Device Classification Engine 1.0.0

CounterACT® Update

Release Notes

July 2017

Version Information

CounterACT Device Classification Engine version 1.0.0

Supported CounterACT Versions

Customers who are working with the following CounterACT version can install the component:

- 7.0.0

Requirements

- 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 component is bundled with CounterACT 7.0.0 Service Pack 3.0.0, and is automatically installed with the service pack. To manually install the component, see How to Install.

- An active Maintenance Contract for CounterACT devices

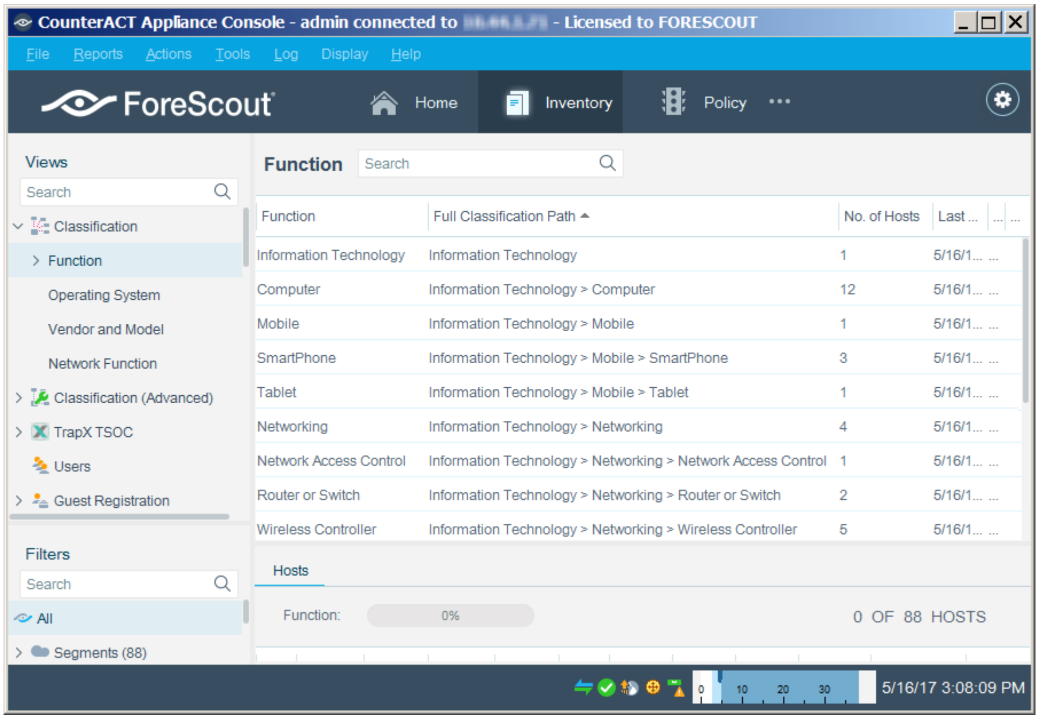
About the Device Classification Engine

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. 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, 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.

The key benefits of the new device classification feature 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. You can see each classification property with its tree taxonomy in the Inventory view when you expand the *Classification* node in the navigation pane.

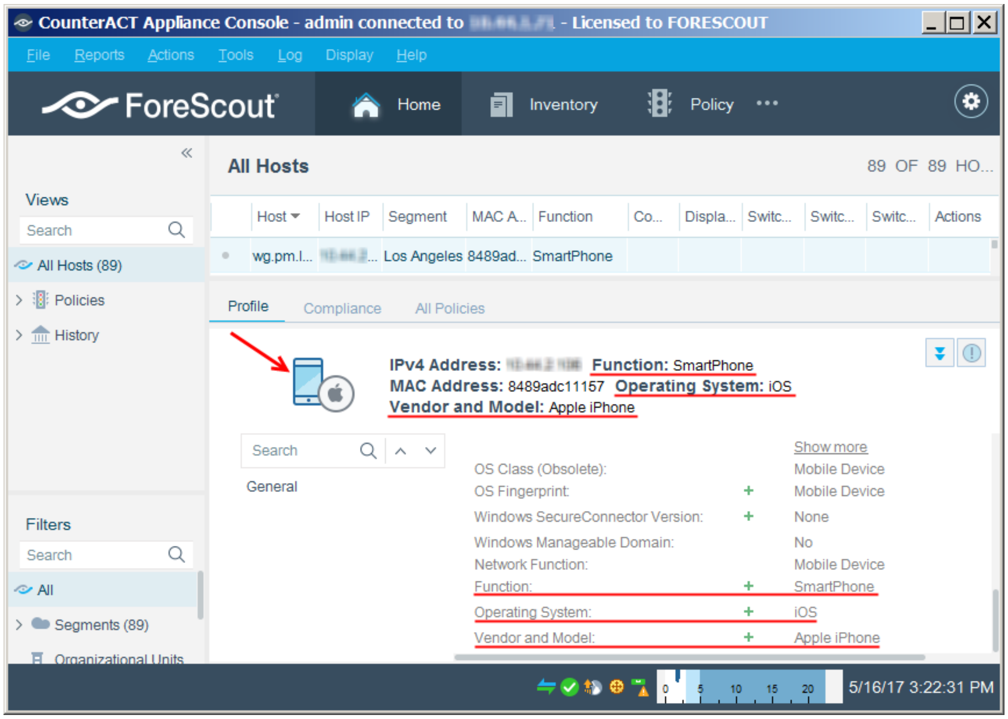

CounterACT Appliance Console - admin connected to [redacted] - Licensed to FORESCOUT

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

- High level of granular classification of function, operating system and vendor, which is not available using the Network Function property. You can see the device classification properties for each endpoint in the Home view.



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

- Broad and extensible Primary Classification policy template for device classification. 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.
- Going forward, content updates will allow rapid growth both to new verticals and to deeper granularity in classification.

How It Works

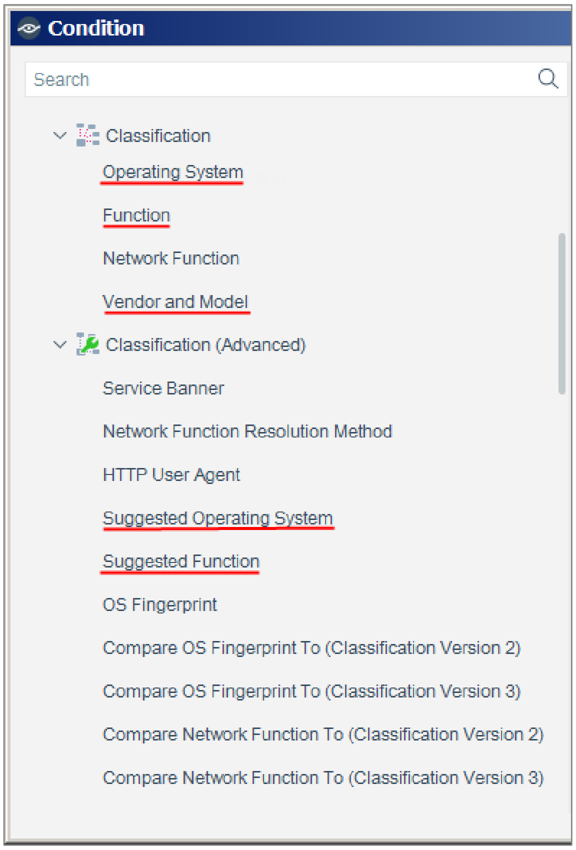
The Device Profile Library contains classification profiles, each of which is a combination of properties that match a specific device type. To classify an endpoint, the Device Classification Engine compares the properties of the endpoint with the profiles in the library to find the best match. The endpoint 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.

New Properties

After the Device Classification Engine is installed, new classification-related properties are available for each detected endpoint.


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 new properties in the Classification condition node.

- The *Function* property indicates the most detailed device function that can be resolved, such as:
  – Information Technology > Accessory > Printer

  - Operational Technology > Healthcare > Patient Monitor
  - Operational Technology > Non-Industry Specific > Facilities > Physical Security > Surveillance > IP Camera

- The *Operating System* property indicates the most detailed operating system information that can be resolved, such as:
  - Windows > Windows Server 2012 > Windows Server 2012 Essentials
  - Macintosh > OS X 10.8 - MountainLion
  - Chrome OS
- The *Vendor and Model* property indicates the vendor, and also the model if known, such as:
  - 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

Unmatched Endpoints

For each of the three properties, the following describes what happens when the Classification Engine cannot match definitively the endpoint to a specific 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.
- If no profiles in the Device Profile Library match the endpoint, the property is resolved as *Unknown*.

Classification (Advanced) Properties

The Device Classification Engine resolves two new properties in the Classification (Advanced) condition node.

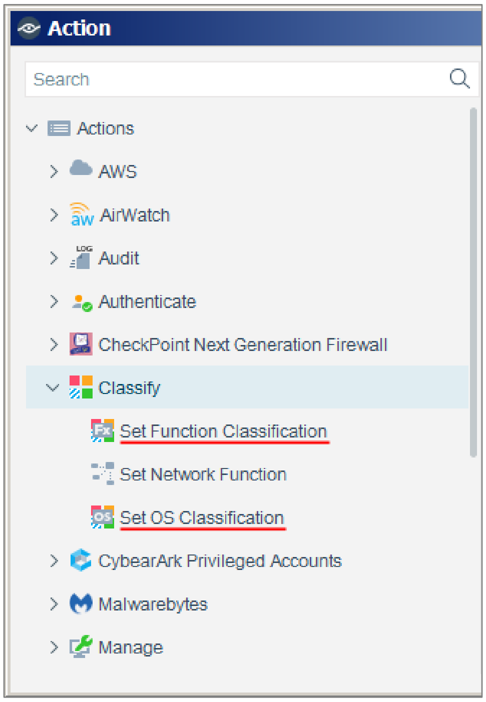
- The *Suggested Function* property indicates all the *Function* property values that matched this endpoint's profile but were considered less accurate than the resolved *Function* property value, possibly due to conflicting choices.
- The *Suggested Operating System* property indicates all the *Operating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

A *Suggested* property is empty if there is a single definite match for its corresponding classification. If Classify Actions were used to override a classification property, the Suggested classification property contains the classification set by the Device Classification Engine.

New Actions

After the Device Classification Engine is installed, the following actions are available to override a classification property set by the Device Classification Engine:

- Set Function Classification
- Set OS Classification



New 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.

A policy created by the Primary Classification template resolves the following classification properties:

- Function
- Operating System
- Vendor and Model
- Suggested Function
- Suggested Operating System

The policy includes sub-rules for devices found in most environments. It is recommended to enhance the policy by adding additional sub-rules above the *Approved Misc Devices* sub-rule for devices that are particular to your environment.

Replacing Your Asset Classification Policy with a Primary Classification Policy

The advantages of the Primary Classification policy over the Asset Classification is policy are:

- The Primary Classification policy categorizes endpoints into more sub-rules, offering a finer grained classification.
- The Primary Classification policy gives you insight into detailed classification via the new properties.

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, so that when these actions are enabled, your other policies will not be affected when the Asset Classification policy is stopped. For more information about the policy templates, refer to the *CounterACT Templates* and *Policy Management* chapters of the Console User Manual.

Known Issues

This section describes all known issues for this release.

Issue	Description
DCE-97	The Classification Engine can only classify endpoints with IP addresses.

How to Install

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.

More Information

Refer to the configuration guide for more information about the Device Classification Engine.

To access the configuration guide:

1. After the component is installed, select **Options** from the Console **Tools** menu.
2. Navigate to and select the **Plugins** folder. The Plugins pane opens.
3. Select the component from the Plugins pane and then select **Help**.

Currently Available Releases

You can view information about Device Classification Engine releases supported by specific CounterACT versions. To view, click the following link:

https://updates.forescout.com/support/files/plugins/classification/Updates.pdf

New features or fixes may be provided after this release. These items will be made available as releases to the upcoming version until the final version is posted on the ForeScout Customer Support page.