ForeScout CounterACT®

Device Profile Library

Configuration Guide

Updated February 2018

Table of Contents

About the Device Profile Library

The Device Profile Library 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. Each profile maps to a combination of values for function, operating system, and/or vendor & model. 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 CounterACT Device Classification Engine classifies any endpoint with property values matching those specified in the *Apple iPad* classification profile as:

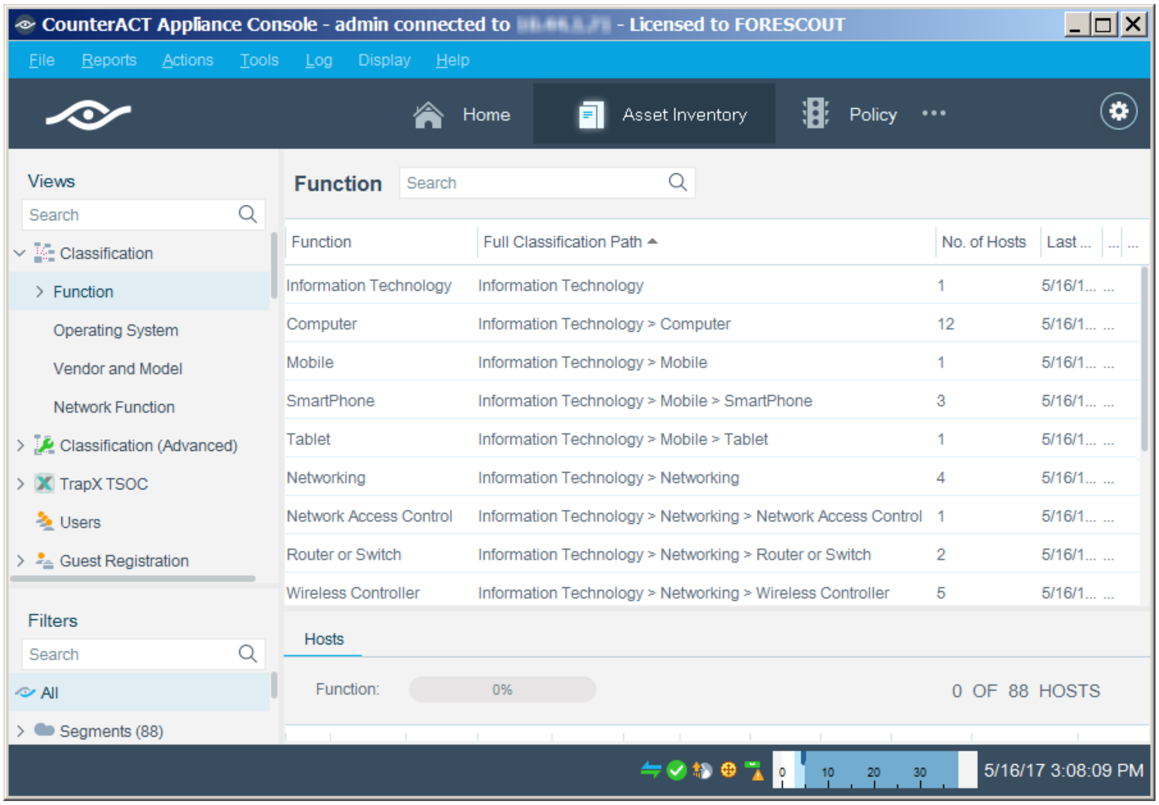
- *Function*: Information Technology > Mobile > Tablet
- *Operating System*: iOS
- *Vendor and Model*: Apple > Apple iDevice > Apple iPad

The classification values form a tree-structured taxonomy which ultimately describes what the endpoint is. The CounterACT Device Classification Engine uses these classification profiles to classify devices that are detected in your network.

The classification profile content is updated periodically to improve the quality and breadth of profiles so that more devices types can be classified even more precisely. It is recommended to install the latest version of the content module containing the Device Profile Library to take advantage of the most current classifications.

How It Works

The Device Classification Engine uses information provided by the Device Profile Library to provide the best possible classification for the device based on the properties available to CounterACT. Refer to the *CounterACT Device Classification Engine Configuration Guide*. See Additional CounterACT Documentation for information about how to access the guide.



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

Each detected endpoint may be classified according to three different metrics:

- Function
- Operating System
- Vendor and Model

The taxonomy of each classification metric is based on a tree structure. Each level in the tree is more specific than the level above it. Endpoints are classified to the most specific value that CounterACT can resolve.

Function

The Device Profile Library provides for over 95 possible *Function* classifications. The high level structure is:

- Information Technology
  - Accessory
  - Appliance
  - Computer
  - Mobile
  - Multimedia & Entertainment
  - Networking
  - Storage
  - Wearable

- Operational Technology
  - Energy & Power
  - Gaming
  - Healthcare
  - Metal & Allied
  - Mining
  - Non-Industry Specific
  - Retail & Financial
  - Traffic & Parking Management

Lower level branches provide more specific classification. For example, Operational Technology > Non-Industry Specific > Facilities > Physical Security > Surveillance > IP Camera.

Operating System

The Device Profile Library provides for over 170 possible *Operating System* classifications. The high level structure is:

- Android
- ArubaOS
- Blackberry
- Chrome OS
- Cisco IOS
- FortiOS
- iOS
- Linux
- Macintosh
- NetBSD
- Palm OS
- PAN-OS
- Symbian
- Unix
- VxWorks
- Windows
- None, for embedded devices that do not run an operating system

For many common operating systems, lower level branches resolve more specific versions and flavors. For example, Windows > Windows Server 2008 R2 > Windows Server 2008 R2 Datacenter.

Vendor and Model

The *Vendor and Model* taxonomy includes hundreds of select major vendors, especially of IoT devices, such as wearables and mobiles, and industry specific operational technology, such as operational technology, including industrial control systems and industry specific devices. Lower level branches include the model if known. For example, Apple > Apple iDevice > Apple iPhone. Over 800 vendors and device models can be classified according to this taxonomy.

CounterACT Software Requirements

The module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0
- An active Maintenance Contract for CounterACT devices

For optimal endpoint classification, it is recommended to install the highest available versions of the following CounterACT components, and ensure they are running:

- Core Extensions Module version 1.0, including the following plugins:
  - DHCP Classifier Plugin
  - Device Classification Engine
- Windows Applications Content Module version 2.1.4
- Endpoint Module version 1.0, including the following plugins:
  - HPS Inspection Engine
  - Linux Plugin, if there are Linux endpoints in your environment
  - OS X Plugin, if there are macOS/OS X endpoints in your environment
- NIC Vendor DB Content Module version 1.2.3
- Network Module version 1.0, including the Switch Plugin

Install the Module

The content module containing the Device Profile Library is included in the CounterACT version 8.0 installation. It is recommended to install the latest available version of the module to take advantage of the most current classifications.

After a new version of the 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 them, or cancel the changes and roll back to a previous Device Profile Library version. For details, refer to the *Device Classification Engine Configuration Guide*. See Additional CounterACT Documentation for information about how to access the guide.

To install the module:

1. Navigate to one of the following ForeScout portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module **`.fpi`** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **`.fpi`** file.
8. Select **Install**. The Installation wizard opens.
9. Select **I agree to the License Agreement**, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

Make sure you have selected the correct module to install. The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.

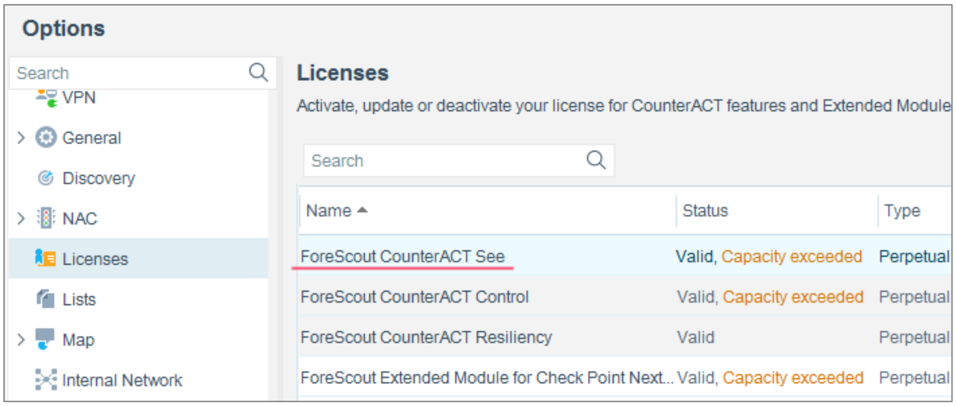
In modules that contain more than one component, the installation proceeds automatically one component at a time.

10. When the installation completes, select **Close** to close the wizard. The installed module is displayed in the Modules pane.

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.



Activate, update or deactivate your license for CounterACT features and Extended Module

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

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

Configure the Component

This component does not require any configuration. Endpoints are classified only after the Function, Operating System, or Vendor and Model classification properties are used in a policy. It is recommended to use the *Primary Classification* policy template to fully leverage the Device Classification Engine technology.

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**.

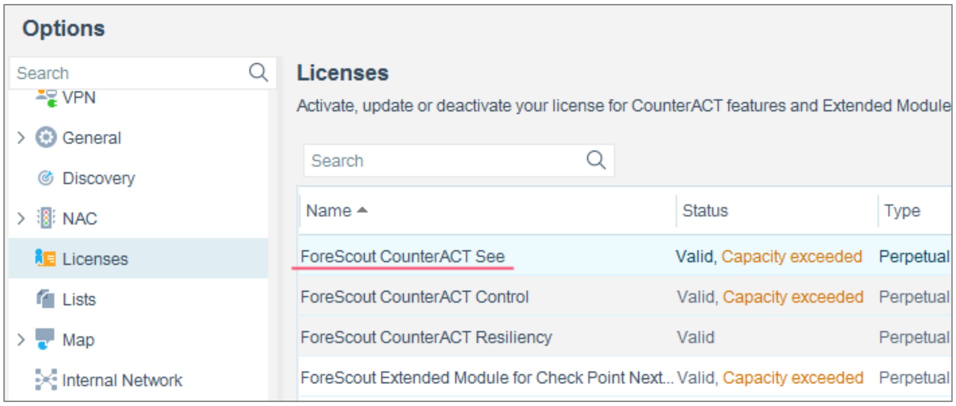
Documentation Portal

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.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

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

Legal Notice

2018-04-10 09:21