ForeScout CounterACT®

Windows Applications

Configuration Guide

Updated February 2018

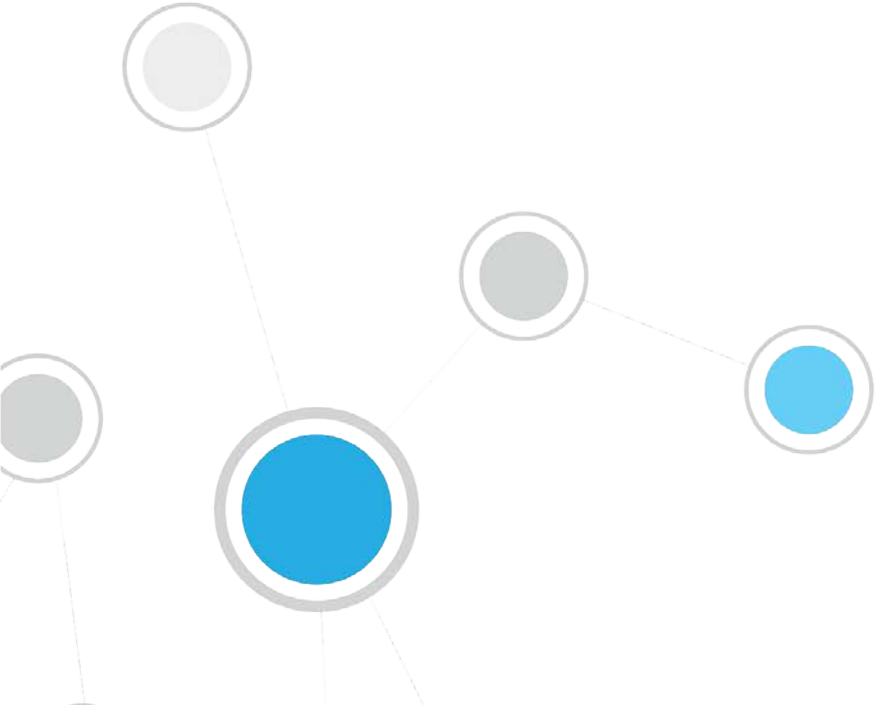


Table of Contents

About Windows Applications 3
Requirements 3

Installation 4
Verify That the Module Is Running 5

Configuration 5

Working with Endpoint Information 5
Detect Windows Versions 6
Detect Third-Party Applications 7
Manage Third-Party Applications 9
Kill Cloud Storage on Windows 9
Kill Instant Messaging on Windows 10
Kill Peer-to-Peer on Windows 10
Start Antivirus on Windows 11
Update Antivirus on Windows 12

Appendix A: Endpoint Applications Detected by CounterACT 12
Supported Windows Antivirus Vendors 13
Supported Windows Peer-to-peer Vendors 13
Supported Windows Instant Messaging Vendors 13
Supported Windows Anti-Spyware Vendors 13
Supported Windows Personal Firewall Vendors 14
Supported Hard Drive Encryption Applications 14
Supported Cloud Storage Applications 14

Additional CounterACT Documentation 15
Documentation Downloads 15
Documentation Portal 15
CounterACT Help Tools 16

About Windows Applications

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.

Refer to the Windows Applications Release Notes for information regarding changes, updates, and recommendations for working with this release.

Requirements

The module requires the following CounterACT releases and other CounterACT components:

- CounterACT® version 8.0
- An active Maintenance Contract for CounterACT devices is required.
- Endpoint Module version 1.0 with the HPS Inspection Engine running.
- NIC Vendor DB Content Module version 1.2.3 running.

Installation

To install the module:

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

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in 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 wizard opens.
9. Select **I agree to the License Agreement**, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

🗎 *Make sure you have selected the correct module to install. The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.*

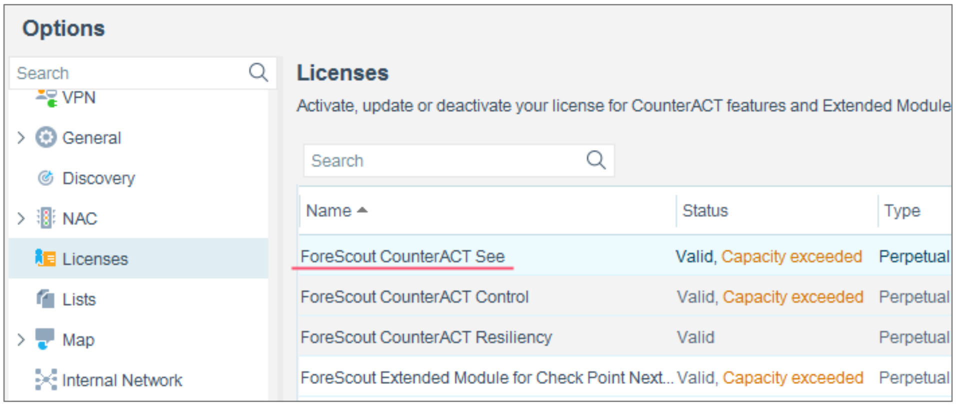
🗎 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

10. When the installation completes, select **Close** to close the wizard. The installed module is displayed in the Modules pane.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Verify That the Module Is Running

After installing the module, verify that it is running.

To verify:

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

Configuration

No configuration is required.

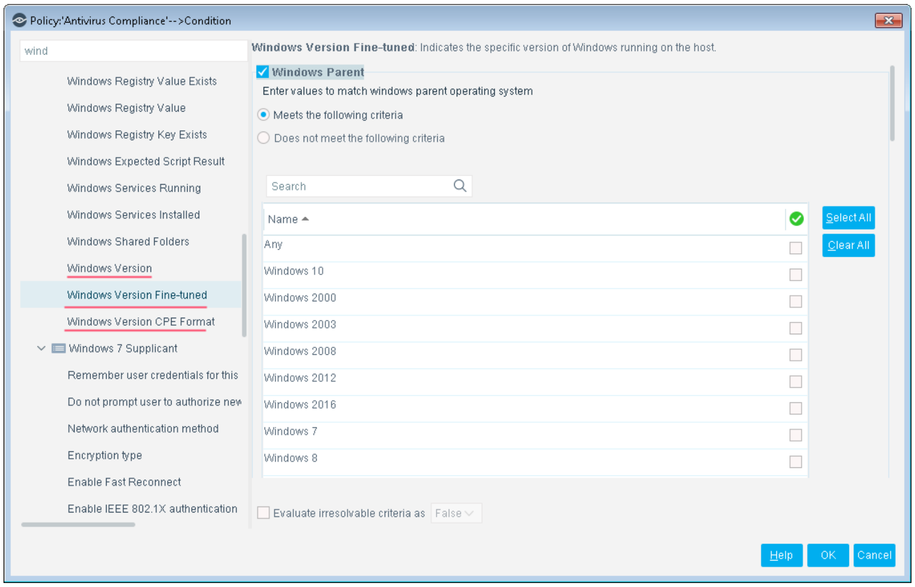
Working with Endpoint Information

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



Policy:'Antivirus Compliance'-->Condition

wind

- Windows Registry Value Exists
- Windows Registry Value
- Windows Registry Key Exists
- Windows Expected Script Result
- Windows Services Running
- Windows Services Installed
- Windows Shared Folders
- Windows Version
- Windows Version Fine-tuned
- Windows Version CPE Format
- Windows 7 Supplicant
  - Remember user credentials for this
  - Do not prompt user to authorize new
  - Network authentication method
  - Encryption type
  - Enable Fast Reconnect
  - Enable IEEE 802.1X authentication

Windows Version Fine-tuned: Indicates the specific version of Windows running on the host.

☑ Windows Parent

Enter values to match windows parent operating system

● Meets the following criteria

○ Does not meet the following criteria

Search

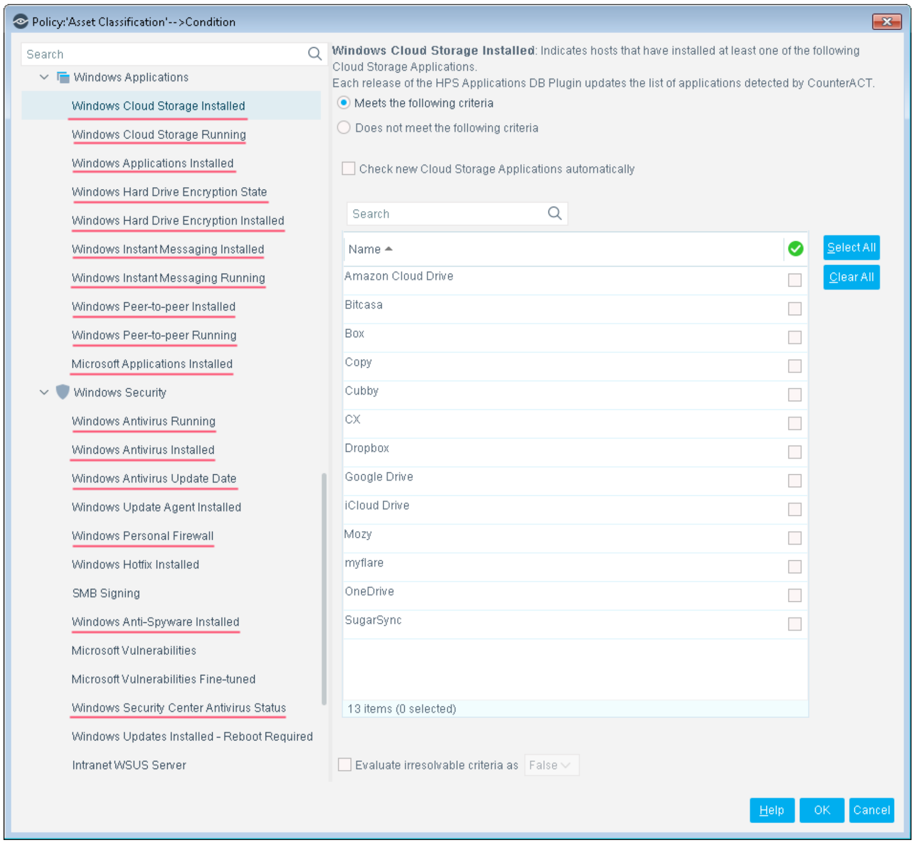
Name ▲	✓
Any	□
Windows 10	□
Windows 2000	□
Windows 2003	□
Windows 2008	□
Windows 2012	□
Windows 2016	□
Windows 7	□
Windows 8	□

□ Evaluate irresolvable criteria as False

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.

Detect Third-Party Applications

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



Policy:'Asset Classification'-->Condition

Search

- Windows Applications
  - Windows Cloud Storage Installed
  - Windows Cloud Storage Running
  - Windows Applications Installed
  - Windows Hard Drive Encryption State
  - Windows Hard Drive Encryption Installed
  - Windows Instant Messaging Installed
  - Windows Instant Messaging Running
  - Windows Peer-to-peer Installed
  - Windows Peer-to-peer Running
  - Microsoft Applications Installed
- Windows Security
  - Windows Antivirus Running
  - Windows Antivirus Installed
  - Windows Antivirus Update Date
  - Windows Update Agent Installed
  - Windows Personal Firewall
  - Windows Hotfix Installed
  - SMB Signing
  - Windows Anti-Spyware Installed
  - Microsoft Vulnerabilities
  - Microsoft Vulnerabilities Fine-tuned
  - Windows Security Center Antivirus Status
  - Windows Updates Installed - Reboot Required
  - Intranet WSUS Server

Windows Cloud Storage Installed: Indicates hosts that have installed at least one of the following Cloud Storage Applications.
Each release of the HPS Applications DB Plugin updates the list of applications detected by CounterACT.

● Meets the following criteria
○ Does not meet the following criteria

□ Check new Cloud Storage Applications automatically

Search

Name ▲	✓
Amazon Cloud Drive	□
Bitcasa	□
Box	□
Copy	□
Cubby	□
CX	□
Dropbox	□
Google Drive	□
iCloud Drive	□
Mozy	□
myflare	□
OneDrive	□
SugarSync	□

13 items (0 selected)

□ Evaluate irresolvable criteria as False

These host properties list the third-party applications that CounterACT detects. Each release of this module 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 module detects them more accurately and inspects them more deeply. New releases of the module typically add supported applications, or enhance support for known applications.

When you use these properties in policies rules, remember that these properties do not detect or inspect unsupported applications. For example:

- The **Windows Instant Messaging Installed** property detects supported messaging applications installed on endpoints. It does not detect other messaging 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.

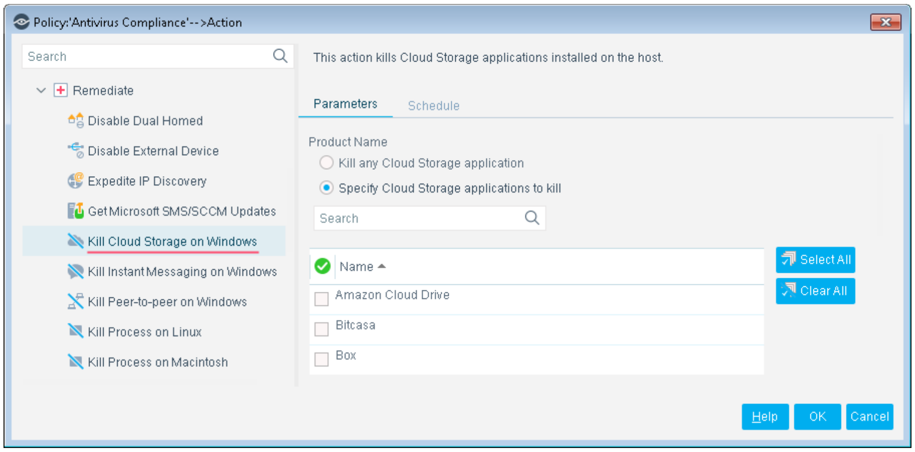
Manage Third-Party Applications

The module 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.



Policy:'Antivirus Compliance'-->Action

This action kills Cloud Storage applications installed on the host.

Product Name

○ Kill any Cloud Storage application

● Specify Cloud Storage applications to kill

	Name
□	Amazon Cloud Drive
□	Bitcasa
□	Box

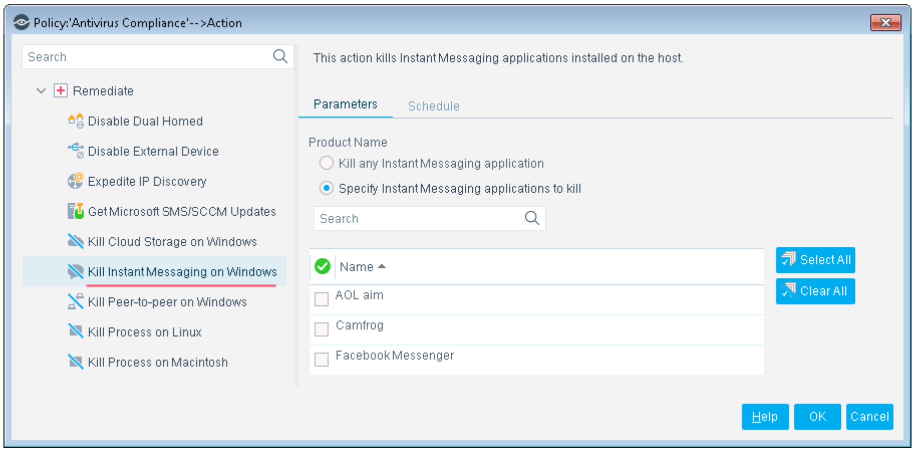
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

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, 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 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 Configuration Guide *for details about scripts.*

Kill Instant Messaging on Windows

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



Policy:'Antivirus Compliance'-->Action

Search

- Remediate
  - Disable Dual Homed
  - Disable External Device
  - Expedite IP Discovery
  - Get Microsoft SMS/SCCM Updates
  - Kill Cloud Storage on Windows
  - Kill Instant Messaging on Windows
  - Kill Peer-to-peer on Windows
  - Kill Process on Linux
  - Kill Process on Macintosh

This action kills Instant Messaging applications installed on the host.

Parameters | Schedule

Product Name

○ Kill any Instant Messaging application

● Specify Instant Messaging applications to kill

Search

✓	Name ▲
□	AOL aim
□	Camfrog
□	Facebook Messenger

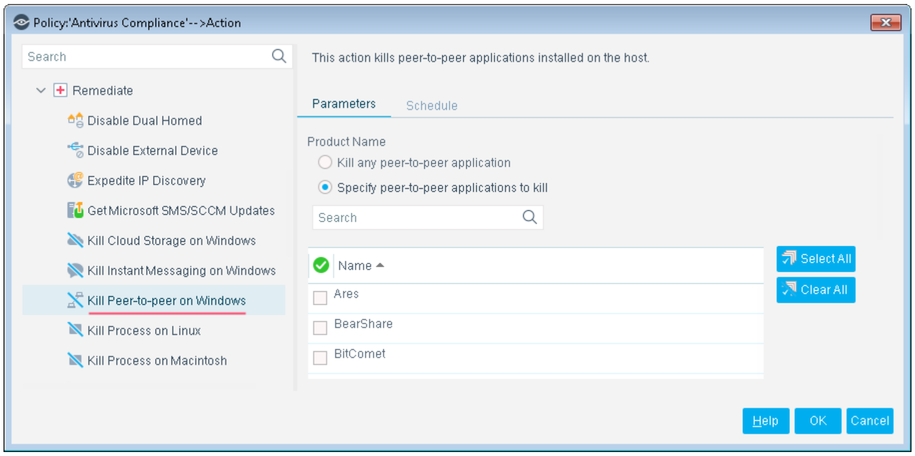
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

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, 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 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 Configuration Guide *for details about scripts.*

Kill Peer-to-Peer on Windows

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



Policy:'Antivirus Compliance'-->Action

Search

- Remediate
  - Disable Dual Homed
  - Disable External Device
  - Expedite IP Discovery
  - Get Microsoft SMS/SCCM Updates
  - Kill Cloud Storage on Windows
  - Kill Instant Messaging on Windows
  - Kill Peer-to-peer on Windows
  - Kill Process on Linux
  - Kill Process on Macintosh

This action kills peer-to-peer applications installed on the host.

Parameters | Schedule

Product Name

○ Kill any peer-to-peer application

● Specify peer-to-peer applications to kill

Search

✓	Name ▲
□	Ares
□	BearShare
□	BitComet

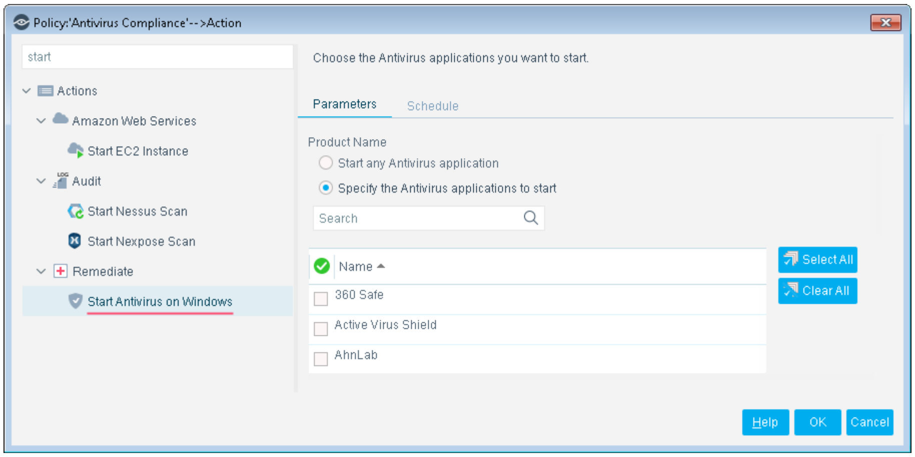
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

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, 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 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 Configuration Guide *for details about scripts.*

Start Antivirus on Windows

Launch antivirus applications that have been halted at Windows endpoints.



Policy:'Antivirus Compliance'-->Action

start

Choose the Antivirus applications you want to start.

Product Name

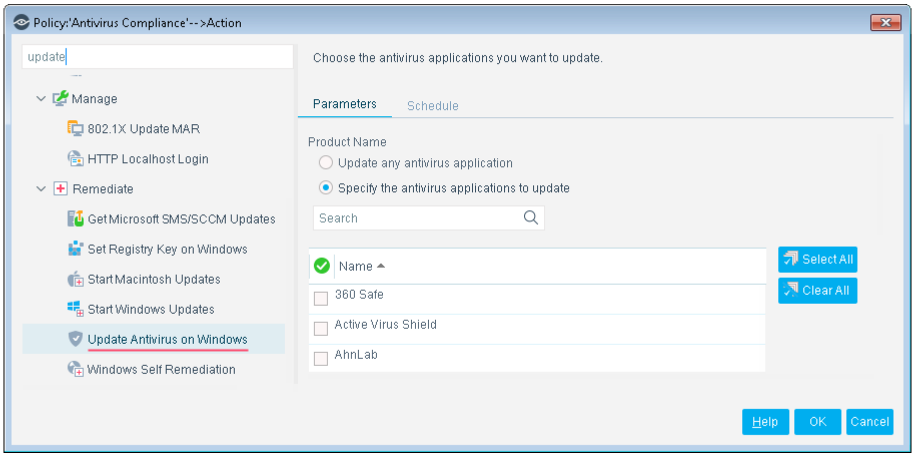
○ Start any Antivirus application

● Specify the Antivirus applications to start

✓	Name ▲
□	360 Safe
□	Active Virus Shield
□	AhnLab

Update Antivirus on Windows

Update outdated antivirus applications at Windows endpoints.



Choose the antivirus applications you want to update.

Product Name

○ Update any antivirus application

● Specify the antivirus applications to update

Name
□ 360 Safe
□ Active Virus Shield
□ AhnLab

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 Configuration Guide *for details about scripts.*

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
- Supported Windows Peer-to-peer Vendors
- Supported Windows Instant Messaging Vendors
- Supported Windows Anti-Spyware Vendors
- Supported Windows Personal Firewall Vendors
- Supported Hard Drive Encryption Applications
- Supported Cloud Storage Applications

Supported Windows Antivirus Vendors

Active Virus Shield
AhnLab
AVG/Avast
Avira
BitDefender
CA E-trust
ClamAV
Comodo
eScan
ESET
ESTsoft
F-Secure
G Data
Hauri
K7 Computing
Kaspersky
LANDesk
Lightspeed
McAfee
Microsoft
New Technology Wave
Panda
PC Ziggy
Qihoo 360
Rising
Sophos
Symantec
Trend Micro
Vipre

Supported Windows Peer-to-peer Vendors

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

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

🗎 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

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.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

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

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT 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.

CounterACT Administration Guide

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 **Modules**.
2. Select the plugin and then select **Help**.

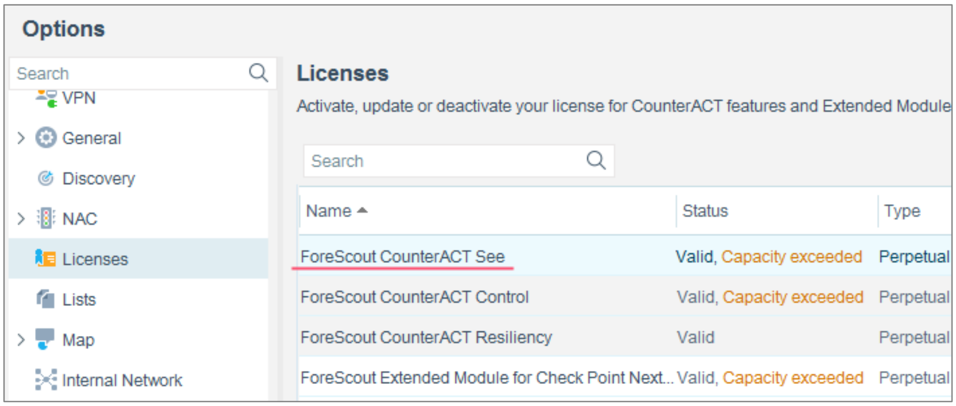
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21