FORESCOUT

Forescout

HPS Applications Plugin

Configuration Guide

Version 2.1.25

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

2020-02-13 14:44

Table of Contents

About the HPS Applications Plugin

Windows Applications is a Content Module that works with the HPS Inspection Engine to support in-depth discovery and management of the following software and applications on Windows endpoints:

- Windows operating system information, including:
  - Release
  - Package/flavor
  - Service Pack
- The following third-party applications, which present unique security challenges:
  - Antivirus
  - Peer-to-peer
  - Anti-spyware
  - Personal Firewall
  - Instant Messaging
  - Hard Drive Encryption
  - Cloud Storage
  - Microsoft products and other applications on Windows endpoints

The Windows Applications Module provides host properties and actions that let you detect and manage endpoints based on this information. Use CounterACT policies to discover endpoints running specific applications, and to apply remediation actions.

For example:

- Identify endpoints running specific Windows operating systems, and apply patches or vulnerability updates.
- Identify endpoints running specific peer-to-peer applications, and kill the application.
- Update a specific antivirus package, and start it on an endpoint.

Supported Applications

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Refer to the HPS Applications Release Notes provided with each release for information regarding changes and updates.

Requirements

- CounterACT® version 7.0.0.
- Service Pack 2.0.1 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates. Do not install Service Pack beta releases with this plugin.
- An active Maintenance Contract for CounterACT devices.
- These plugins:
  - HPS Inspection Engine Plugin version 10.2.2 or above
  - HPS NIC Vendor DB Plugin

Installation

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.

Configuration

No configuration is required.

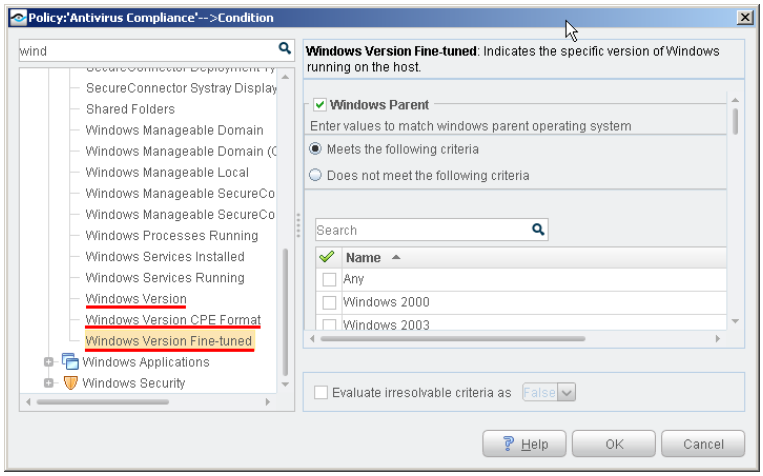
Working with Endpoint Information

The plugin provides host properties and actions to support the following policy-based detections and management actions:

- Detect Windows Versions
- Detect Third-Party Applications
- Manage Third-Party Applications

Detect Windows Versions

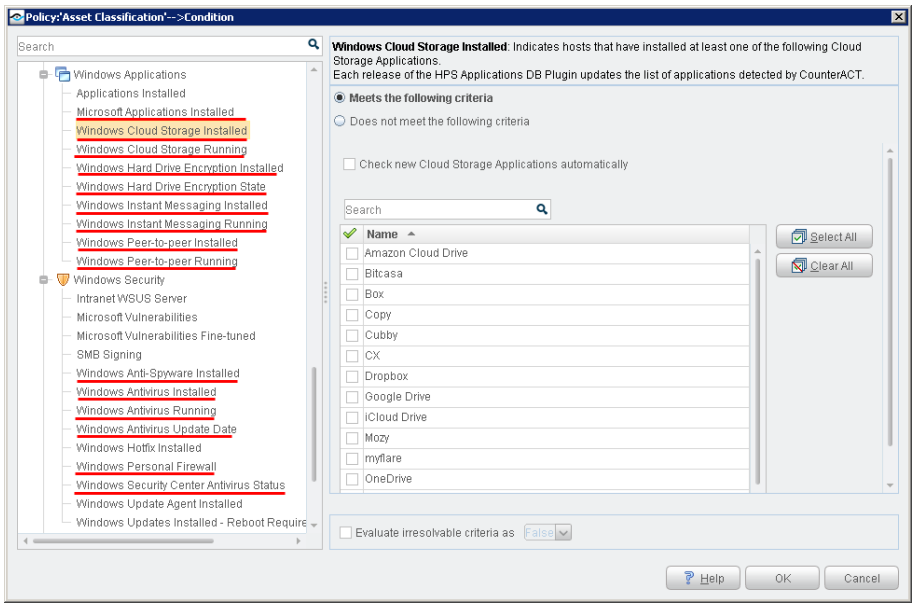
The plugin provides the following host properties to detect Windows applications.



Windows Version	Indicates Windows versions detected on the endpoint.
Windows Version CPE Format	Indicates Windows versions running on an endpoint, in Common Platform Enumeration format. The property returns the full CPE 2.3 name string for each Windows version, as follows: **`cpe:2.3:o:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>`** Use CounterACT text matching tools to create policy conditions that identify logical parts or substrings of the CPE name string.
Windows Version Fine-tuned	Indicates Windows versions detected on the endpoint, based on detailed criteria such as Windows version, flavor, and service packs installed.

Detect Third-Party Applications

The plugin provides the following host properties to detect third-party applications.



These host properties list the third-party applications that CounterACT detects. Each release of this plugin updates the applications that are listed, as CounterACT detects new applications.

The **Check new…** and **Detect new…** checkboxes determine whether new applications supported by subsequent updates are added to the condition you define.

- By default the checkbox is cleared, and the condition remains as you defined it. New applications are not included in the condition criteria.
- Select the checkbox to include new applications in the condition criteria.

Windows Anti-Spyware Installed	Indicates the anti-spyware applications(s) installed on the Windows endpoint.
Windows Antivirus Installed	Indicates the antivirus applications(s) installed on the Windows endpoint, as detected by CounterACT.
Windows Antivirus Running	Indicates the antivirus application(s) running on the Windows endpoint, as detected by CounterACT.
Windows Antivirus Update Date	Indicates the most recent date and time that antivirus application(s) were updated on the Windows endpoint, as detected by CounterACT.
Windows Cloud Storage Application Installed	Indicates the cloud storage applications(s) installed on the Windows endpoint.
Windows Cloud Storage Application Running	Indicates the cloud storage application(s) running on the Windows endpoint.
Windows Hard Drive Encryption Installed	Indicates whether supported encryption applications are installed on the Windows endpoint.

Windows Hard Drive Encryption State	Indicates whether one or more drives/partitions on the Windows endpoint have been encrypted using supported encryption applications.
Windows Instant Messaging Installed	Indicates the instant messaging applications(s) installed on the Windows endpoint.
Windows Instant Messaging Running	Indicates the instant messaging application(s) running on the Windows endpoint.
Microsoft Applications Installed	Indicates the Microsoft application(s) installed on the Windows endpoint.
Windows Peer-to-peer Installed	Indicates the peer-to-peer applications(s) installed on the Windows endpoint.
Windows Peer-to-peer Running	Indicates the peer-to-peer application(s) running on the Windows endpoint.
Windows Personal Firewall	Indicates the personal firewall applications(s) installed on the Windows endpoint.
Windows Security Center Antivirus Status	Indicates the presence and status of antivirus applications installed on the Windows endpoint, as reported by the Windows Security Center.

To create policy conditions based on these properties, choose from the list of supported third-party applications. Forescout has analyzed the structure, footprint, and related processes of these applications, so the plugin detects them more accurately and inspects them more deeply. New releases of the plugin typically add supported applications, or enhance support for known applications.

When you define policy rules to handle detected endpoints, remember that the scope of these properties is limited to supported applications: they do not detect or inspect unsupported applications.

For example:

- The **Windows Instant Messaging Installed** property detects endpoints on which at least one supported messaging application is installed. It does not detect other applications that may be present on the Windows endpoint. When no *supported* applications are detected on the endpoint, the property resolves to the value *None* - but unsupported messaging applications may be present.
- Similarly, the **Windows Hard Drive Encryption State** property detects drives/partitions encrypted by supported applications. When no drives are encrypted by *supported* applications, the property resolves to the value *Not Encrypted* for each partition on the endpoint - but partitions may be encrypted by unsupported applications.

Use other host properties to create conditions that inspect endpoints and detect files or processes of unsupported applications.

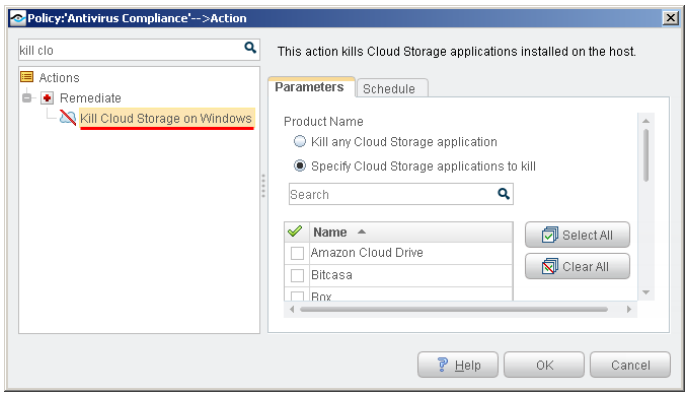
Manage Third-Party Applications

The plugin provides the following actions to remediate/manage third-party applications.

- Kill Cloud Storage on Windows
- Kill Instant Messaging on Windows
- Kill Peer-to-Peer on Windows
- Start Antivirus on Windows
- Update Antivirus on Windows

Kill Cloud Storage on Windows

This action halts the specified cloud storage applications that are running on Windows endpoints.



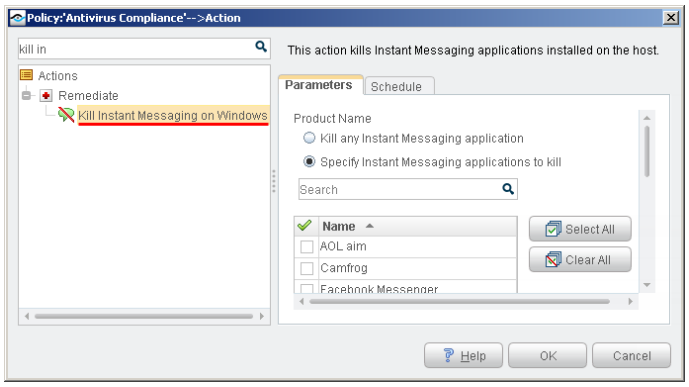
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

To increase kill frequency, CounterACT can automatically install SecureConnector on endpoints when this action is applied to them. When you configure the HPS Inspection engine plugin, select the **Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process, Kill IM and P2P actions** checkbox. See the *HPS Inspection Engine Plugin Configuration Guide* for details about SecureConnector configuration.

CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials ***Manageable (Domain)****. See the* HPS Inspection Engine Plugin Configuration Guide *for details about scripts.*

Kill Instant Messaging on Windows

This action halts specific instant messaging applications that are running on Windows endpoints.



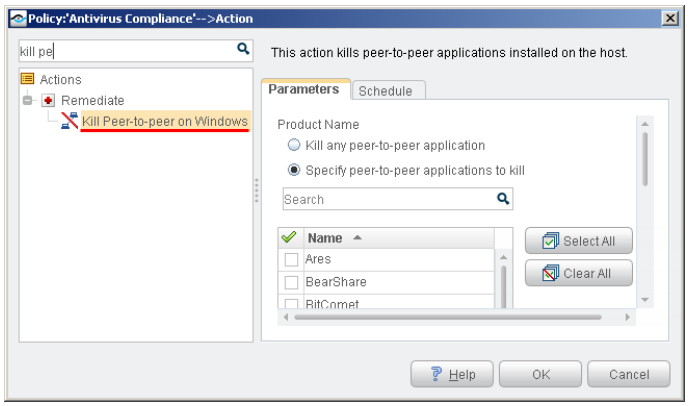
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

To increase kill frequency, CounterACT can automatically install SecureConnector on endpoints when this action is applied to them. When you configure the HPS Inspection engine plugin, select the **Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process, Kill IM and P2P actions** checkbox. See the *HPS Inspection Engine Plugin Configuration Guide* for details about SecureConnector configuration.

> *CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials* ***Manageable (Domain)****. See the* HPS Inspection Engine Plugin Configuration Guide *for details about scripts.*

Kill Peer-to-Peer on Windows

This action halts specific peer-to-peer applications installed at Windows endpoints.



By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

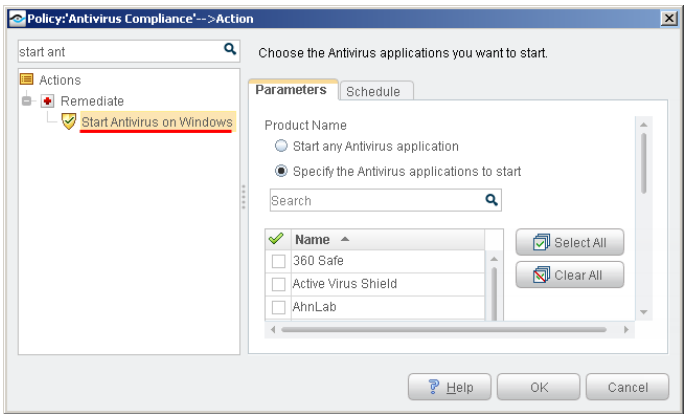
To increase kill frequency, CounterACT can automatically install SecureConnector on endpoints when this action is applied to them. When you configure the HPS

Inspection engine plugin, select the **Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process, Kill IM and P2P actions** checkbox. See the *HPS Inspection Engine Plugin Configuration Guide* for details about SecureConnector configuration.

CounterACT runs a script on the endpoint to apply this action if the endpoint is managed via domain credentials ***Manageable (Domain)****. See the* HPS Inspection Engine Plugin Configuration Guide *for details about scripts.*

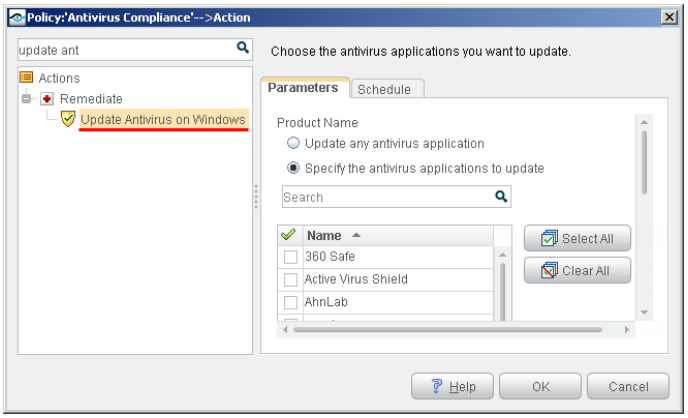
Start Antivirus on Windows

Launch antivirus applications that have been halted at Windows endpoints.



Update Antivirus on Windows

Update outdated antivirus applications at Windows endpoints.



You may need to select more than one application if you think several antivirus applications are installed on endpoints in the policy scope. If more than one antivirus application is installed on an endpoint, CounterACT updates only the first of the selected applications that it detects.

CounterACT runs a script on the endpoint to apply this action if the endpoint is managed via domain credentials **Manageable (Domain)****. Refer to the** HPS Inspection Engine Plugin Configuration Guide *for details about scripts.*

Additional Forescout Documentation

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

- Forescout Resources Page
- Product Updates Portal
- Documentation Portal
- Forescout Help Tools

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, 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:

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

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 **CounterACT 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 the Documentation Portal (Per-Appliance licensing).

Appendix A: Endpoint Applications Detected by CounterACT

The Windows Applications Module discovers applications of the following vendors on Windows endpoints, for the following types of software:

Supported Windows Antivirus Vendors

Active Virus Shield	ESTsoft	Microsoft
AhnLab	F-Secure	New Technology Wave
AVG/Avast	FortiClient	Panda
Avira	G Data	Palo Alto Networks
BitDefender	Hauri	PC Ziggy
CA E-trust	K7 Computing	Qihoo 360
Carbon Black	Kaspersky	Rising
ClamAV	LANDesk	Sophos
Comodo	Lightspeed	Symantec
CrowdStrike	Malwarebytes	Trend Micro
eScan	McAfee	VIPRE
ESET		Webroot

Supported Windows Peer-to-peer Vendors

Ares Galaxy	Foxy	Shareaza
BearShare (Gnutella)	Free Download Manager	Soulseek
Bitcomet	FrostWire	Spotify
BitLord	iMesh	Tixati
BitSpirit	Jubster	Transmission
BitTorrent	Kazaa	TrustyFiles
BitTyrant	LimeWire	Twister
Deluge	Miro	uTorrent
eMule	Morpheus	Vuze
ezPeer	MP3 Rocket	Warez
FolderShare	OneSwarm	Xunlei

Supported Windows Instant Messaging Vendors

AOL
Camfrog
Cisco
Facebook
Google
ICQ
Microsoft
Nate
Paltalk
QQ
Skype
Trillian
Yahoo

Supported Windows Anti-Spyware Vendors

Anonymizer
BrightFort (Spyware Blaster/Spyware Doctor)
CounterSpy
Kephyr
Lavasoft
McAfee
Microsoft
Safer-Networking (Spybot)
Trend Micro
Webroot

Supported Windows Personal Firewall Vendors

McAfee
Microsoft
Sophos
Sygate
Symantec
Zone Labs/Check Point

Supported Hard Drive Encryption Applications

Microsoft BitLocker
Check Point Endpoint Full Disk Encryption
Symantec Endpoint Encryption

Supported Cloud Storage Applications

Amazon Cloud Drive
Bitcasa
Box
Copy
Cubby
CX
Dropbox
Google Drive
iCloud Drive
Mozy
myflare
OneDrive
SugarSync

Refer to the Windows Applications Release Notes for information regarding changes or updates in application support.