ForeScout CounterACT®

Hardware Inventory Plugin

Configuration Guide

Version 1.0.3

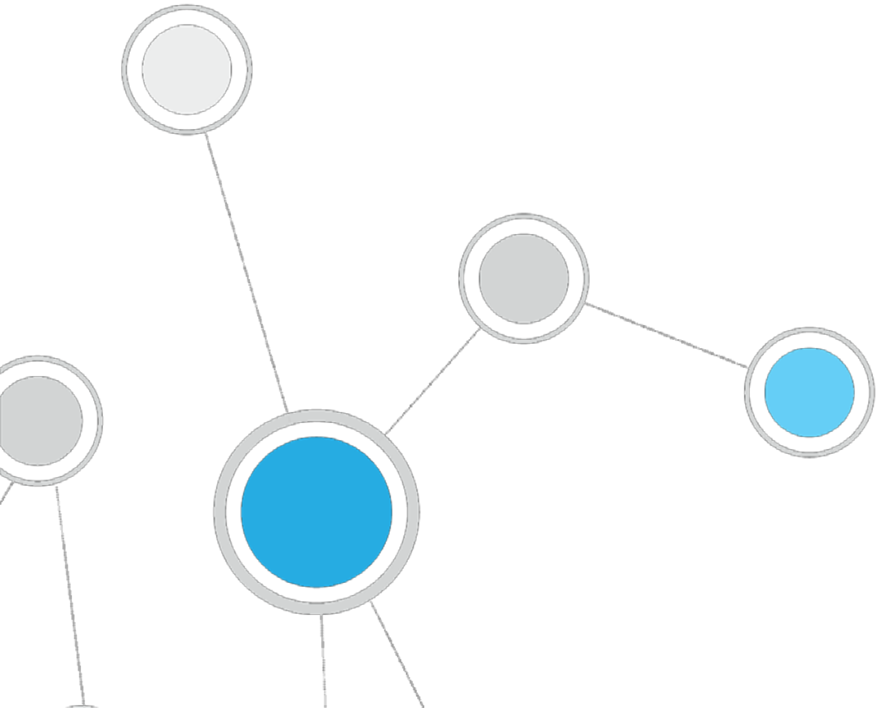
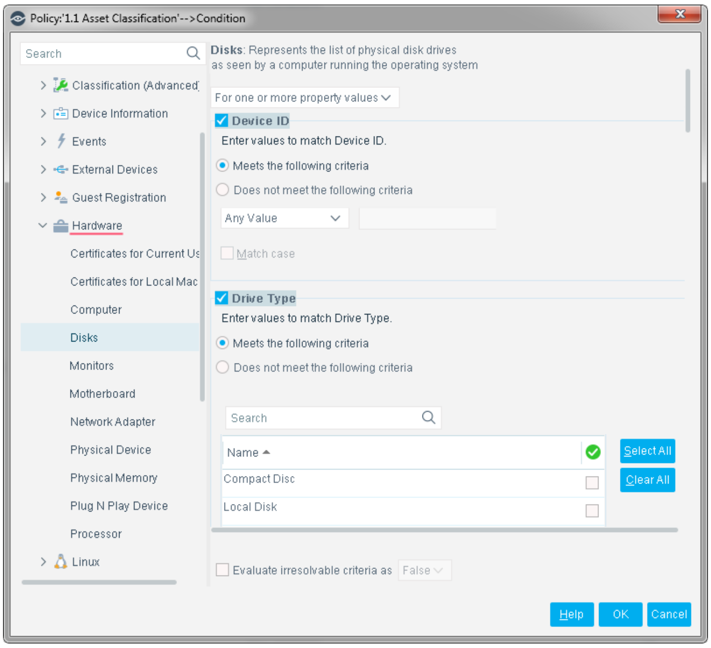


Table of Contents

About the Hardware Inventory Plugin

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.


Policy:'1.1 Asset Classification'-->Condition

Disks: Represents the list of physical disk drives as seen by a computer running the operating system

For one or more property values

☑ Device ID

Enter values to match Device ID.

● Meets the following criteria

○ Does not meet the following criteria

Any Value

□ Match case

☑ Drive Type

Enter values to match Drive Type.

● Meets the following criteria

○ Does not meet the following criteria

Name	✓
Compact Disc	□
Local Disk	□

□ Evaluate irresolvable criteria as False

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 CounterACT 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 CounterACT releases and other CounterACT components:

- CounterACT version 7.0.0 or above.
- HPS Inspection Engine plugin version 10.4.1 or above installed and running.

Installation

This section describes how to install the plugin.

To install the plugin:

1. Navigate to the Product Updates Portal, Base Plugins page and download the plugin **`.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 plugin **`.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 plugin is listed in the Plugins pane.

Use Hardware Inventory Information

CounterACT can retrieve and work with a broad range of hardware inventory properties, supporting many security and managements actions.

🗎 *Hardware inventory monitoring can significantly increase communication between CounterACT devices and hosts. In particular, 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 details of host computer usage, define CounterACT policies that identify non-compliant hosts. For example:

- Use the *Power Management Supported* field of the **Computer** property and related properties 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 certificate related properties to identify pending or expired software licenses.
- Use the *Subject*, *Serial Number*, or *Issuer* fields to define exception lists of certificates used in spoofing attacks.

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

Use the *Drive Type* field of the **Disks** property 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 CounterACT to a large collection of information from Windows machines - and CounterACT must poll hosts for property values. This can increase communication between CounterACT devices and hosts.

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

Deploy hardware inventory properties strategically – and selectively. CounterACT 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 CounterACT distribute polling interactions to prevent traffic spikes. Use the following 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 changes impact management policies. These properties can be examined every 15 minutes, or several times in a day.
- Changes that present security risks require rapid discovery. For example, a policy that detects 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, you can use the hardware properties described in this section to create conditions in CounterACT policies.

Most CounterACT 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 CounterACT to inspect the endpoint.*

- HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates

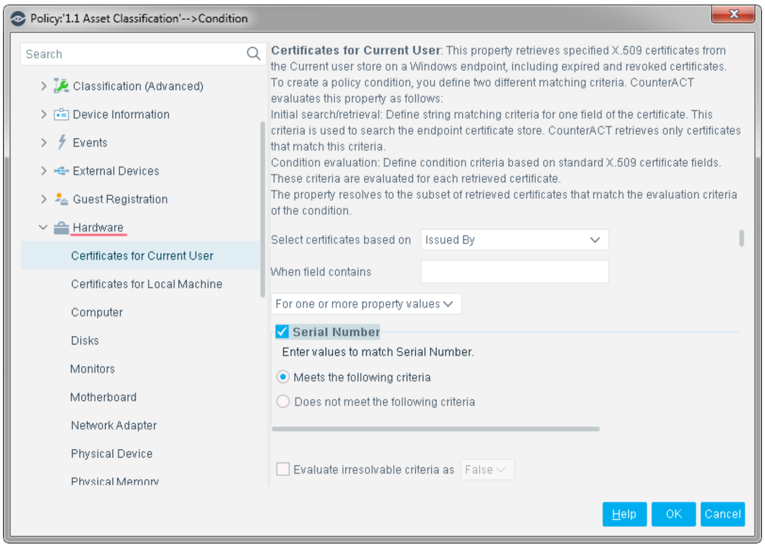
- HKEY_CURRENT_USER\Software\Policy\Microsoft\SystemCertificates

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. CounterACT uses script-based queries 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 search criteria that are used to retrieve* a subset of certificates *on the endpoint. See* *Working with Certificate Properties*.



Certificates for Current User: This property retrieves specified X.509 certificates from the Current user store on a Windows endpoint, including expired and revoked certificates.
To create a policy condition, you define two different matching criteria. CounterACT evaluates this property as follows:
Initial search/retrieval: Define string matching criteria for one field of the certificate. This criteria is used to search the endpoint certificate store. CounterACT retrieves only certificates that match this criteria.
Condition evaluation: Define condition criteria based on standard X.509 certificate fields. These criteria are evaluated for each retrieved certificate.
The property resolves to the subset of retrieved certificates that match the evaluation criteria of the condition.

Select certificates based on: Issued By

When field contains:

For one or more property values

☑ **Serial Number**

Enter values to match Serial Number.

● Meets the following criteria

○ Does not meet the following criteria

□ Evaluate irresolvable criteria as False

The following information is returned for each certificate:

- Serial Number
- Status
- Name
- Subject
- Issuer
- Thumbprint
- Store
- Not Before
- Not After

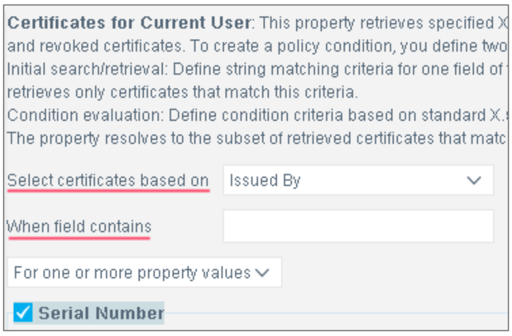
Working with Certificate Properties

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***. CounterACT only retrieves information for certificates that match these criteria. To define retrieval criteria:

- Use the **Select certificates based on** drop-down to specify which certificate field is examined.
- Use the **When field contains** field to specify a matching condition.



Certificates for Current User: This property retrieves specified X
and revoked certificates. To create a policy condition, you define two
Initial search/retrieval: Define string matching criteria for one field of
retrieves only certificates that match this criteria.
Condition evaluation: Define condition criteria based on standard X.
The property resolves to the subset of retrieved certificates that matc

Select certificates based on: Issued By

When field contains:

For one or more property values

☑ **Serial Number**

The plugin retrieves only the certificates on the endpoint for which the specified certificate field matches the criteria.

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

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

Computer

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

Detect hosts based on the following properties of the Win32_LogicalDisk class.

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

Monitors

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

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

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

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

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

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

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, CounterACT creates a Hardware folder 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.

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 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
- Product Updates 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 https://updates.forescout.com/support/files/counteract/docs_portal/.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Product Updates Portal

The Product Updates 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 Product Updates 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

2018-10-07 16:43