



Fore Scout

Network Function Property Algorithm

Technical Note

Fore Scout version 8.1



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

Legal Notice

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

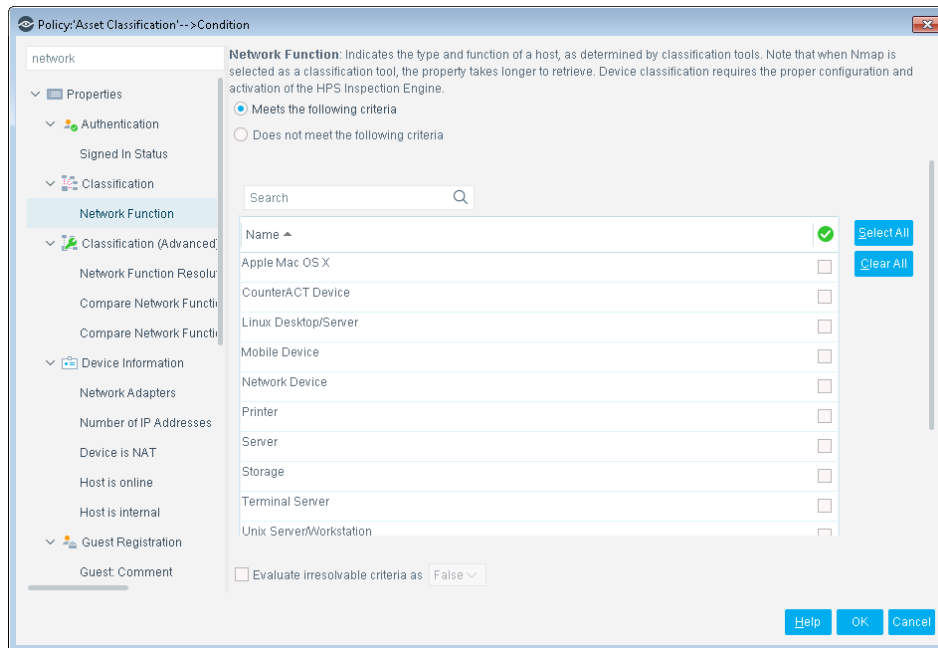
2019-03-20 14:43

Table of Contents

About the Network Function Property	4
Network Function Algorithm Criteria	5
1. Manual Classification	5
2. Managed CounterACT Appliance	5
3. Managed Endpoint	5
4. Switch Plugin	6
5. VPN Plugin	6
6. Wireless Plugin	6
7. Switch CDP	6
8. VoIP Connected to Managed Switch	6
9. Trusted Vendor MAC	6
10. DHCP Classification	6
11. Passive Detection of HTTP User Agent	6
12. Samba Traffic	7
13. HTTP User Agent on Forescout Web Server	7
14. Passive Fingerprinting	7
15. Nmap Active Banner Scan	7
16. Nmap Active OS Scan	7
Property Resolution Method	7
Additional Forescout Documentation	8
Documentation Downloads	9
Documentation Portal	9
Forescout Help Tools	10

About the Network Function Property

The Network Function host property is used in ForeScout® policies to detect endpoint network function values, for example, Windows machines, mobile devices or network printers. This property can be used to help you continuously track and control your network assets.



The following property values may be resolved:

- Windows Machine
- Unix Server/Workstation
- Server
- Printer
- Mobile Device
- VoIP Device
- Linux Desktop/Server
- Apple Mac OS X
- Terminal Server
- Storage
- CounterACT Device
- Network Devices, switches, routers and storage devices

If a device does not meet the criteria for any of the above values it is resolved as *irresolvable*.

Network Function Algorithm Criteria

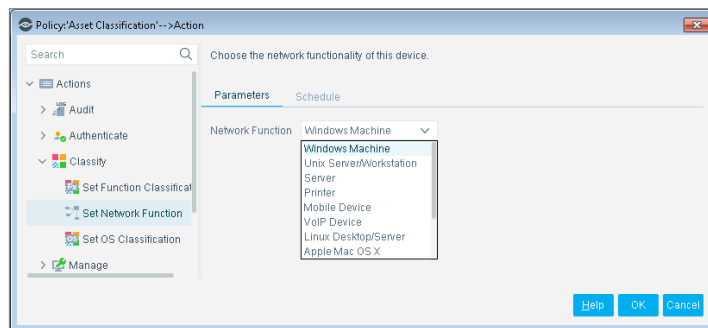
Network Function property resolution is based on a hierarchal algorithm. The algorithm applies a series of inspection criteria on each endpoint. If the endpoint does not match the first criterion, the next possible criterion is inspected.

The Network Function is resolved when the first matching item in the list of criteria matches a value discovered on the endpoint. For example, manually classifying an endpoint as a *Windows Machine* will override any property resolution determined using the algorithm.

This section lists the hierarchy of the criteria applied and describes each criterion.

1. Manual Classification

Derived from the *Classify > Set Network Function* action in the Forescout Console.



2. Managed CounterACT Appliance

The Enterprise Manager resolves itself as a managed CounterACT Appliance, as well as any Appliances it manages. Standalone Appliances resolve themselves as managed CounterACT Appliances as well.

3. Managed Endpoint

Derived from the Forescout platform managing an endpoint.

- a. Managed by HPS using RI (Windows Machine)
- b. Managed by HPS using SC (Windows Machine)
- c. Managed by HPS Windows CE Agent (Mobile Device)
- d. Managed by Mac/Linux Plugin Remote Inspection SSH (Linux Desktop/Server | Unix Server/Workstation | Apple Mac OS X)
- e. Managed by Mac/Linux Plugin SecureConnector (Linux Desktop/Server | Unix Server/Workstation | Apple Mac OS X)
- f. Managed by Android Plugin SecureConnector (Mobile Device)
- g. Managed by Fiberlink Plugin (Mobile Device)
- h. Managed by iOS Plugin (Mobile Device)
- i. Managed by Other MDM Plugin (Mobile Device)

4. Switch Plugin

Any devices managed by the Switch Plugin are resolved as *Network Device*.

5. VPN Plugin

Any devices managed by the VPN Plugin are resolved as *Network Device*.

6. Wireless Plugin

Any devices managed by the Wireless Plugin are resolved as a *Network Device*.

7. Switch CDP

The Switch Plugin may report information about devices learned via CDP from managed switches. This information can be used to determine the network function of those devices.

8. VoIP Connected to Managed Switch

A device managed by the Switch Plugin determines that an attached endpoint is resolved as a *VoIP Device*.

9. Trusted Vendor MAC

The Forescout platform determines the NIC vendor based on the IEEE list of MAC address prefixes. The Forescout platform has a list of reliable vendor name matches which it will match against. Currently, this list matches against certain MAC ranges assigned to HTC and RIM only, and resolves such endpoints as *Mobile Device*.

In addition to the predefined matching performed by the Forescout platform, in cases where other network devices can be resolved based on a known NIC vendor or MAC prefix, this raw data can be used in custom policies to classify devices.

10. DHCP Classification

Resolved by using passive fingerprinting of DHCP traffic. This relies on the OS type calculated by the DHCP Classifier Plugin based on the DHCP traffic it sees.

In addition to the predefined matching performed by the Forescout platform, in cases where other network devices can be resolved based on DHCP traffic information, the raw data (such as options and request fingerprints) can be used in custom policies to classify devices.

11. Passive Detection of HTTP User Agent

The Packet Engine listens to HTTP traffic and notes the user agent header in HTTP requests. Based on defined translation rules, the user agent is used to resolve the value of the network function.

In addition to the predefined matching performed by the Forescout platform, in cases where other network devices can be resolved based on string matching within the HTTP user agent, this raw data can be used in custom policies to classify devices.

12. Samba Traffic

The Packet Engine passively listens to Samba traffic and based on unique signatures in the traffic, determines the value of the network function. This is useful for determining *Windows Machine* devices.

13. HTTP User Agent on Forescout Web Server

Same as [11. Passive Detection of HTTP User Agent](#), except that instead of passively listening for traffic, the HTTP User Agent of the client connecting to the Forescout web server is read (for example, during a HTTP hijack or compliance portal access). The same rules are then used to translate this into a defined network function.

In addition to the predefined matching performed by the Forescout platform, in cases where other network devices can be resolved based on string matching within the HTTP user agent, this raw data can be used in custom policies to classify devices.

14. Passive Fingerprinting

The Packet Engine performs passive fingerprinting of the SYN and SYN-ACK packets.

15. Nmap Active Banner Scan

Resolved by the Forescout platform when it actively scans the service banners of an endpoint using Nmap.

In addition to the predefined matching performed by the Forescout platform, in cases where other network devices can be resolved based on string matching to TCP service banners, this raw data can be used in custom policies to classify devices.

16. Nmap Active OS Scan

Resolved by the Forescout platform when it actively scans the OS fingerprint of an endpoint using Nmap. This is done by analyzing the fingerprint of the TCP/IP stack.

Property Resolution Method

The lookup table typically has a mapping between regular expressions and network function values. If a given input does not match any regular expression in the lookup table, that item is considered to not have resolved the network function and the following item, in order of priority, is used.

Example 1

The classification at criterion [9. Trusted Vendor MAC](#) takes the vendor name of the NIC (based on the IEEE MAC address lookup table) and then considers whether it matches the following regular expression:

```
^htc corporation$|^rim$|^RESEARCH IN MOTION$|^RESEARCH IN MOTION LIMITED$
```

If it does, then the resulting value is 'Mobile Device'.

Example 2

The inspection at criterion [11. Passive Detection of HTTP User Agent](#) and [13. HTTP User Agent on Forescout Web Server](#), where the User Agent string of the HTTP request is matched against the following regular expressions to get corresponding property values:

*Regular Expression	Resulting Value
Windows\s*(Mobile Phone)	Mobile Device
/. *bsalsa. * . *kerberos-sec. *//Microsoft Windows	Windows Machine
Jetdirect	Printer
Netware	Server
VoIP IP\s*Phone	VoIP Device
(^\W)hp. *switch>hp~netdevice,iPhone iPad iPod Mobile. *Darwin	Mobile Device
Android Maemo>handheld~linux,Black\s*berry Symbian HP. *Palm Samsung. *phone Cisco\s*Cius Amazon\s*Kindle MIDP Hand\s*Hel d	Mobile Device
/(tcp\s* Openwall GNU. *)Linux telnetd Apache httpd [\s\d. (]*Unix. *OpenSSL//RHN-	Linux Desktop/Server
(^\W)emc(\$\W)	Storage
juniper aruba meru router wap switch wireless bridge Integrated\s*Lights\W*Out Allegro(Soft)?\s*Rom ConnectUPS VxW ork	Network Device

* This is not a complete list.

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](#), or 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 will 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.

 *If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.*

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

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

Plugin Help Files

- After the plugin is installed, 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).