ForeScout

CounterACT® Device Profile Library

Configuration Guide

Version 2.0.0 and Above

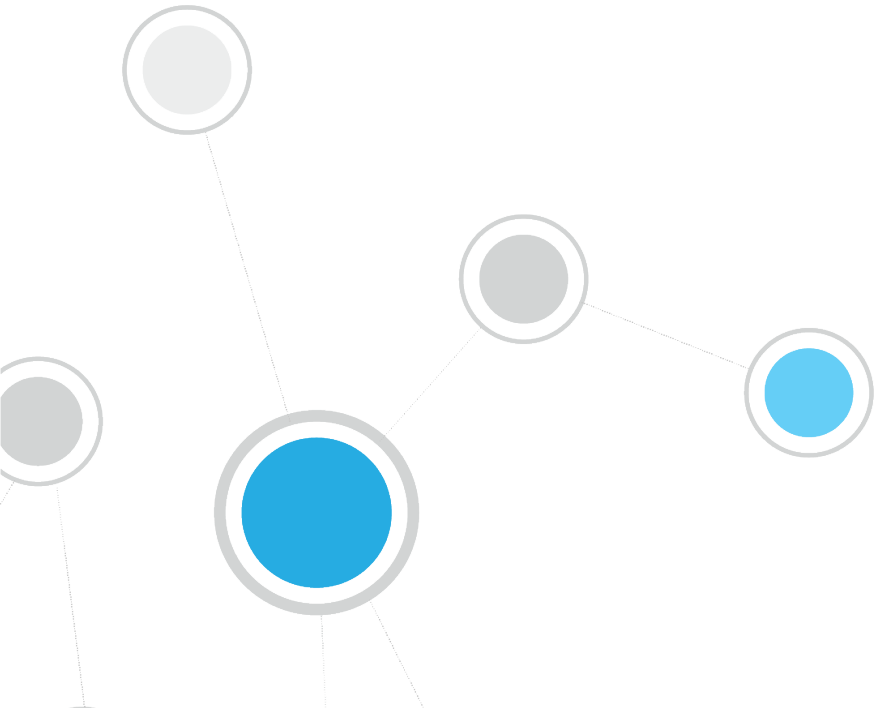


Table of Contents

About the Device Profile Library

The CounterACT Device Profile Library is 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:

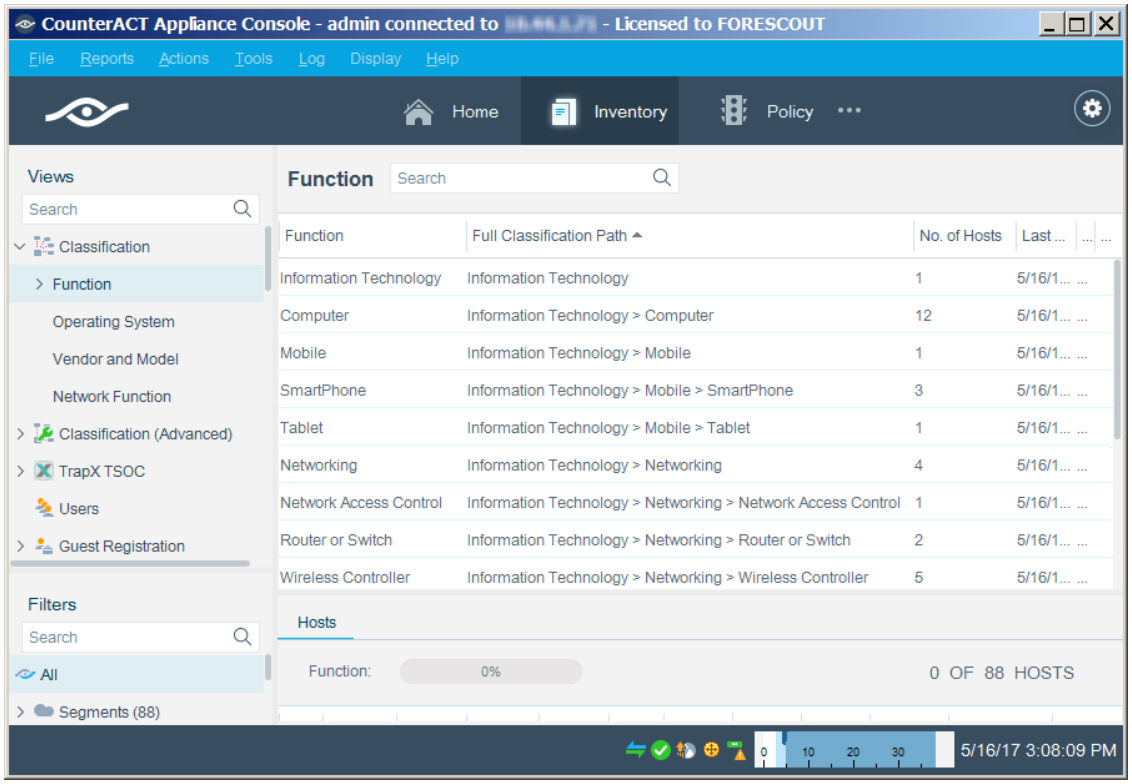
- *Function*: Information Technology > Mobile > Tablet
- *Operating System*: iOS
- *Vendor and Model*: Apple > Apple iDevice > Apple iPad

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 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. See the *CounterACT Device Classification Engine Configuration Guide*.



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 profile that CounterACT can resolve.

Function

The Device Profile Library provides for over 80 possible *Function* classifications. The high level structure is:

- Information Technology
  - Accessory
  - 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
- Blackberry
- Chrome OS
- Cisco IOS
- FortiOS
- iOS
- Linux
- Macintosh
- NetBSD
- Palm OS
- Symbian
- Unix
- Windows

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 medical equipment. 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

This component requires the following CounterACT releases and other CounterACT components:

- CounterACT version 7.0.0
- An active Maintenance Contract for CounterACT devices
- Service Pack 3.0.0 or above, which includes Device Classification Engine version 1.0.0 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.

  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 Install the Component.

For optimal endpoint classification, it is recommended to install the highest available versions of the following CounterACT components:

- DHCP Classifier Plugin version 2.0.5 or above
- HPS Applications Plugin version 2.1.3.1 or above
- HPS Inspection Engine version 10.7.0 or above
- HPS NIC Vendor DB version 1.2.1 or above
- Macintosh/Linux Property Scanner version 7.0.1 or above
- Switch Plugin version 8.9.3 or above
- If there are managed Linux endpoints in your environment, then Linux Plugin version 1.1.0 or above
- If there are managed macOS/OS X endpoints in your environment, then OS X Plugin 2.0.0 or above

Install the Component

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

You can manually install the component.

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 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.

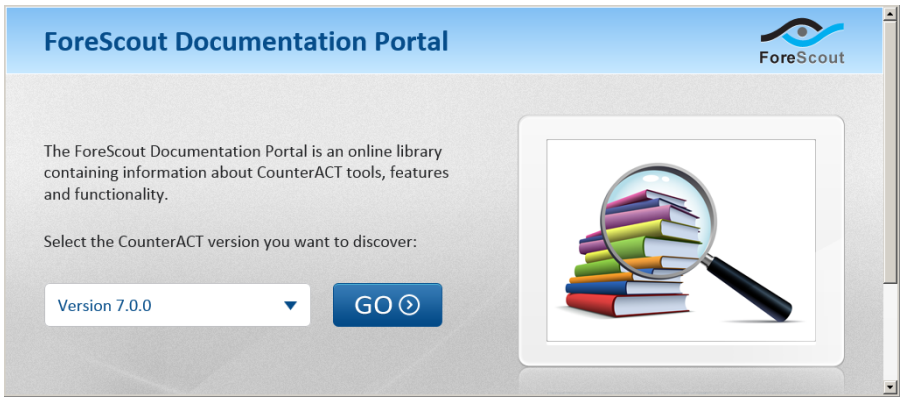
Additional CounterACT Documentation

For 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.



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

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

2017-07-06 13:57