FORESCOUT

Forescout

Device Profile Library

Configuration Guide

Version 20.0.2

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2020-02-17 13:36

Table of Contents

About the Device Profile Library

The Forescout 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 and 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 Forescout Device Classification Engine (a component of the Forescout Core Extensions Module) classifies any endpoint with property values matching those specified in the *Apple iPad* classification profile as:

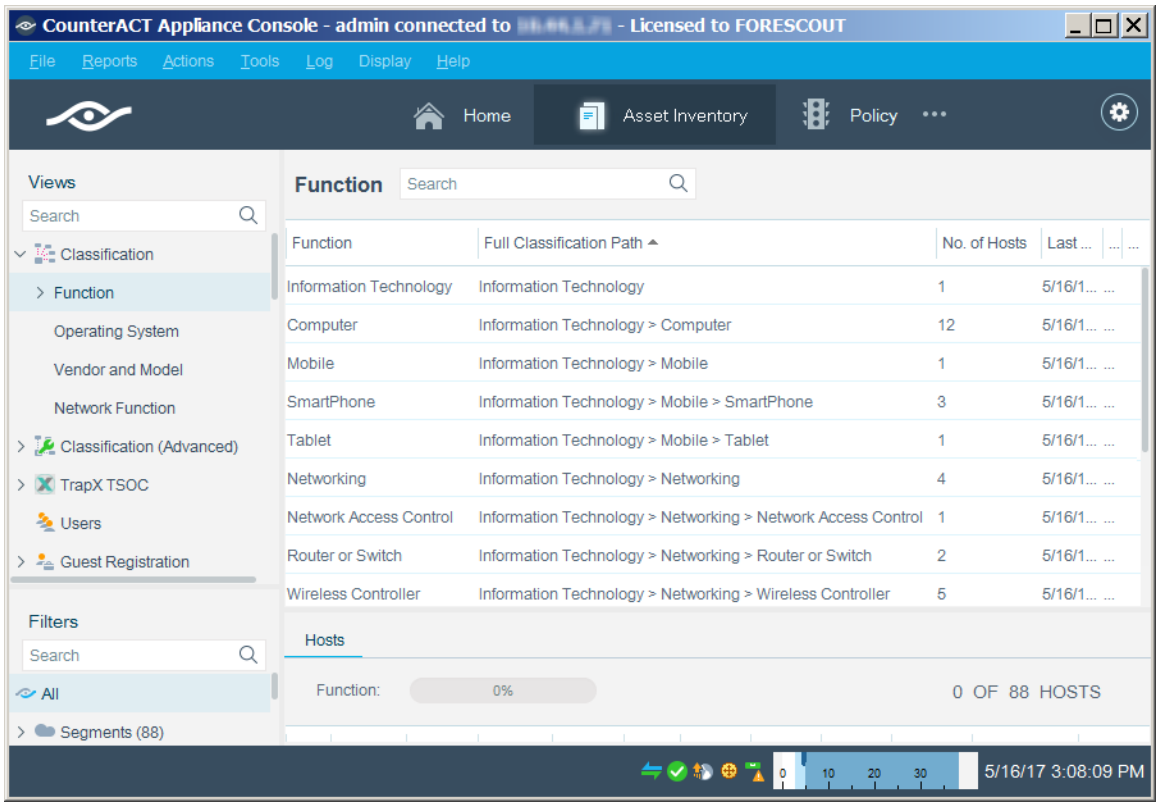
- *Function*: Information Technology > Mobile > Tablet
- *Operating System*: iOS
- *Vendor and Model*: Apple > Apple iDevice > Apple iPad

The classification values form a tree-structured taxonomy that ultimately describes what the endpoint is. The 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 Forescout eyeSight. Refer to the *Forescout Core Extensions Module: Device Classification Engine Configuration Guide*. See Additional Forescout Documentation for information on how to access the 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 value that eyeSight can resolve.

Function

The Device Profile Library provides for over 185 possible *Function* classifications. The high-level structure is:

Information Technology

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

Operational Technology

- 3D Printer
- Automotive
- Barcode Scanner
- Coffee Maker
- Customer Self Service Kiosk
- Data Acquisition System
- Energy & Power
- Facility
- Gaming
- Healthcare
- Industrial Control System
- Manufacturing
  Metal & Allied
- Mining
- Process Instrumentation and Metrology
- Real Time Location System
- Remote Monitoring & Control
- Retail & Financial
- Scientific and Analytical Instrumentation
- Shooter Detection
- Tooling
- Traffic & Parking Management

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

Operating System

The Device Profile Library provides for over 590 possible *Operating System* classifications. The high-level structure is:

- Alcatel-Lucent AOS-W
- Android
- Android TV OS
- APC AOS
- Arista EOS
- Avaya NOS
- Blackberry
- BrightSign OS
- Brocade/BigIron
- Brocade/Brocade NOS
- Brocade/FastIron
- Brocade/NetIron
- Brocade/ServerIron
- Brocade/TurboIron
- CellOS
- Check Point IPSO
- Chrome OS
- Cisco/Cisco AireOS
- Cisco/Cisco ASA-OS
- Cisco/Cisco CatOS
- Cisco/Cisco IOS
- Cisco/Cisco IOS-XE
- Cisco/Cisco IOS-XR
- Cisco/Cisco NX-OS
- Cisco/Cisco SAN-OS
- Contiki OS
- Dell DNOS
- eCos
- Extreme/ExtremeXOS
- Embedded Firmware
- FortiOS
- Hirschmann HiOS
- HPE/ArubaOS
- HPE/Comware
- HPE/ProCurve
- Huawei VRP
- iOS
- Juniper/JunOS
- Juniper/ScreenOS
- LG webOS
- Linux
- Macintosh
- Microware OS-9
- My Cloud OS
- Nucleus RTOS
- Nut OS
- OpenVMS
- Orbis OS
- Palm OS
- PAN-OS
- QNX
- Roku OS
- ROS
- Symbian
- ThreadX RTOS
- tvOS
- Unix
- VxWorks
- watchOS
- 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
- 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 1585 vendors and device models can be classified according to this taxonomy.

Requirements

The module requires the following:

- CounterACT version 8.0.1

For optimal endpoint classification, it is recommended to install the **highest available versions** of the following Forescout components that are compatible with CounterACT 8.0.1, and ensure they are running:

- Core Extensions Module, including the following plugins:
  - DHCP Classifier Plugin
  - Device Classification Engine
- Windows Applications Content Module
- Endpoint Module, 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
- Network Module including the Switch Plugin

Install the Module

The Device Profile Library is included in the CounterACT version 8.0.1 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 *Forescout Core Extensions Module Device Classification Engine*

Configuration Guide. See Additional Forescout Documentation for information on how to access the guide.

To install the module:

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

   To identify your licensing mode, select **Help > About ForeScout CounterACT...** from 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 screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

   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 window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

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 Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources page provides links to the full range of technical documentation.

To access the Forescout Resources page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

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

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After installing the plugin, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).

Appendix A: Ports and Protocols

The following table lists all the destination ports that may be queried on endpoints during the classification process.

Port	Protocol	Device
21	TCP	Network Attached Storage Device
22	TCP	Network Attached Storage Device
80	TCP	Temperature Monitor
102	TCP	PLC Device
104	TCP	DICOM Server
111	TCP	Printer
161	UDP	Networking Device
161	UDP	Printer
443	TCP	Network Attached Storage Device
500	UDP	Medication Dispensing System
515	TCP	Printer
554	TCP	IP Camera
1720	TCP	VoIP Device
1732	UDP	Patient Monitor
1801	TCP	Medication Dispensing System
1950	TCP	Patient Monitor
2000	TCP	Patient Monitor
2000	TCP	Medical Cart
2050	TCP	Patient Monitor
2100	TCP	Patient Monitor
2150	TCP	Patient Monitor
2222	UDP	PLC Device
5247	UDP	Networking Device
5684	UDP	IKEA Gateway
8080	TCP	Network Attached Storage Device
9007	TCP	Printer
9100	TCP	Printer
24000	TCP	Philips Intellivue Device
24001	TCP	Philips Intellivue Device
24002	TCP	Philips Intellivue Device
24003	TCP	Philips Intellivue Device
24004	TCP	Philips Intellivue Device

Port	Protocol	Device
24005	TCP	Philips Intellivue Device
44818	TCP	PLC Device
51243	TCP	Infusion Pump
53213	UDP	Printer
62078	TCP	Mobile Device