FORESCOUT

Forescout

Endpoint Module: Hardware Inventory Plugin

Configuration Guide

Version 1.1

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

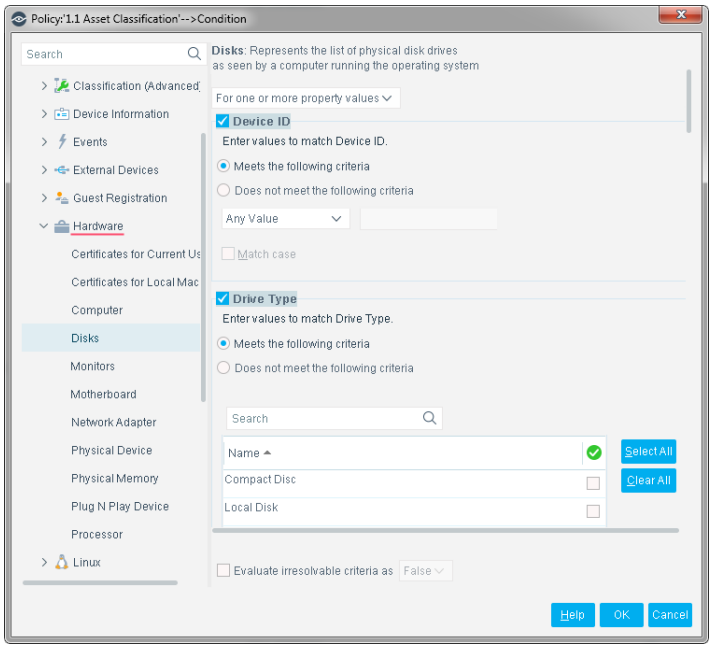
2019-02-20 16:12

Table of Contents

About the Hardware Inventory Plugin

The Hardware Inventory Plugin is a component of the Forescout® Endpoint Module. See Endpoint Module Information for details about the module.

The Hardware Inventory Plugin extends the host properties discovered by the HPS Inspection Engine to include physical hardware devices, endpoint configuration settings, and related information such as serial numbers.



Use these properties to create policies that identify and group endpoints based on system configuration or status, and to filter displays in the Home, Asset Inventory, and Asset Portal views.

For example, you can implement the following management activities using hardware-based policies:

- Discover plug-and-play or hot-swappable devices introduced by a host.
- Identify monitors and other equipment that do not comply with energy conservation guidelines.
- Administer security certificates for network adaptors and other components, or for software applications.
- Track and manage hardware inventory by serial number, vendor, configuration details, or other information.
- Find candidates for disk space and operating system upgrades.

Most Forescout hardware inventory properties are based on the standard WMI object model defined by the Distributed Management Task Force (DMTF).

What to Do

You must perform the following to work with this plugin:

- Verify that requirements are met. See Requirements for details.
- Define and implement policies that discover hosts based on hardware inventory properties. See Use Hardware Inventory Information for details.

Requirements

The plugin requires the following:

- Forescout version 8.1
- Endpoint Module version 1.1.0 with the HPS Inspection Engine running

Verify That the Plugin Is Running

After installation, verify that the plugin is running.

To verify:

1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Use Hardware Inventory Information

The Forescout platform can retrieve and work with a broad range of hardware inventory properties, supporting many security and management actions.

Hardware inventory monitoring can significantly increase communication between CounterACT devices and hosts. The general discovery policies described here, which retrieve information for all monitored hosts, can generate a large volume of traffic. See Optimizing Hardware Inventory Performance.

Inventory Policies to Support Host Management

You can use policies that examine hardware inventory properties to implement a broad range of administration and management tasks.

Example: Compliance with Corporate Usage Guidelines

When corporate guidelines govern the details of host computer usage, define Forescout platform policies that identify non-compliant hosts. For example:

- Use the **Power Management Supported** field of the Computer property to verify compliance with energy-conservation rules.
- Use the **Current Time Zone** and **Status** fields of the Computer property to enforce time restrictions on computer access.

Example: Management of Machine Certificates

The **Certificates for Current User** and **Certificates for Local Machine** properties report detailed information about certificates on the endpoint.

- Use the **Not Before** and **Not After** fields of the certificate-related properties to identify pending or expired software licenses.
- Use the **Subject**, **Serial Number**, or **Issuer** fields to define exceptions for certificates used in spoofing attacks.

Example: Identifying Hot-Swappable Disks and other Hardware Security Risks

Use the **Drive Type** field in the Disks properties to find disks and other devices that may present data security risks:

Example: Hardware Maintenance

Policies can examine a broad range of properties to find candidates for hardware maintenance and/or upgrade actions. For example:

- Define conditions based on the **Free Space**, **Drive Type**, and **Status** fields of the Disks property to discover disks and storage devices that operate at maximum capacity. Use time limits and recheck options to identify endpoints that regularly exceed threshold values.
- Use the **CPU Status**, **Load Percentage**, **Family**, and **Max Clock Speed** fields of the Processor property to identify processors that should be upgraded.
- Use the **Manufacturer** or **Serial Number** fields of the Physical Device property to identify equipment from specific vendors.

Optimizing Hardware Inventory Performance

The CIM specifications are very detailed. This plugin opens the Forescout platform to a large collection of information from Windows machines, and the Forescout platform must poll hosts for property values. This can increase communication between CounterACT devices and hosts.

Use the following strategies to minimize the traffic resulting from hardware inventory reporting:

Deploy hardware inventory properties strategically – and selectively. The Forescout platform only retrieves hardware properties that are referenced by active policies.

Carefully consider the hardware properties that you want to use, and create policies with only those properties.

Limit the scope of policies that use hardware properties. Combine conditions to target a focused set of relevant hosts or devices.

Tune run/recheck intervals to minimize polling. Many hardware properties do not change often, or at all. You can run/recheck policies that examine these properties less frequently than most policies. Longer recheck intervals let the Forescout platform distribute polling interactions to prevent traffic spikes. Follow these general guidelines to determine how frequently to run a policy that uses hardware properties:

- Stable values such as number of processors, model, or serial numbers rarely change. Typically, you examine these properties to identify unauthorized hosts or to identify upgrade candidates. These policies can be run once a day, or on demand.
- Performance or configuration values, such as certificates, power consumption, or free memory, may change infrequently, but such changes impact management policies. These properties can be examined every 15 minutes, or several times a day.
- Changes that present security risks require rapid discovery. For example, a policy that detects the insertion of removable storage media can be run more frequently. Use additional conditions to limit the scope of the policy.

Hardware Inventory Properties

When the Hardware Inventory plugin is installed as part of the Endpoint Module, you can use the hardware properties to create conditions in Forescout platform policies.

Most hardware inventory properties are based on the standard WMI object model defined by the Distributed Management Task Force (DMTF). The relevant class definition of the Win32 object namespace is referenced in the descriptions below.

Certificate Properties

The plugin provides two properties that let you detect endpoints based on digital certificates present on the endpoint:

Certificates for Current User reports certificates found in the following Windows registry locations:

> *The CURRENT_USER referenced in these paths is the account used by the Forescout platform to inspect the endpoint.*

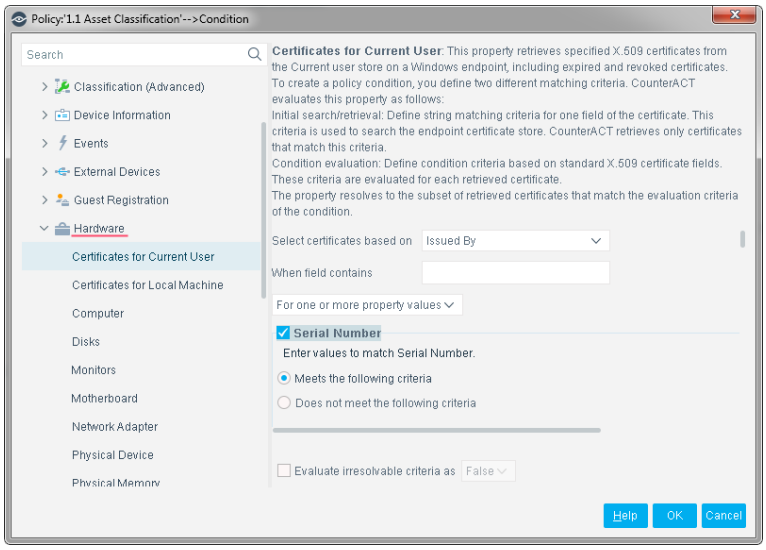
- HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates
- HKEY_CURRENT_USER\Software\Policy\Microsoft\SystemCertificates

Certificates for Local Machine reports certificates found in the following Windows registry locations:

- HKEY_LOCAL_MACHINE\Software\Microsoft\SystemCertificates
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates
- HKEY_LOCAL_MACHINE\Software\Microsoft\EnterpriseCertificates
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Services\ServiceName\SystemCertificates

These properties are not based on the WMI object model. Script-based queries are used to retrieve certificate information.

These properties do not necessarily contain all *the certificates at these locations of the endpoint registry. When you use these properties, you define the search criteria used to retrieve a subset of certificates on the endpoint. See* *Working with Certificate Properties*.



The following information is returned for each certificate:

- Serial Number
- Status
- Name
- Subject
- Issuer
- Not After

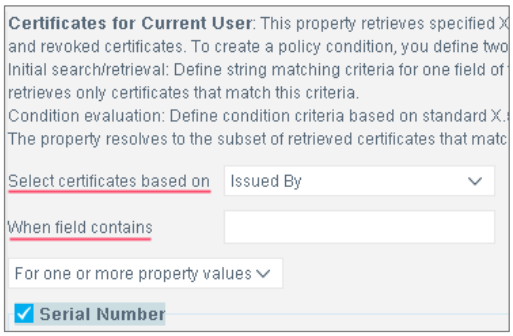
Working with Certificate Properties

Certificate properties provided by this plugin do not contain all the certificates at these locations of the endpoint registry. When you use these properties, you define search criteria that are used to retrieve a subset of certificates on the endpoint.

To create a policy condition based on certificate information, follow this two-step procedure:

1. ***Define data retrieval criteria***. The Forescout platform only retrieves information for certificates that match these criteria. To define retrieval criteria:

– From the **Select certificates based on** drop-down menu, select the certificate field to be examined.
– In the **When field contains** field, select a matching condition.



The plugin retrieves only the certificates on the endpoint that match the defined criteria.

2. ***Define a policy condition***. As for other policy conditions, define a matching condition using one or more of the certificate property fields.

   For each endpoint, the condition is evaluated only for certificates retrieved based on the data retrieval criteria.

Computer

You can detect hosts based on the following properties of the Win32_ComputerSystem class:

- Name
- User Name
- Primary Owner Contact
- Primary Owner Name
- Support Contact Description
- Part of Domain
- Domain
- Domain Role
- Workgroup
- Roles
- Manufacturer
- Model
- OEM String Array
- Description
- Caption
- System Type
- PC System Time
- Current Time Zone
- Bootup State
- Number Of Processors
- Total Physical Memory (Megabytes)
- Keyboard Password Status
- Power Management Supported
- Power State
- Thermal State
- Status

Disks

You can detect hosts based on the following properties of the Win32_LogicalDisk class:

- Device ID
- Name

- DriveType
- Volume Name
- Free Space (Megabytes)
- Size (Megabytes)
- Availability
- Description
- MediaType
- Status
- File System

Monitors

You can detect hosts based on the following properties of the Win32_DesktopMonitor class:

- Name
- Monitor Manufacturer
- Monitor Type
- Device ID
- Status
- Availability
- Is Locked
- Power Management Supported
- Screen Height
- Screen Width
- Error Description

Motherboard

You can detect hosts based on the following properties of the Win32_BaseBoard class:

- Name
- Caption
- Description
- Manufacturer
- Model
- Other Identifying Info
- Part Number
- Serial Number
- SKU
- Product
- Version
- Hosting Board
- Hot Swappable
- Removable
- Replaceable

Network Adapter

You can detect hosts based on the following properties of the Win32_NetworkAdapter class:

- Index
- Description
- Service Name
- IP Address
- IP Subnet
- Default IP Gateway
- IP Enabled
- IP Connection Metric
- MACAddress
- DHCP Enabled
- DHCP Server
- DNS Domain
- DNS HostName
- DNS Server Search Order
- Domain DNS Registration Enabled
- IGMP Level

Physical Device

You can detect hosts based on the following properties of the Win32_PhysicalMedia class:

- Name
- Caption
- Description
- Manufacturer
- Model
- Other Identifying Info
- Part Number
- Serial Number
- SKU
- Status
- Tag
- Version

Physical Memory

You can detect hosts based on the following properties of the Win32_PhysicalMemory class:

- Name
- Caption
- Description
- Manufacturer
- Removable
- Replaceable
- SKU
- Part Number
- Serial Number
- Other Identifying Info
- Status
- Capacity
- Memory Type
- Data Width
- Bank Label
- Device Locator
- Speed

Plug and Play Device

You can detect hosts based on the following properties of the Win32_PNPEntity class:

- Name
- Caption
- Description
- Manufacturer
- Class GUID
- Device ID
- PNP Device ID
- Service

Processor

You can detect hosts based on the following properties of the Win32_Processor class:

- Name
- Family
- Device ID
- Processor ID
- Manufacturer
- Address Width
- Architecture
- Max Clock Speed
- Number Of Cores
- Load Percentage
- CPU Status

Inventory Views

When you use this plugin for the first time, a Hardware folder appears in the Views tree of the Asset Inventory screen. These views group hosts by common characteristics, based on hardware inventory property values. To populate these views, you must define policies that classify hosts based on the hardware properties provided by this plugin.

Endpoint Module Information

The Hardware Inventory plugin is installed with the Forescout Endpoint Module.

The Forescout® Endpoint Module provides connectivity, visibility, and control to network endpoints through the following Forescout components:

- HPS Agent Manager
- HPS Inspection Engine
- Hardware Inventory Plugin
- Linux Plugin
- Microsoft SMS/SCCM Plugin
- OS X Plugin

The Endpoint Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of the Forescout platform.

Components listed above are installed and rolled back with the Endpoint Module.

Executable Files Used by the Plugin on Windows Endpoints

This plugin deploys the following executable files on endpoints to resolve inventory related properties.

Name	Description	Last Updated
hwi_cert_store_new.exe	Resolves the **Certificates for Current User** and the **Certificates for Local Machine** properties.	1.1.0
hwi_disks_query.vbs	Resolves the **Disks** property.	1.1.0
hwi_monitors.vbs	Resolves the **Monitors** property.	1.0.2

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).