ForeScout®

CounterACT® Device Classification Engine

Configuration Guide

Version 1.0.0

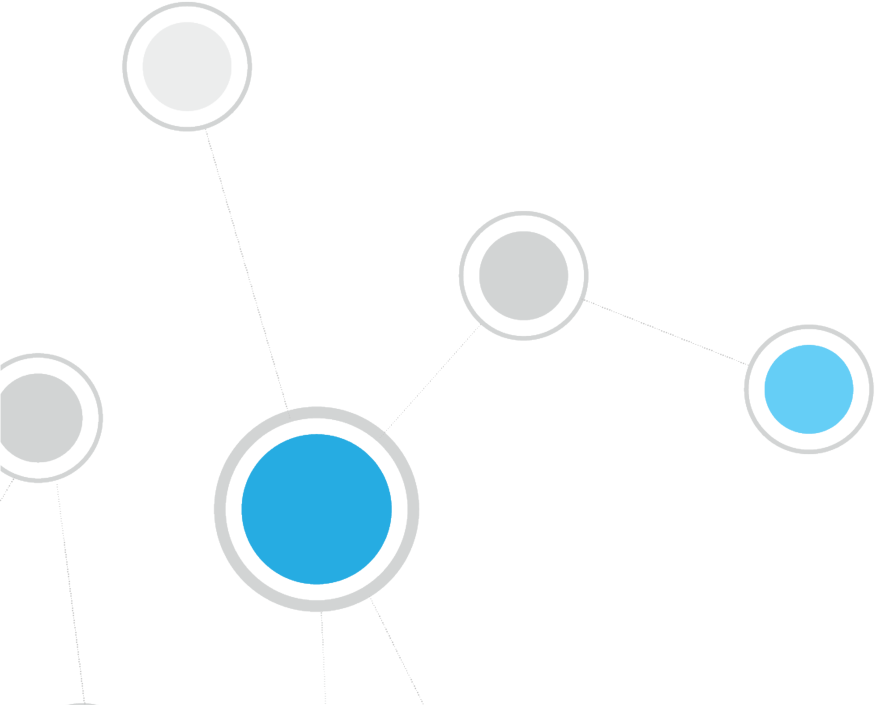


Table of Contents

About the Device Classification Engine

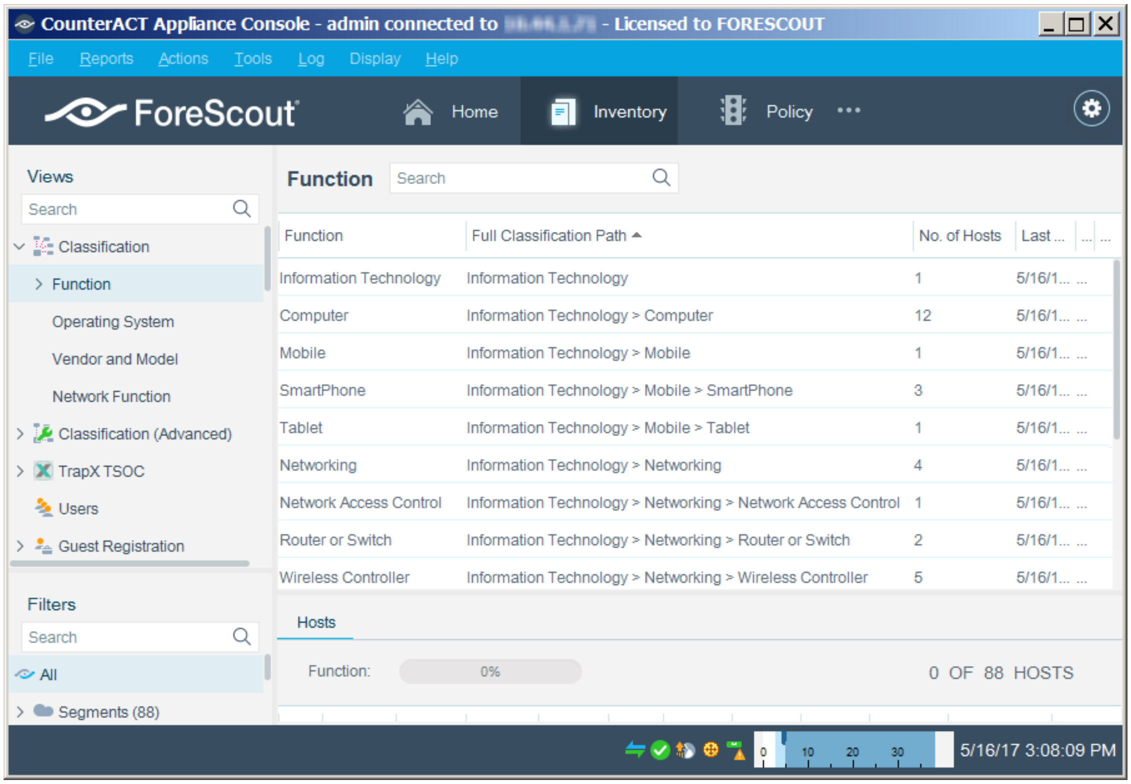
The Device Classification Engine is a core feature of CounterACT that resolves classification-related properties for comprehensive classification of each endpoint.

The key benefits of the Device Classification Engine are:

- 'Out 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.
- Going forward, content updates will allow rapid growth both to new verticals and to deeper granularity in classification.

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 Inventory view.

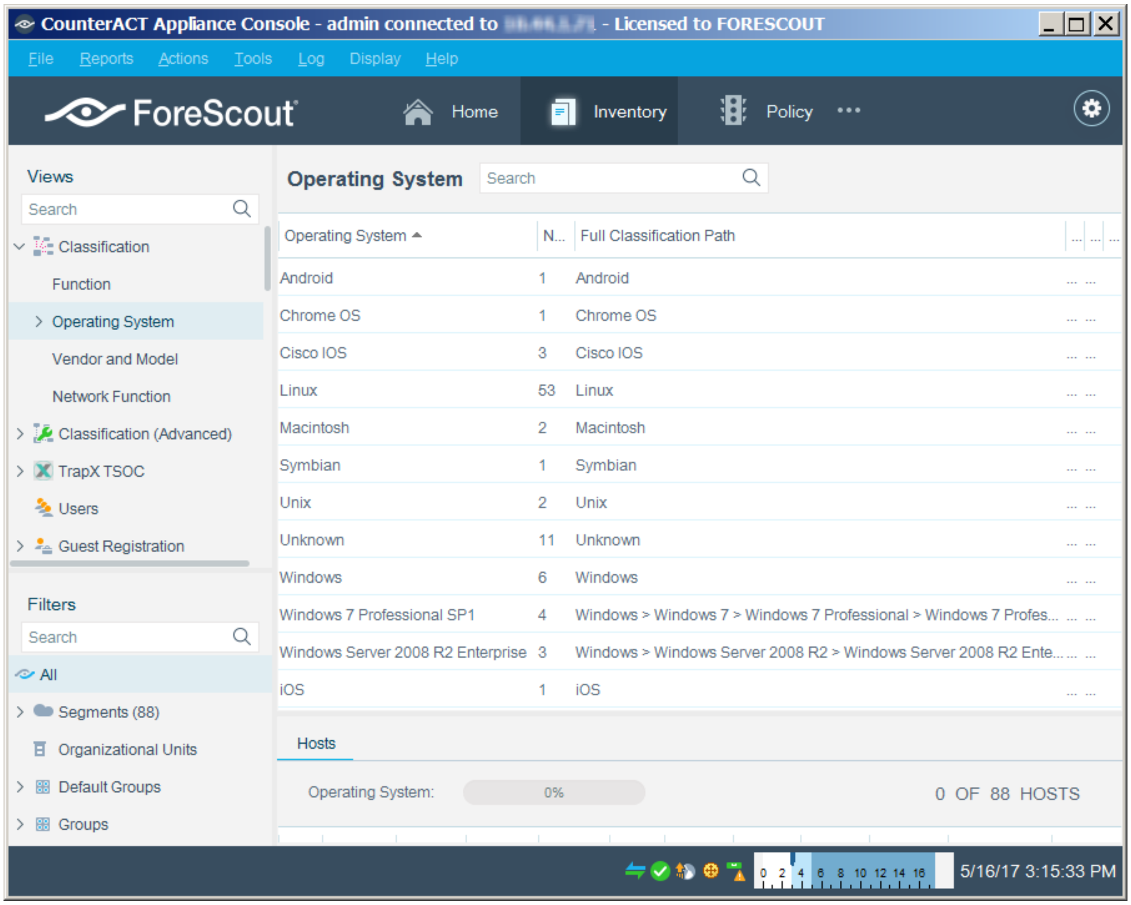


CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT

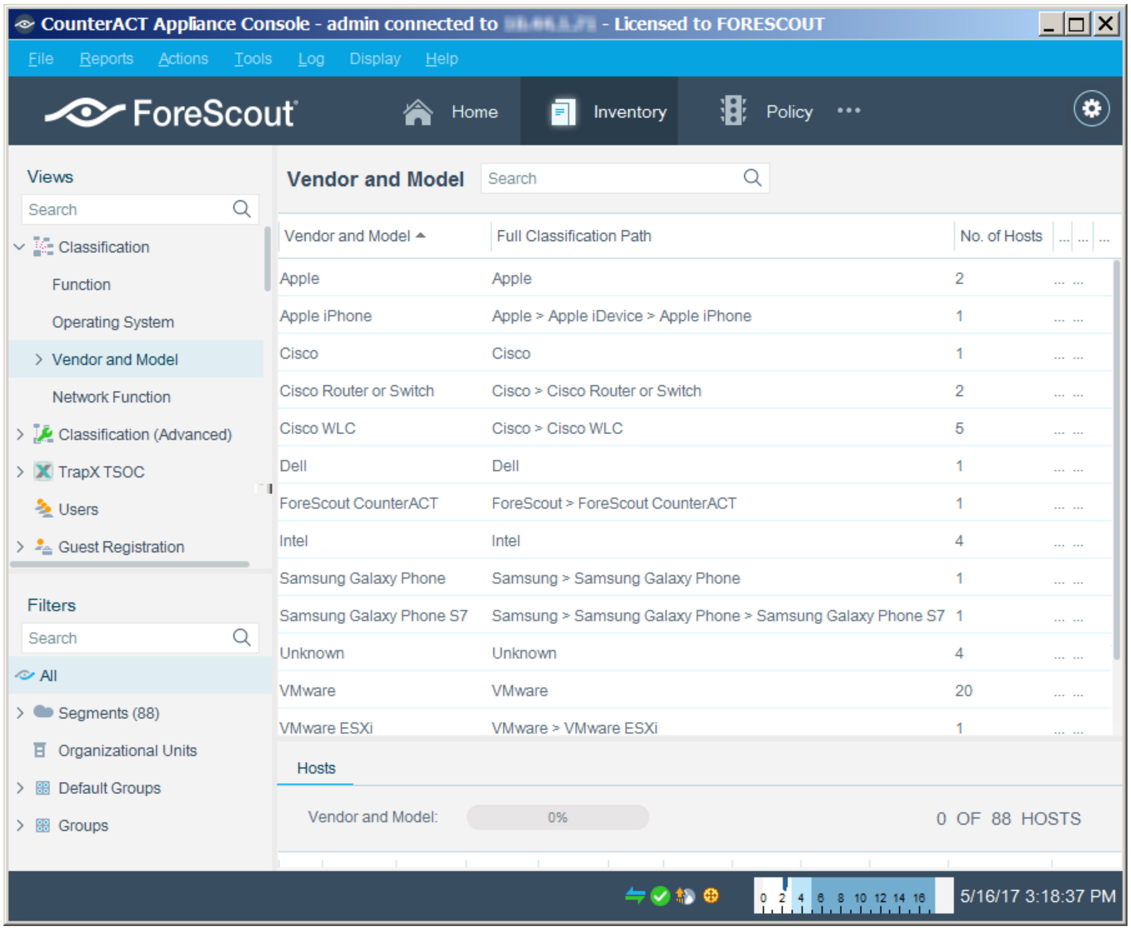
Function	Full Classification Path	No. of Hosts	Last ...	...	...
Information Technology	Information Technology	1	5/16/1...	...	
Computer	Information Technology > Computer	12	5/16/1...	...	
Mobile	Information Technology > Mobile	1	5/16/1...	...	
SmartPhone	Information Technology > Mobile > SmartPhone	3	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



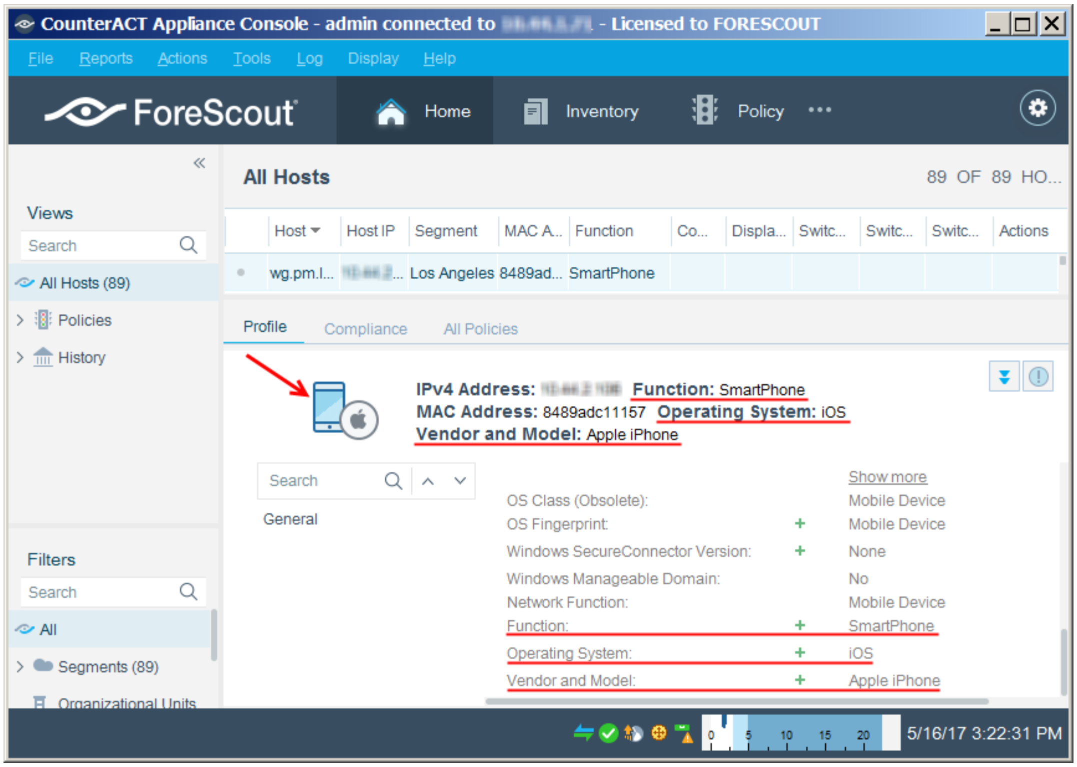
Operating System	N...	Full Classification Path
Android	1	Android
Chrome OS	1	Chrome OS
Cisco IOS	3	Cisco IOS
Linux	53	Linux
Macintosh	2	Macintosh
Symbian	1	Symbian
Unix	2	Unix
Unknown	11	Unknown
Windows	6	Windows
Windows 7 Professional SP1	4	Windows > Windows 7 > Windows 7 Professional > Windows 7 Profes...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



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	...	...

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.



All Hosts 89 OF 89 HO...

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.

If you find that the *Primary Classification* policy provides more comprehensive classification in your environment than the *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 Console User Manual.

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. See the *CounterACT Device Profile Library Configuration Guide*.
5. Install the Device Classification Engine whenever a new version is available.

🗎 *To help ForeScout provide better classification and posture assessment services, you can 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 classification, to be used by ForeScout researchers to improve the product. Refer to* The ForeScout Research and Intelligent Analytics Program *section in the CounterACT Console User Manual for more information about this program.*

CounterACT Software Requirements

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

- CounterACT version 7.0.0
- Service Pack 3.0.0 or above, which includes Device Profile Library version 2.0.0 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.

  🗎 *The Device Profile Library content is updated periodically to improve the quality and breadth of profiles so that more devices types can be classified accurately. It is recommended to install the latest version of the Device Profile Library to take advantage of the most current classifications.*

  This release of the Device Classification Engine is bundled with CounterACT 7.0.0 Service Pack 3.0.0, and is automatically installed with the service pack. To manually install it, see Install the Device Classification Engine.
- An active Maintenance Contract for CounterACT devices

Install the Device Classification Engine

This release is bundled with CounterACT 7.0.0 Service Pack 3.0.0, and is automatically installed with the service pack.

You can also manually install the Device Classification Engine.

To install:

1. Acquire a copy of the component in either one of the following ways:
   – If you are installing a Beta release, acquire the **`.fpi`** file from your ForeScout representative or contact beta@forescout.com.
   – Navigate to the Customer Support, Base Plugins page and download the **`.fpi`** file.
2. Save the file to the machine where the CounterACT Console is installed.

3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved **`.fpi`** file.
7. Select **Install**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The component is listed in the Plugins pane.

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.

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 the Asset Classification policy.*

The policy resolves the following classification properties:

- Function
- Operating System
- Vendor and Model
- Suggested Function - indicates all the Function property values that matched an endpoint if there were multiple matches

- Suggested Operating System - indicates all the Operating System property values that matched an endpoint if there were multiple matches

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.

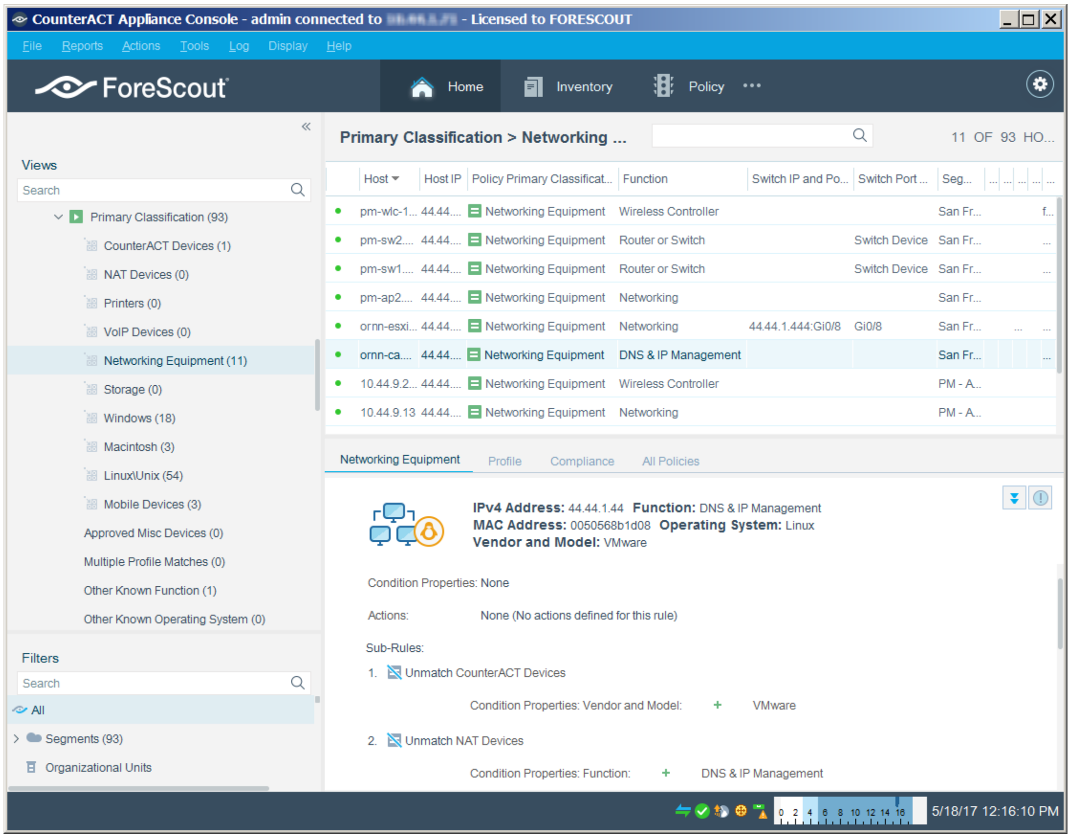
> *If there are endpoints in your network that are known to be sensitive to network probing, see Handling Sensitive Endpoints.*

For more information about the CounterACT Primary Classification policy template, refer to the *CounterACT Templates* and *Policy Management* chapters of the Console User Manual.

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.



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)

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

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

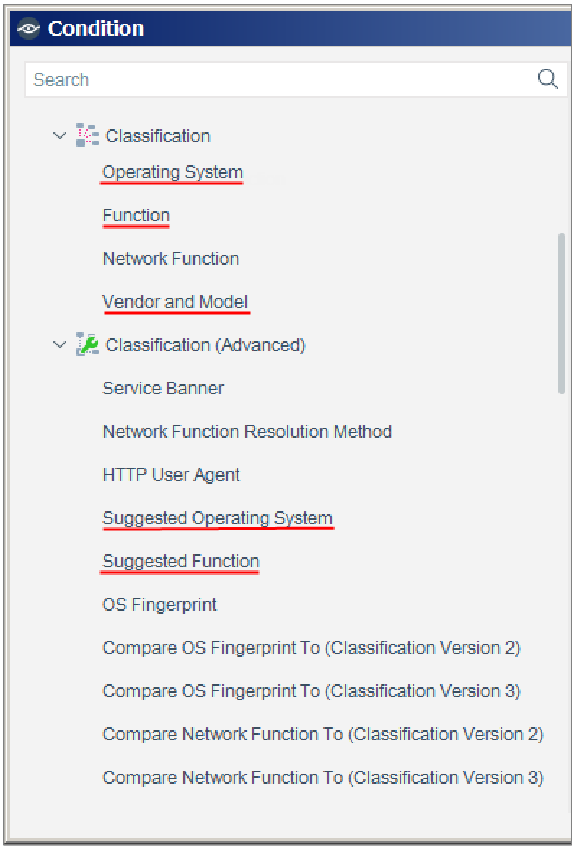
CounterACT uses both passive and active methods to classify endpoints. Active methods include probing the endpoint to check for a small range of open ports, running Nmap against the endpoint, and attempting to connect using WMI, SMB and/or RRP (depending on your HPS Inspection Engine configuration). 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 add the sensitive endpoints to the *Default Groups > Properties - Passive Learning* group.

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
HTTP User Agent
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)

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 two properties in the Classification (Advanced) condition node:

- Suggested Function
- Suggested Operating System

🗎 *If Classify Actions were used to override a classification property, the Suggested classification property contains the classification set by the Device Classification Engine.*

Suggested Function

The *Suggested Function* property indicates all the *Function* property values that matched this endpoint's profile but were considered less accurate than the resolved *Function* property value, possibly due to conflicting choices.

Suggested Operating System

The *Suggested Operating System* property indicates all the *Operating System* property values that matched this endpoint's profile but were considered less accurate than the resolved *Operating System* property value, possibly due to conflicting choices.

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:

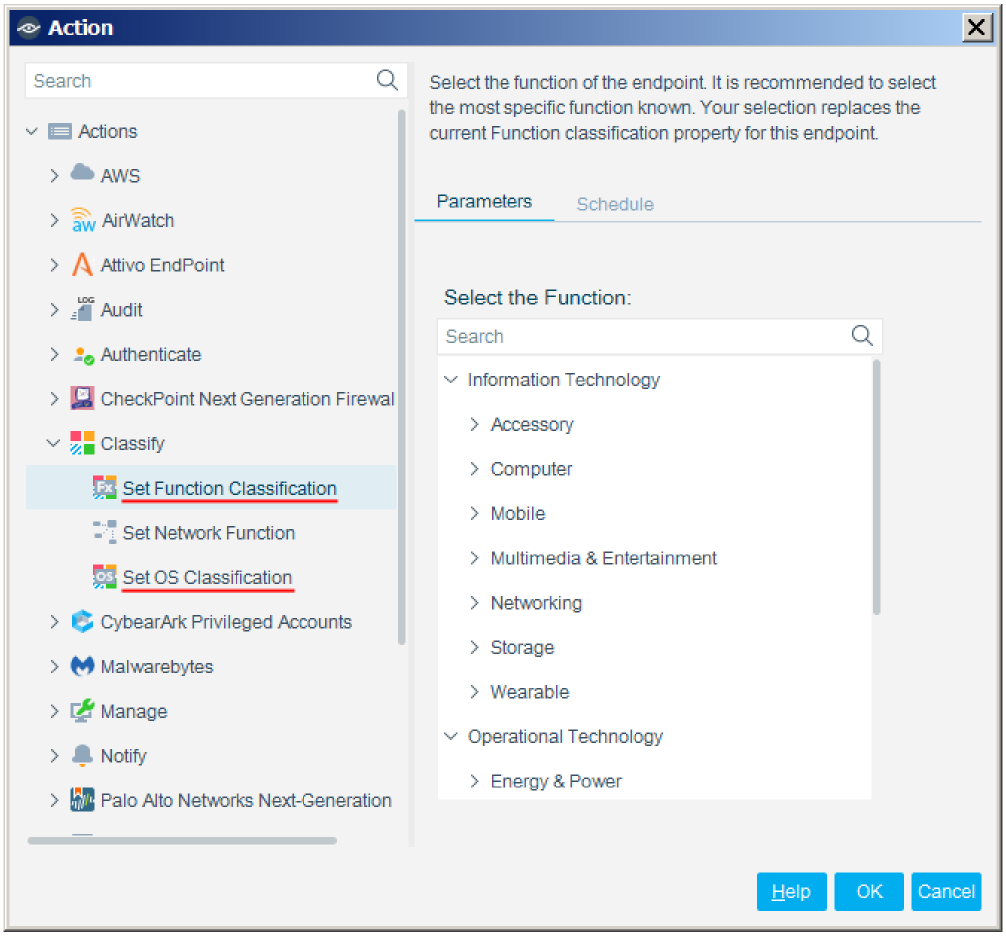
- The classification resolved by CounterACT is not correct or CounterACT was not able to classify an endpoint.
- You are able to refine the classification resolved by CounterACT. For example, CounterACT classified the device as Healthcare, but you know it’s actually an X-Ray device.

- 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. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the Classify folder in the Actions tree.
3. The following actions are available to override a classification property set by the Device Classification Engine:
   - 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.

To manually classify individual endpoints, right-click them and select the **Classify** option.

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

To cancel manual classification of individual endpoints:

1. In the Home tab, right-click the endpoint.
2. Select the **Cancel Actions** option.

Classification Property Fine Tuning

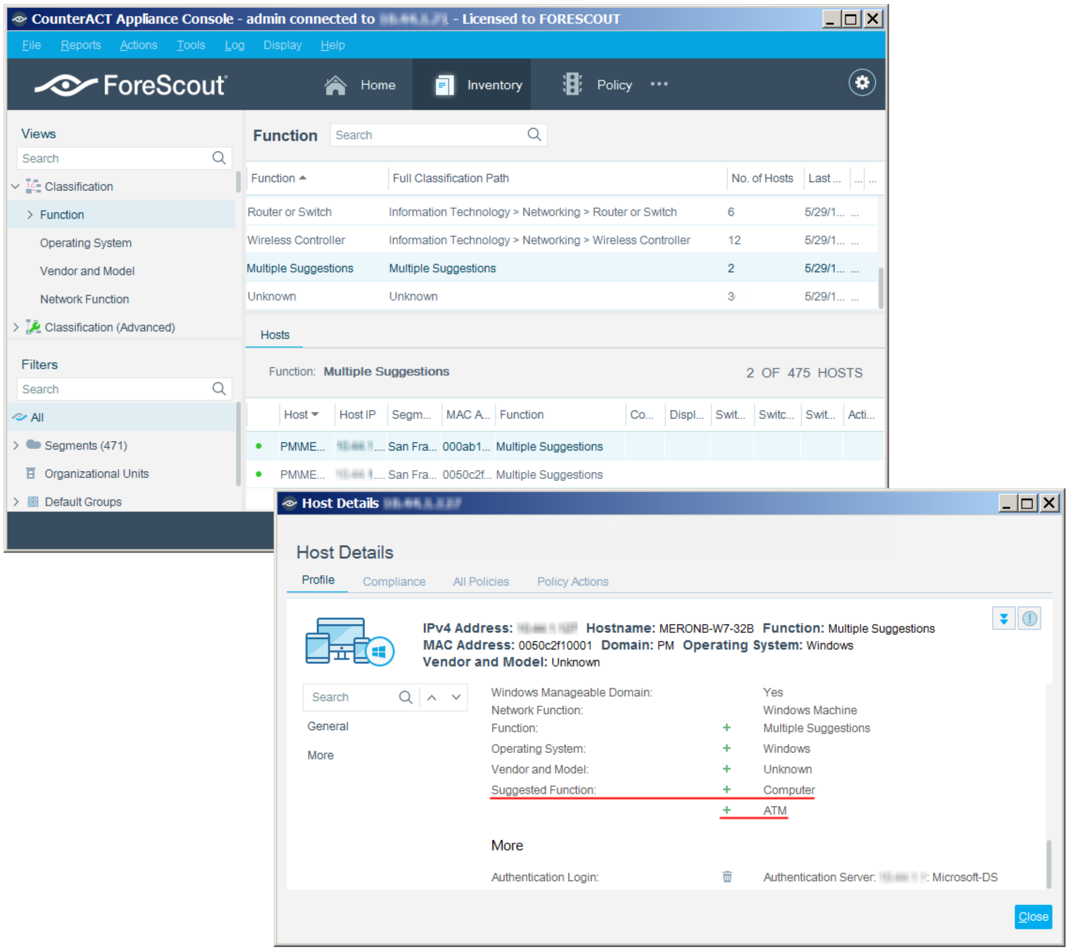
CounterACT classifies your endpoints with a high degree of accuracy. It is possible that some endpoints may not be classified as precisely as possible. It is recommended to fine-tune your policy's classification results.

To fine-tune the initial classification results:

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



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...	...	

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. 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.

Sharing Data with ForeScout

To help ForeScout provide better classification and posture assessment services, you can 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. For more information about this program, refer to *The ForeScout Research and Intelligent Analytics Program* section in the CounterACT Console User Manual.

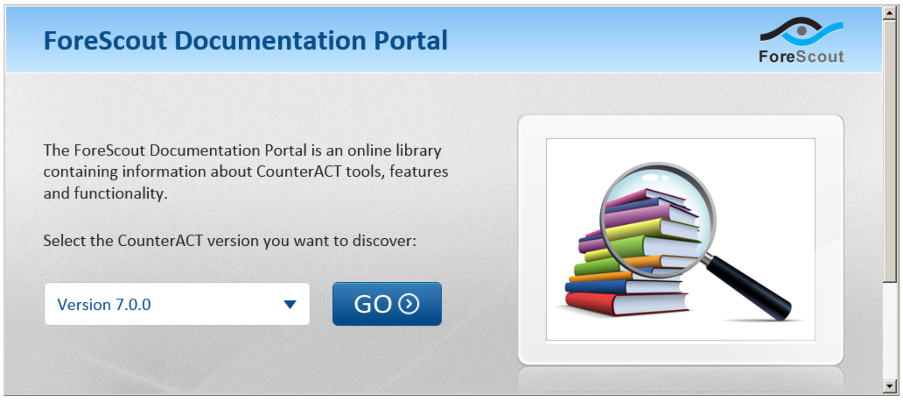
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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



ForeScout Documentation Portal

The ForeScout Documentation Portal is an online library containing information about CounterACT tools, features and functionality.

Select the CounterACT version you want to discover:

Version 7.0.0

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.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:

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

CounterACT Console Online 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.

Console User Manual

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 **Plugins**.
2. Select the plugin and then select **Help**.

Documentation Portal

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

Legal Notice

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-07-06 10:49