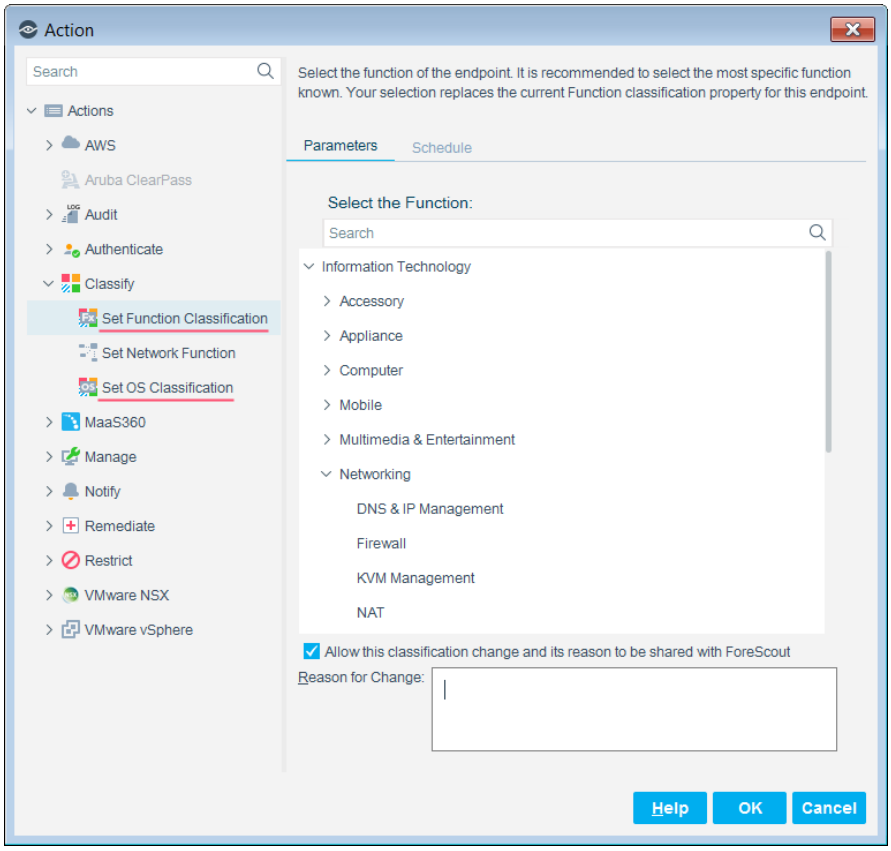
This is useful when:

- The classification resolved by CounterACT is not correct or CounterACT was not able to classify an endpoint.
- You are able to refine the classification resolved by CounterACT. For example, CounterACT classified the device as Healthcare, but you know it's actually an X-Ray device.
- The endpoint was 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. The following actions are available to override a classification property set by the Device Classification Engine:
   - Set Function Classification
   - Set OS Classification



4. If you have opted in to data sharing, the classification change will be 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 that you enter in this field will be sent to ForeScout to help provide better classification services.

   To ensure that your changes are shared with ForeScout, first go to Tools > Options > Advanced > Data Sharing, and select ***Allow selected endpoint properties to be shared with ForeScout****. See Sharing Data with ForeScout.*

Cancel Classify Actions

After using an action to override an endpoint's classification property, you can undo your classification assignment and reset the property value to that 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.

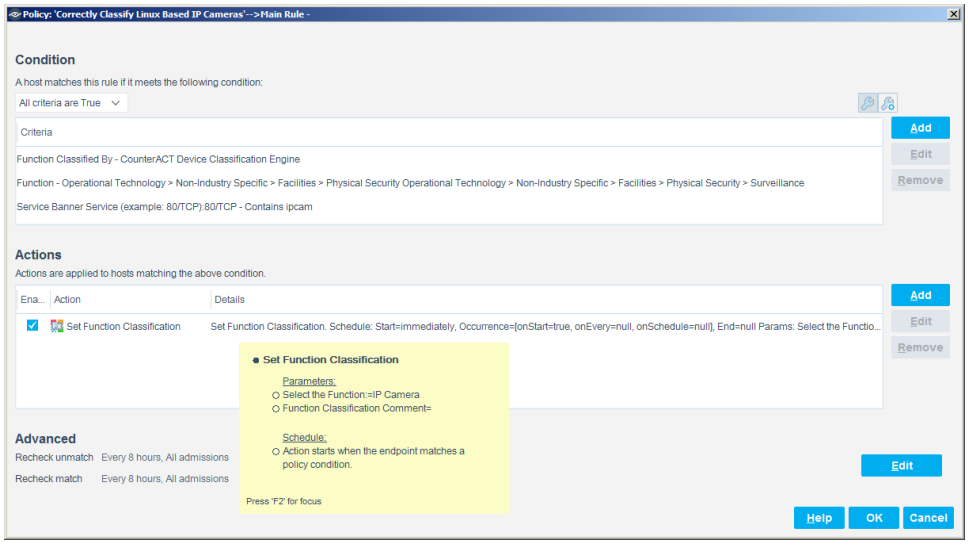
2. Expand the Cancel Actions node. The following actions are available to reset a classification property that was manually changed:
   - Revert to Suggested Function Classification
   - Revert to Suggested Operating System Classification

Classification Property Fine Tuning

CounterACT classifies your endpoints with a high degree of accuracy. It is possible that some endpoints may 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 CounterACT.
   - It was classified as a specific Function.
   - One or more properties provide other specific information about the device that indicates that the device has a more specific, or different, Function.
2. When this condition is met, set the Function to a different value.

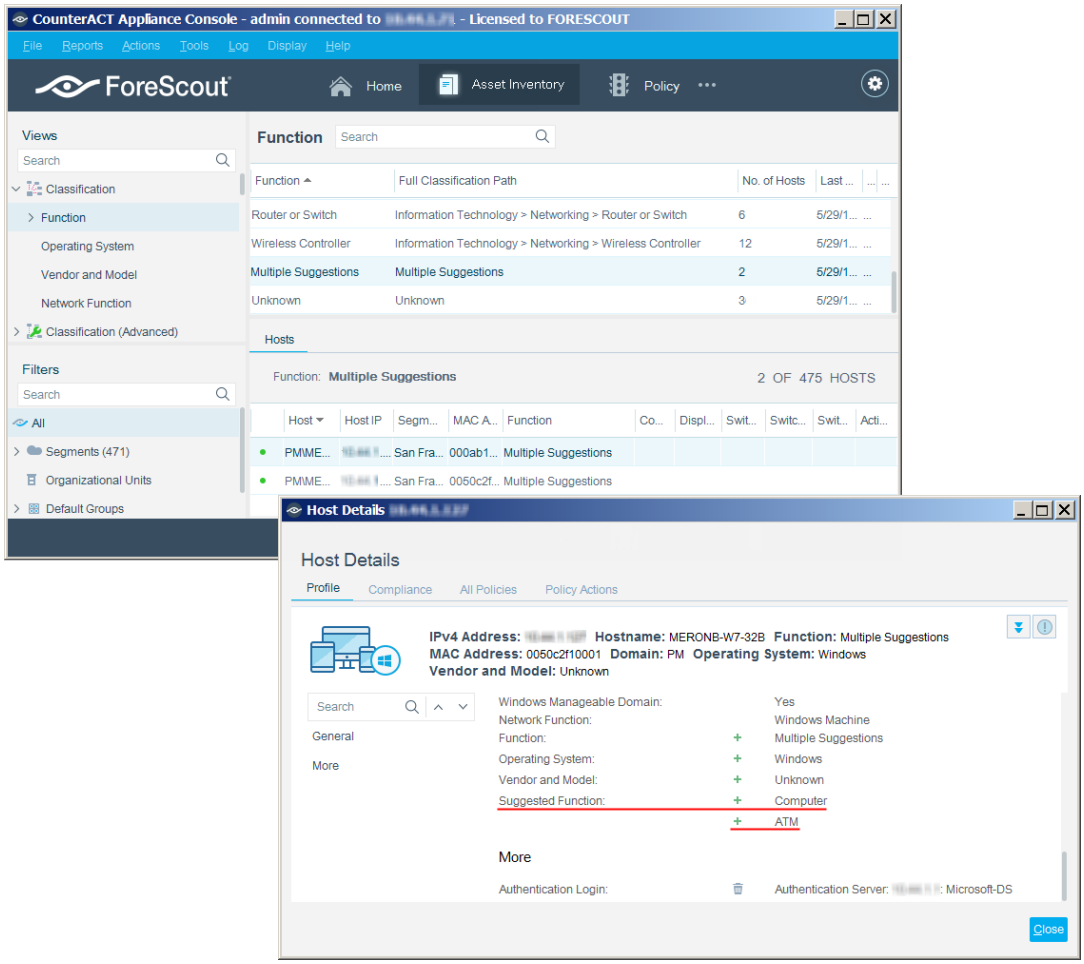


To fine-tune the classification results:

1. 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, a list is displayed of all the endpoints that matched conflicting profiles.

   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. In the example in the screenshot, you might create a policy that uses the *Set Function Classification* action to classify any endpoint that has Suggested Functions of *Computer* as well as *ATM* ***and*** an Operating System of *Windows*, to 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. In the Hosts pane, a list is displayed of all the endpoints that did not match a profile.

For each endpoint in the Hosts pane whose classification you know, 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.

Updating Classification Profiles

ForeScout upgrades the Device Profile Library periodically to improve classification accuracy and to provide better coverage. After a new version of Device Profile Library is installed, it is recommended to run a policy that resolves classification properties. Due to classification profile changes in the new library version, some device classifications may change. Before these changes are applied to the endpoints, you can review all the pending changes and decide if you want to apply them, modify existing policies and then apply the changes, or cancel the changes and roll back to a previous Device Profile Library version.

This Classification Update feature is installed with CounterACT version 8.0 and Device Profile Library version 18.0.4, but it is not triggered until subsequent versions of the Device Profile Library are installed.

To always review pending classification changes following future Device Profile Library upgrades, go to Tools > Options> Device Profile Library, and ensure that the **Always apply classification updates** checkbox is not selected.

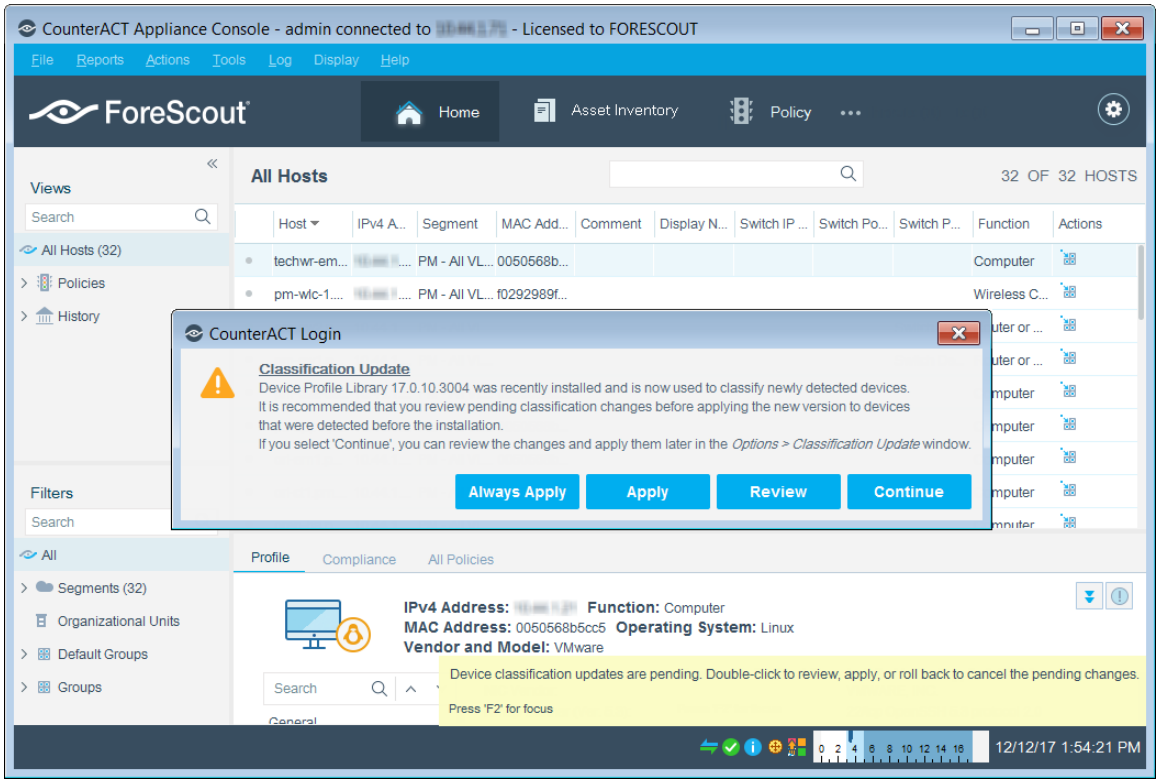
Each time the Device Profile Library is upgraded, the following endpoint properties are resolved and used to indicate pending classification changes:

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

For more information about these properties, see Classification (Advanced) Properties.

To manage the pending classification changes following a Device Profile Library upgrade:

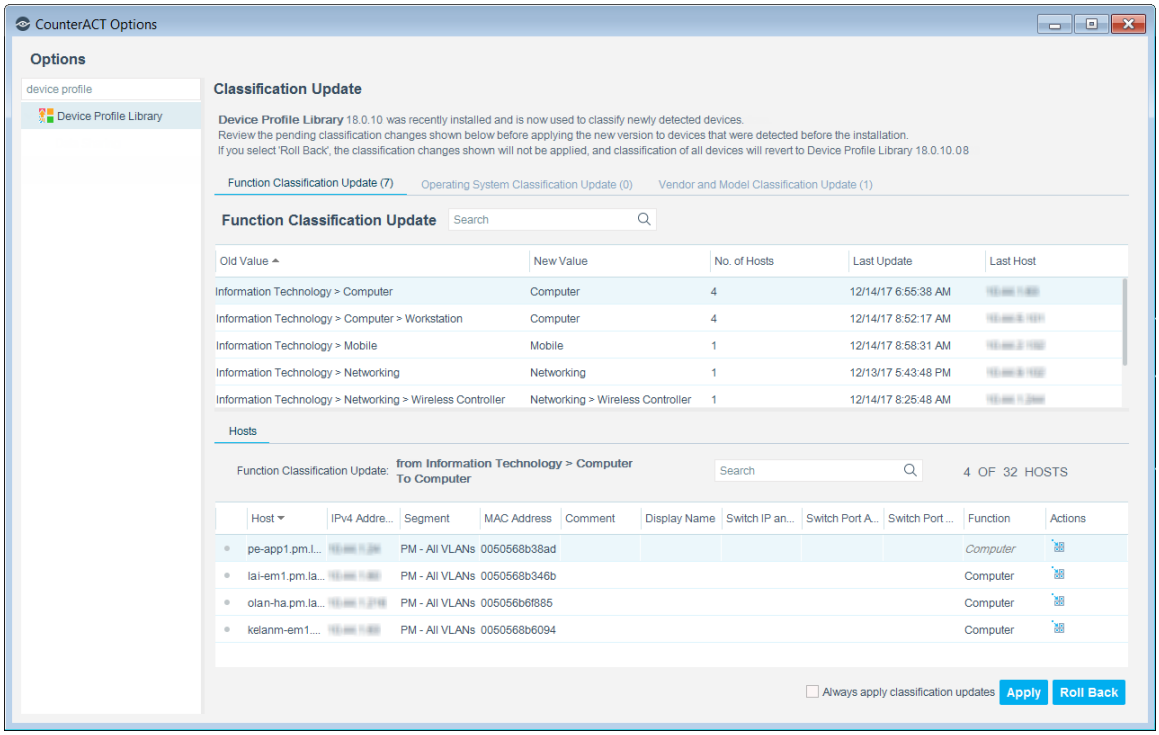
1. To see the pending classification changes following a Device Profile Library upgrade, do one of the following:
   - Eight hours after the Device Profile Library is installed, a *Classification Update* message pops up. To review the changes, select **Review**.



– After a Device Profile Library is installed and an icon appears in the task bar, double-click the icon.

If you do not review the pending classification changes within a reasonable amount of time, the icon will start blinking to remind you to review them.

– At any time, go to Tools > Options > Device Profile Library.



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**. All the classification changes take effect.
   - If you need to modify policies before applying the changes, do not select anything in the window until the policies have been modified. Then return to this window and select **Apply**.
   - If there are a few changes that are not acceptable, you can write a few policies to fine tune the classification and work around these changes. Then return to this window and select **Apply**.
   - If there are changes that are not acceptable, select **Roll Back**, and then select the Device Profile Library version to revert to. All the pending changes are discarded.

4. To immediately apply classification changes following future Device Profile Library upgrades, select the **Always apply classification updates** checkbox. If you do not select the checkbox, you will be presented with pending classification changes whenever the Device Profile Library is upgraded.

Sharing 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 that will 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 *CounterACT Administration Guide*. See Additional CounterACT Documentation for information on how to access the guide.

Core Extensions Module Information

The Device Classification Engine is installed with the CounterACT Core Extensions Module.

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

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

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

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

Refer to the *CounterACT Core Extensions Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

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

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

Software downloads are also available from these portals.

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

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Portal

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

To access documentation on the ForeScout Customer Portal:

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

Documentation Portal

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

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

To access the Documentation Portal:

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

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

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

Plugin Help Files

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

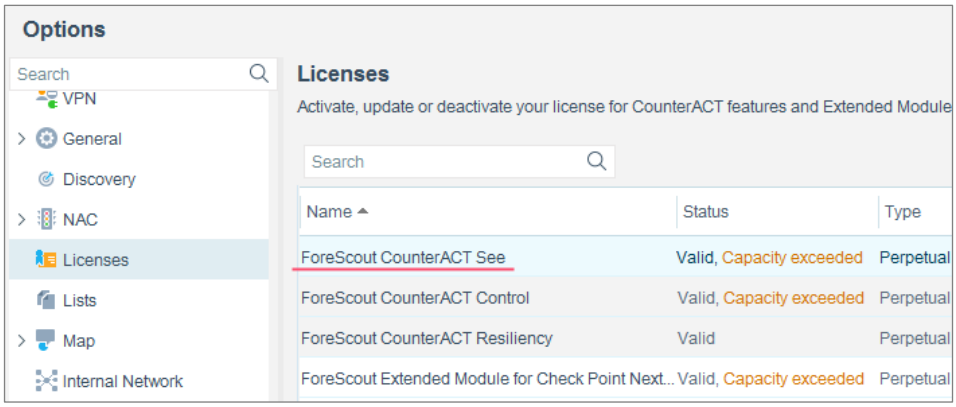
Documentation Portal

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

Identifying Your Licensing Mode in the Console

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

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



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

Legal Notice

2018-04-10 09:21