CounterACT® HPS Inspection Engine
Configuration Guide

Version 10.6.0 and Above
# Table of Contents

## About the HPS Inspection Engine

- Requirements ................................................................. 4
- Supported Windows Operating Systems .......................... 5
- Accessing and Managing Windows Endpoints ................ 5
  - Remote Inspection ......................................................... 5
  - SecureConnector ......................................................... 6

## Configure the Plugin

- Configuration by Region or Appliance ............................ 7
- Troubleshooting Configuration ........................................ 7
- Access the Plugin Configuration Pane ............................. 7
- Remote Inspection ......................................................... 7
  - Domain Credentials .................................................... 8
  - General Remote Inspection Settings .............................. 9
- SecureConnector ........................................................ 11
  - Actions ......................................................................... 11
  - Detection ....................................................................... 12
  - Permanent SecureConnector Deployment Parameters .... 12
  - Additional Options ..................................................... 13
- Windows Updates .......................................................... 13
  - Distributing Vulnerability Information to Windows Endpoints 14
  - Using Windows Server Update Services (WSUS) or Windows Update 14
  - Windows Update Default Settings ................................. 15
- Classification ............................................................... 15
  - CounterACT Classification Version ............................... 16
  - Nmap Scan Options ..................................................... 17
- Tuning ........................................................................... 19
  - Specify Endpoint IP Addresses to Ignore ...................... 20
  - Tune HPS Inspection Engine Processes ....................... 20
  - Tune Nmap Processes .................................................... 20
  - Send HTTP Actions on SecureConnector Connect and User Login 21
  - HTTP Notification Action - Attempt to Open Browser at Endpoint 21
  - User Name Resolve Priorities ....................................... 22
  - Advanced Remote Inspection Configuration ................ 23
- Testing and Verifying Connectivity ................................ 23
  - Configuration for an Appliance or Group of Appliances ......................................................... 24
  - Apply Uniform Configuration Settings to All Appliances ......................................................... 25
  - Define a Configuration for a Single Device or Group of Devices ......................................................... 25

## Working with Remote Inspection

- About MS-WMI ............................................................. 26
- About Registry Service (MS-RRP) and Remote Procedure Calls (RPCs) 27
- About SMB ............................................................... 28
Detecting SMB Relay Behavior ................................................................. 28
Working with SMB Signing ................................................................ 29
About Kerberos .................................................................................. 30
Verify Managed Endpoints .............................................................. 30
Detecting Services Available on Endpoints ......................................... 30
Script Execution Services .................................................................. 31
About Secured Directories and Script Files ........................................... 32
About fsproccsvc.exe ........................................................................ 33
Microsoft Task Scheduler ................................................................... 33
Task Scheduler Limitations ................................................................. 34

Working with SecureConnector ............................................................ 34
How SecureConnector Works .............................................................. 35
Event Driven Monitoring of Host Properties ........................................ 36
Activating SecureConnector ................................................................. 36
SecureConnector Details ..................................................................... 36
Running the SecureConnector Executable ............................................. 37
SecureConnector ID ............................................................................ 38
SecureConnector Installation ............................................................... 39
Stopping SecureConnector From the Endpoint ....................................... 41
Restrict SecureConnector Access to the Appliance ................................. 42
Detecting NAT Behavior Based on SecureConnector Connections .......... 42
Resolving Dual-homed Endpoints Managed by SecureConnector .......... 43
Certificate Based Rapid Authentication of Endpoints ............................ 43

Appendix A: Executable Files Used by the Plugin ................................. 45

Appendix B: Troubleshooting the HPS Inspection Engine ................. 46
Operational Requirements ................................................................. 46
Testing the Domain Credentials .......................................................... 47
Testing the Credentials on a Desktop Using a Localhost Query ............ 47
Testing the Credentials on a Desktop Using Remote Query............... 48

Appendix C: SecureConnector Log Files ............................................. 54
Configure and Retrieve Log files – the fstool sc_config Command ....... 55

Appendix D: Remote Inspection and SecureConnector – Feature Support 56
Related Plugins .................................................................................. 60
User Accounts to Run Scripts on Managed Endpoints ......................... 60

Additional CounterACT Documentation ............................................. 61
Documentation Portal ......................................................................... 61
Customer Support Portal ................................................................. 61
CounterACT Console Online Help Tools ............................................. 61
About the HPS Inspection Engine

The HPS (Host Property Scanner) Inspection Engine allows CounterACT to:

- Access Microsoft Windows endpoints
- Apply Classification procedures to endpoints to determine their Network Function.
- Perform comprehensive, deep inspection for the purpose of resolving an extensive range of endpoint information, such as operating system details, Windows security, machine, services, application information and more.
- Use CounterACT actions to manage, remediate or control endpoints.

This document describes how to configure the plugin and provides other information including supported operating systems, executables and processes generated by the plugin, and troubleshooting issues.

If you are working with Mac OS or Linux endpoints, use the Macintosh/Linux Property Scanner Plugin and the OS X Plugin.

Plugin Updates

The plugin is bundled with major CounterACT releases. New releases may become available between major version releases. The Plugin Updates icon appears on the status bar of the Console when a plugin update is available.

Requirements

The plugin requires the following CounterACT releases and other CounterACT components.

- CounterACT version 7.0.0
- Service Pack 2.3.1 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- DNS Client Plugin 3.0.0
- Related functionality is provided by the following additional plugins:
  - HPS Applications Plugin – provides host properties and actions related to third-party Antivirus, Peer-to-peer, Anti-spyware, Personal Firewall, and Instant Messaging applications.
  - HPS NIC Vendor DB – provides host properties that map Network Interface Controllers to their vendors.
  - HPS Vulnerability DB – provides Microsoft vulnerability data and related updates.
Supported Windows Operating Systems

The HPS Inspection Engine can manage the following operating systems. 32-bit and 64-bit machines are supported.

- Windows XP Home/Professional/Tablet PC and embedded packages
- Windows Vista Home/Business/Enterprise/Ultimate
- Windows 7 Starter/Home/Professional/Enterprise/Ultimate
- Windows 8 Standard/ Professional/Enterprise
- Windows 8.1 Standard/ Professional/Enterprise
- Windows Server 2008 Standard/Enterprise/Datacenter/Web Server and core packages
- Windows Server 2012 Standard/Essentials/Foundation/Datacenter
- Windows 10 Home/Professional/Enterprise/Education/Enterprise LTSB

Accessing and Managing Windows Endpoints

The plugin accesses endpoints to learn detailed information such as applications and installed files, registry key information and more. In addition, the plugin is used to run scripts on endpoints to implement complex interactions with end users.

When you configure the plugin, you determine the methods you want to use to access and manage endpoints. When CounterACT successfully implements these access methods on an endpoint, the endpoint is resolved as Manageable by CounterACT.

The plugin provides the following methods to access endpoints:

- Remote Inspection
- SecureConnector

For an overview of features supported by Remote Inspection and SecureConnector, see Appendix D: Remote Inspection and SecureConnector – Feature Support.

Remote Inspection

Remote Inspection uses WMI and other standard domain/host management protocols to query the endpoint, and to run scripts. When you configure the plugin, you specify a set of protocols that are available in your environment, and CounterACT uses these to support detailed inspection, scripts, and other complex behaviors on all endpoints.

Agentless

Remote Inspection is agentless - CounterACT does not install any applications on the endpoint to query it. This makes Remote Inspection useful when administrators or end users do not want to install utilities or other executables on the endpoints.
Polling-Based Reporting
Remote Inspection periodically polls endpoints for endpoint property values. Polling frequency is determined by scheduled CounterACT policy rechecks.

Specify remote inspection settings in the Remote Inspection tab during plugin configuration. For more information, see Working with Remote Inspection.

SecureConnector
SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information to CounterACT, and implements scripts for authentication and other end-user interactions. The Start SecureConnector action installs SecureConnector on endpoints detected by a CounterACT policy.

Agent-Based
The SecureConnector executable file must be installed and maintained on the endpoint. This may not be acceptable in certain network environments, or for some endpoints or users. SecureConnector can be installed in several ways:

- As a permanent application
- As a permanent service
- As a dissolvable utility

Event Driven Reporting
SecureConnector continually checks host properties, and proactively sends updates to the HPS Inspection Engine only when it detects a change. This event-driven reporting eliminates latency in detecting changes on the endpoint, and helps reduce communications traffic between the HPS Inspection Engine and hosts. See Event Driven Monitoring of Host Properties for a list of monitored properties.

Specify SecureConnector settings in the SecureConnector tab during plugin configuration. Additional settings related to SecureConnector are in the Tuning tab. For more information, see Working with SecureConnector.

Configure the Plugin
You can configure the plugin to:

- Add or update Windows domain credentials
- Define general SecureConnector settings
- Define global options when working with the Start Windows Updates action
- Fine tune the Asset Classification mechanism
- Specify resolution methods and default values for various global parameters
- Specify test parameters and test connectivity
Configuration by Region or Appliance

By default, the settings defined for the HPS Inspection Engine are applied to all Appliances. If required, you can create separate configurations for each Appliance or for a group of Appliances in the same geographical region. See Configuration for an Appliance or Group of Appliances for details.

Troubleshooting Configuration

If you have configured the plugin but cannot access certain Windows endpoints or you see that deep inspection is not being carried out properly, see Appendix B: Troubleshooting the HPS Inspection Engine for details.

Access the Plugin Configuration Pane

To configure the plugin:

1. In the CounterACT Console, select Options from the Tools menu.
2. Select HPS Inspection Engine. Then select Configure.
3. Configure as required. If you are logged into the Enterprise Manager but want to configure all Appliances or a specific Appliance, make your selection from the Appliances drop-down list.
   
   The options in each of the tabs are described in the following sections.
4. Select Apply to save your changes.

Remote Inspection

Remote Inspection uses MS-WMI and other standard inspection/management protocols to manage endpoints. When you use Remote Inspection to manage endpoints, use this tab to configure how the plugin performs Remote Inspection.
Domain Credentials

Domain credentials are domain-level administrator privileges used by CounterACT to connect to network endpoints. Basic configuration of domain credentials is usually performed when setting up the CounterACT Console via the Console Initial Setup Wizard. For more information, see the CounterACT Installation Guide.

Although Domain Administrator privileges are not required for Remote Inspection, local machine administrator credentials are required. Any user account in the Local Administrators group of the endpoints has sufficient privileges to perform Remote Inspection on that endpoint. You may use a Domain Administrator account, but it is only necessary to define a domain account which exists in the Local Administrators group of endpoints in the relevant network segment.

Domain credentials defined during initial setup appear in the Domain Credentials table of the Default tab. For more efficient network communication, and to support networks with distinct regions or segments, you can define separate lists of domain credentials for Appliances or groups of Appliances. For example, you can create a list of credentials that are used by Appliances that monitor a specific network segment or regional subnet. The list of domain credentials defined during initial setup is used if none of the local-specific credentials succeeds. See Configuration for an Appliance or Group of Appliances.

Select Add to define new domain credentials, or Edit to modify existing credentials.

At least one set of administrator credentials must be defined.

The following options are available in the Add and Edit dialog boxes:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Administrator</td>
<td>The user name of an administrator account for endpoints that are handled by the plugin.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The Windows domain (name) to which managed endpoints belong. The administrator account must also belong to this domain. To authenticate endpoints, NTLMv2 requires a domain name in upper-case letters. To use Kerberos, enter the FQDN.</td>
</tr>
<tr>
<td>Domain Password</td>
<td>The password of the administrator account.</td>
</tr>
</tbody>
</table>
General Remote Inspection Settings

Define the following general settings:

Endpoint Remote Inspection method

Choose the protocol that the plugin uses to communicate with Windows endpoints. Options include:

- **Using MS-RRP** – The plugin interacts with the endpoint using remote procedure calls (RPCs) to the Windows Remote Registry Service (MS-RRP) on the endpoint.

- **Using MS-WMI** – The plugin uses only the Windows Management Instrumentation (WMI) service to interact with the endpoint. Because WMI does not support interactive scripts on all Windows endpoints, these scripts are implemented using the method you select in the Script Execution Method field.

- **MS-WMI with fallback to MS-RRP** - The plugin first tries to use the Windows Management Instrumentation (WMI) service to interact with each endpoint. If WMI services are not running on an endpoint, the plugin uses the Windows Remote Registry Service to interact with that endpoint.

See [Working with Remote Inspection](#) for more information about Remote Inspection options and the services that must be running on Windows endpoints.

When Remote Inspection uses MS-WMI, run scripts with

Choose the service the plugin uses to run scripts on the endpoint. Options include:

- **MS-WMI** – note that interactive scripts are not supported by WMI on all Windows endpoints. Functionality that relies on interactive endpoint scripts is not implemented when you choose this option. For example, the Start AntiVirus and Update AntiVirus actions require interactive scripts to manage some antivirus packages.

- **CounterACT fsprocsvc** – fsprocsvc is a proprietary ForeScout service utility downloaded by the plugin to endpoints. This utility is able to implement interactive scripts on endpoints.

When Remote Inspection uses MS-RRP, run scripts with

Choose the service the plugin uses to run scripts on the endpoint. Options include:

- **CounterACT fsprocsvc** - a proprietary ForeScout service utility downloaded by the plugin to endpoints.

- **Windows Task Scheduler** – this standard service launches scripts and other processes on most Windows platforms.

See [Script Execution Services](#) for more information about these options.

Authentication Method

Choose the protocol CounterACT uses to authenticate connections to endpoints for Remote Inspection. Options include:

- **Kerberos** - CounterACT uses the Kerberos servers installed in domain controllers of your environment. See [About Kerberos](#) for configuration details to support Kerberos.
- **NTLMv1 only** - this option is provided for backwards compatibility, but for security reasons it is not recommended.

- **NTLMv2 only** - for security reasons, CounterACT does not drop back to NTLMv1 when this option is selected.

For enhanced security, it is strongly recommended to use the NTLMv2 or Kerberos protocols for authentication.

> For security reasons, LMv2 responses are disabled by default. To enable use of LMv2 responses, change this setting in the Tuning tab of the HPS Inspection Engine configuration pane.

### Minimum SMB Protocol Version

SMB clients and servers negotiate the SMB version they will use. Choose the minimum SMB version that CounterACT uses to connect with endpoints.

When you configure this setting, you must balance between two considerations:

- The enhanced security provided by newer SMB versions
- The presence of endpoints in your network that run Windows versions with limited SMB support.

The following table summarizes SMB version support over recent Windows version history.

> Early Windows 10 and Windows Server 2016 previews used SMB dialect version 3.1.

<table>
<thead>
<tr>
<th>SMB Version</th>
<th>Earliest Windows Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB 3.1.1</td>
<td>Windows 10</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>SMB 3</td>
<td>Windows 8</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td>SMB 2</td>
<td>Windows Vista</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
</tr>
<tr>
<td>SMB 1</td>
<td>Previous versions</td>
</tr>
</tbody>
</table>

### Require SMB signing

When this option is selected, CounterACT requires digitally signed SMB communication for every new connection to an endpoint. When this option is cleared, CounterACT supports SMB signing but does not require it.

SMB signing is supported by most Windows endpoints; Microsoft has issued patches that support SMB signing on most legacy Windows versions. It is strongly recommended to enable this option to enhance security during Remote Inspection interactions. See [Working with SMB Signing](#).
SecureConnector

SecureConnector is a light footprint executable that can be run on endpoints to make them manageable by CounterACT. For more information about how SecureConnector works, see Working with SecureConnector.

The following SecureConnector configuration and deployment options are set from the SecureConnector tab of the plugin configuration screen.

- **Actions**
- **Detection**
- **Permanent SecureConnector Deployment Parameters**
- **Additional Options**

### Actions

**Automatically run SecureConnector when using the Disable External Device action**

The *Disable External Device* action disables external devices currently connected to the endpoint. This feature is supported only when SecureConnector is installed at the endpoint. Select this option to automatically install SecureConnector when the *Disable External Device* action is used.

**Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process and other Kill application actions**

The *Kill Process*, *Kill Instant Messaging* and *Kill Peer-to-peer* actions halt Windows processes related to these features. When SecureConnector is installed the process is killed once a second; if not, the process is killed once a minute. Select this option to automatically install SecureConnector and increase kill frequency (recommended).
Automatically run SecureConnector when using the Disable Dual Homed action

SecureConnector is required to implement the Disable Dual Homed action on endpoints. Select this option to install SecureConnector on endpoints that are not running it, when a policy applies the Disable Dual Homed action. When this option is not enabled, SecureConnector is not installed on endpoints that do not already run it, and the Disable Dual Homed action is not applied to these endpoints.

Show balloon messages at desktop

Select this option to display balloon messages generated by SecureConnector when the Disable External Devices, Kill Process, Kill Instant Messaging and Kill Peer-to-peer actions are performed. The message indicates which processes were killed.

Detection

Use SecureConnector to learn MAC address from local ARP tables

Select this option to instruct CounterACT to learn MAC addresses from the endpoint ARP table when the endpoint is managed by SecureConnector. This enables detection of endpoints that may be otherwise unreachable. When this option is cleared, other methods of MAC learning are used, for example from the Switch Plugin. This option is not available if SecureConnector is located behind a NAT address.

Permanent SecureConnector Deployment Parameters

This section describes options available when you deploy SecureConnector as a permanent application.

- You determine whether SecureConnector is deployed as a permanent service, a permanent application, or a dissolvable utility when you configure the Start SecureConnector action. See the Console User Guide or online help for details of this action.

Run SecureConnector before any other program

Select this option to run SecureConnector before any other desktop program is launched. It is recommended to launch SecureConnector before other programs to prevent other services or applications from blocking SecureConnector. This option is applicable when you install SecureConnector as a permanent application.

SecureConnector Password Protection

You can prevent users from uninstalling, exiting or stopping SecureConnector at the desktop by enforcing password access to these options. Type the password in the field. The password is limited to 24 characters.
**Additional Options**

This section of the tab includes other options for SecureConnector.

**Minimum supported TLS version**

Select the minimum TLS version that is accepted during TLS negotiation for SecureConnector communication.

- When you configure SecureConnector to require TLS version 1.1 or 1.2 to connect to an Appliance, the following versions of Windows cannot be managed by SecureConnector due to their TLS support limitations:
  - Windows XP
  - Windows Vista
  - Windows 2008 Server (pre-R2)

**Use FIPS compliant encryption**

When this option is enabled, SecureConnector communication uses encryption that complies with Federal Information Processing Standard (FIPS) requirements.

**Additional Appliance Connections**

Specify CounterACT devices that SecureConnector connects to when it cannot connect to the managing Appliance of the endpoint. SecureConnector first tries to connect to the Enterprise Manager that manages the Appliance, and then to the CounterACT devices listed here. Enter a comma-separated list of IP addresses. In most deployments, this list contains other Appliances managed by this Enterprise Manager.

**Windows Updates**

Specify parameters to use when scanning for vulnerabilities and installing missing updates. Scanning is activated when you create policies that use the Microsoft Vulnerabilities and Microsoft Vulnerabilities Fine-tuned properties, and the Start Windows Updates and Windows Self Remediation actions.
Distributing Vulnerability Information to Windows Endpoints

It may be more efficient for endpoints to retrieve vulnerability information from WSUS or Windows Updates, rather than use the information provided by the HPS Vulnerability DB. It is recommended to continue using WSUS or Windows Update in the following situations:

- When a local WSUS instance is deployed in your network environment.
- When endpoints are connected to your network through a VPN and are physically located at a distance from the Appliance, it may be faster for the endpoint to retrieve vulnerability information directly from the Microsoft Updates website or a local WSUS.

When they are available, you may use other methods to distribute the Microsoft Vulnerability CAB file to endpoints in your environment. The plugin looks for the following file on Windows endpoints:

%systemroot%\temp\wsusscn2.cab

If this file is different than the CAB file provided by the HPS Vulnerability DB, CounterACT downloads its own CAB file to the endpoint.

Refer to the HPS Vulnerability DB Configuration Guide for details of CAB file distribution by CounterACT.

Using Windows Server Update Services (WSUS) or Windows Update

This section describes how to configure CounterACT to work with vulnerability information retrieved directly from WSUS or Windows Updates.

To use vulnerability information from WSUS or Windows Updates:

1. In the Windows Updates tab, select Add. Enter a range of endpoint IP addresses that should retrieve vulnerability information directly from the Windows Updates website or a WSUS instance, depending on the configuration of the Windows endpoint.

Endpoints not included in the specified ranges receive vulnerability information from CounterACT using the HPS Vulnerability DB.

2. If a local WSUS instance exists, enter the URLs of the target WSUS server and WSUS report server in the WSUS Environment Settings area.

3. Select Apply to save changes. To test the server connection, select Test.

In large, geographically dispersed networks with several WSUS instances you can define settings for specific Appliances or groups of Appliances. See Configuration by Region or Appliance for details.

When a local WSUS instance is present and endpoints are configured to use WSUS, only vulnerabilities tracked by the local WSUS instance can be specified in CounterACT policy conditions. In this case, vulnerabilities of interest are determined
at the WSUS, and CounterACT policy conditions should detect endpoints with any vulnerability tracked by the WSUS instance. Configure policy conditions as follows:

1. In the CounterACT Console, select the **Policy** tab.
2. Use the search field to locate policies that use the **Microsoft Vulnerabilities** or **Microsoft Vulnerabilities Fine-tuned** host property.
3. For each condition based on these properties:
   - Add all currently listed vulnerabilities to the condition (**Add>Select All**).
   - Select the **Check new vulnerabilities automatically** checkbox.

The condition now checks for all vulnerabilities tracked by the WSUS instance associated with an endpoint.

**Windows Update Default Settings**

The following parameters can be configured in this section:

- Update method
- Maximum Concurrent Vulnerability DB File HTTP Uploads - You can minimize bandwidth usage during Microsoft vulnerability file download processes by limiting the number of concurrent HTTP downloads to endpoints. The default is 20 endpoints simultaneously.

**Classification**

This tab contains controls that determine how the plugin performs endpoint classification.

The HPS Inspection Engine powers CounterACT tools used for classifying assets. These tools include the classification engine that is part of the plugin, the Asset Classification and Mobile Classification templates, the **Classification** action, and Classification/Advanced Classification properties.

The classification engine attempts to identify the category of network asset to which each endpoint belongs. The **Network Function** property reports the results, sorting endpoints into the following categories:

- Windows devices
- Mobile devices
- MAC/OS X devices
- CounterACT devices
- Printers
- Servers
- Terminal Servers
- VoIP devices
- Network devices such as switches
- Unix servers/workstations
- Linux desktop/servers
- Network Address Translation (NAT) devices
Use classification policy templates and advanced properties to further refine these categories, or to classify devices into groups which are relevant to your deployment.

The HPS Inspection Engine uses several methods to retrieve information used for classification, such as: knowledge of domain credentials; analysis of HTTP and SMB banners; passive TCP/IP fingerprinting; information resolved on devices managed by CounterACT or switches configured to work with CounterACT; and Nmap scans. Nmap is typically a last resort when other methods do not yield sufficient information to classify an endpoint.

Information reported by other means during endpoint discovery or resolution of host properties is used to aid classification; similarly, information discovered by classification tools is used to populate relevant host properties.

CounterACT Classification Version

The set of methods used for classification in CounterACT evolves over time to include different tools and larger endpoint fingerprint databases. Choose the set of methods used to classify endpoints:

- Classification Version 2 is the default version and uses Nmap 5.21.
- Classification Version 3 uses Nmap 7.01 but otherwise relies on the same classification algorithms as Version 2. This version is recommended for all new deployments.

When you change this configuration setting, there may be significant changes in endpoint classification outcomes. See Upgrading the Classification Version.

Upgrading the Classification Version

When you change the set of classification methods used by CounterACT, there may be significant changes in the results of the plugin’s classification processes. These changes are evident when some endpoints receive new values for the Network Function and OS Fingerprint properties, and can strongly influence how classification policies evaluate endpoints.

Before you upgrade it is highly recommended to follow this procedure:

1. Create and run a policy based on the Classification Migration template. This policy detects endpoints for which the new and old classification methods yield different results.
Refer to the Console Online Help for details about the Classification Migration template.

2. Carefully analyze the endpoints which are classified differently by the two classification versions, especially these cases:
   - Endpoints classified correctly by classification version 2, but not classified at all under version 3
   - Endpoints classified correctly by classification version 2, but classified incorrectly under classification version 3

3. Decide how to handle changes in classification results. If necessary, adjust existing classification policies to ensure that all endpoints are correctly classified by classification version 3. You may need to create rules that use the **Classify** action to apply a desired classification to some endpoints.

You may also find that many endpoints which were not accurately classified by classification version 2 are now handled correctly by the improved capabilities of classification version 3. In these cases, you may be able to remove sub-rules that you inserted to correct automatic classification, simplifying classification policies.

**Nmap Scan Options**

The following options enable NMAP scanning for classification:

**Use Nmap Banner Scan**

When this option is selected, the plugin uses Nmap banner scans to improve the resolution of device services, application versions and other operating system details.

**Use Nmap Fingerprint Scan**

When this option is selected, the plugin uses Nmap fingerprint scans to resolve operating system and network function.
**Use Nmap results with low confidence level**

Typically the plugin must detect one open port and one closed port on an endpoint to implement an Nmap fingerprint scan. When this option is enabled, the plugin uses low-confidence Nmap estimates when it cannot detect the open and closed ports required for a full Nmap fingerprint scan.

**Nmap Scan Commands Used by the Plugin**

Nmap output is not logged. For troubleshooting purposes, the following Boolean properties may be set to enable recording of Nmap output. When these properties are enabled, corresponding log files are created in the plugin’s log file directory.

- **Nmap output logging consumes significant resources, and should only be enabled as needed for troubleshooting purposes.**

<table>
<thead>
<tr>
<th>Property</th>
<th>Equivalent Nmap Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>config.nmap_log_banners_normal.value</td>
<td>-oN : enables normal output</td>
</tr>
<tr>
<td>config.nmap_log_banners_xml.value</td>
<td>-oX : enables XML output</td>
</tr>
<tr>
<td>config.nmap_log_banners_grepable.value</td>
<td>-oG : enabled grep output</td>
</tr>
<tr>
<td>config.nmap_log_banners_all.value</td>
<td>Enables all output formats</td>
</tr>
</tbody>
</table>

To enable logging, log in as root to the Appliance that handles the range of IP addresses you wish to examine, and submit the following command:

```
fstool va set_property <config_property> true
```

where `<config_property>` is one of the Nmap logging configuration properties.

To disable logging, submit the following command:

```
fstool va set_property <config_property> false
```

**Banner Scan**

When the **Use Nmap Banner Scan** option is enabled, Nmap is used to scan endpoints using the following command line parameters:

```
-T Insane -sV -p T: 21,22,23,53,80,135,88,1723,3389,5900
```

**Fingerprint Scan**

When the **Use Fingerprint Scan** option is enabled, the following Nmap scans are implemented as needed for discovery and detection:

1. The endpoint is subjected to an initial Nmap scan of a small set of ports of interest. The following line parameters are passed to Nmap:

```
-T Insane -v -v -v -O -P 0 -p T: 80,9100,515
```

2. If the scan of the previous step does not yield enough information to classify the device, the plugin launches another Nmap scan with the same parameters, but against a greater range of ports:

```
T: 4,21,22,23,25,79,80,110,111,135,139,220,445,513,631,143,8080,41351,62078
```
Tuning

Use the settings in this tab to modify various global parameters and plugin behaviors.

### Tuning Options

- Specify Endpoint IP Addresses to Ignore
- Tune HPS Inspection Engine Processes
- Tune Nmap Processes
- Send HTTP Actions on SecureConnector Connect and User Login
- HTTP Notification Action - Attempt to Open Browser at Endpoint
- User Name Resolve Priorities
- Advanced Remote Inspection Configuration
Specify Endpoint IP Addresses to Ignore

The table lists endpoint IP addresses that are ignored when calculating the Number of IP Addresses host property.

- Select Add to add an IP address to the table.
- Select Edit to modify an address in the table.
- Select an entry in the table, then select Remove to delete it from the table.

Tune HPS Inspection Engine Processes

You can tune the number of Remote Inspection and SecureConnector processes that run concurrently on each Appliance to resolve endpoint properties. You can use automatic tuning or customize tuning.

**To enable automatic tuning:**

- Select the Dynamically scale concurrent HPS Inspection Engine processes based on available memory checkbox to enable automatic tuning of HPS Inspection Engine processes.

For each Appliance to which this setting applies, the maximum number of concurrent Remote Inspection and SecureConnector processes is determined dynamically as memory usage changes.

**To customize tuning (for advanced use only):**

- Deselect the Automatic Tuning for HPS Inspection Engine Processes checkbox.
  - Enter a value in the Concurrent RI HPS - Inspection Engine Processes field to set the maximum number of processes which communicate with endpoints managed by Remote Inspection that can be active at one time.
  - Enter a value in the Concurrent SC HPS - Inspection Engine Processes field to set the maximum number of processes which communicate with endpoints managed by Secure Connector that can be active at one time.

> Configuring a higher maximum value allows more concurrent endpoint connections, but consumes more Appliance resources. Tune these settings carefully. If Appliance performance is impacted, reduce these values.

Tune Nmap Processes

You can tune the number of concurrent Nmap processes that run on each Appliance. You can use automatic tuning or customize tuning. The following default maximum values are defined. The plugin selects a default value based on total Appliance memory.

<table>
<thead>
<tr>
<th>Available Memory</th>
<th>Default Concurrent Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 1 GB</td>
<td>5</td>
</tr>
<tr>
<td>Up to 2 GB</td>
<td>10</td>
</tr>
</tbody>
</table>
To enable automatic tuning:

- Select the **Set maximum concurrent Nmap processes based on Appliance specifications** checkbox to enable automatic tuning of Nmap processes.

  The plugin does not exceed the default maximum concurrent processes on each Appliance.

To customize tuning (for advanced use only):

- Deselect the **Automatic Tuning for Nmap Processes** checkbox. Enter a value in the **Concurrent Nmap Processes** field.

To limit Nmap ports:

In very rare instances, Nmap OS and banner scanning processes may cause storms of ACK messages. In such cases, select the **Limit source ports for Nmap scanning** checkbox. Nmap fingerprinting processes use source ports higher than 61000.

Send HTTP Actions on SecureConnector Connect and User Login

Start **HTTP Login**, **HTTP Notification** and **HTTP Redirection to URL** actions immediately after SecureConnector connection or user login events.

These actions have an **Attempt to open a browser at the detected endpoint** option. If this option is selected, the action tries to open a browser immediately, rather than waiting for the endpoint user to browse.

If the **Send HTTP actions on SecureConnector connect and user login events** option is not selected and the user is not logged in at the time that the action is issued, the HTTP message will not be displayed. With this option set, the message will be displayed when the user logs in or connects via SecureConnector.

HTTP Notification Action - Attempt to Open Browser at Endpoint

These options apply if the **Attempt to open a browser at the detected endpoint** option is selected in the Message tab of the **HTTP Notification** action.

**Open as Explorer Dialog Box**

Selecting this option causes the **HTTP Notification** action to open an Explorer dialog box rather than the default Web browser.

**Customize notification popup height / width (in % of screen size)**

These options let you customize the appearance of redirected HTTP notification pages when **Open as Explorer Dialog Box** is selected.
User Name Resolve Priorities

Several options are available for customizing the Device Information > User property resolution.

Learn endpoint user name from HTTP login

Instruct CounterACT how to learn endpoint user names. Three options are available:

- Always use HTTP login name when available. The name will be accessed when working with the HTTP Login action.
- Only use HTTP login name when machine user name is not available
- Only use machine login name

Use HTTP Login name when Sign In page is closed

Use this option to instruct CounterACT to use the HTTP login name when the HTTP sign in page is closed.

Resolve to last known username when no users are logged in to endpoint

When this option is selected, the last known username is used when the property cannot be resolved on an endpoint. When this option is cleared, the User property is evaluated as Irresolvable when no users are detected on the endpoint.
**Remember name for (hours)**

Use this option to instruct CounterACT for how long to remember the login name. This time is calculated from the last successful login.

**Learn endpoint user name from 802.1x authentication configuration**

In environments that use 802.1X authentication, there may be conflicts between the user/account information reported by the 802.1x Plugin and the HPS Inspection Engine. The **Learn endpoint user name from 802.1x authentication configuration** option gives priority to 802.1x user information.

When this option is selected, CounterACT ignores local user accounts that the HPS Inspection Engine discovers on an endpoint, and assigns the user name based on the supplicant user associated with the endpoint during 802.1x resolution.

**Advanced Remote Inspection Configuration**

When Remote Inspection is used, the plugin uses the NT LAN Manager protocol to authenticate its connection to endpoints for remote inspection.

The **Support LMv2 responses when using NTLMv2** option controls whether the plugin uses the less secure LMv2 authentication variant. It is recommended to only enable this option if backwards compatibility with LMv2 is required.

**Testing and Verifying Connectivity**

In the Test tab, specify parameters used for connectivity testing.

The following options are available:

<table>
<thead>
<tr>
<th><strong>Test Address</strong></th>
<th>A test IP address. Depending on the test type, the address can be used to verify:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>▪ Connectivity to the domain name, administrator and password.</td>
</tr>
<tr>
<td></td>
<td>▪ Remote registry connection.</td>
</tr>
<tr>
<td></td>
<td>▪ CounterACT identifies a running Windows service.</td>
</tr>
<tr>
<td></td>
<td>It is recommended to use an address that grants permissions and access to your entire network, for example the domain controller or the LDAP server.</td>
</tr>
</tbody>
</table>
Connectivity Test Type

Specifies whether to test connectivity via SNMP or SMB/RPC. If you are testing via SNMP, you must enter the SNMP access parameters listed below.

(SNMP Test Parameters) OID

The OID number to test.

(SNMP Test Parameters) Community

The community name to test.

(SNMP Test Parameters) Extra Parameters

This option controls the SNMP retry and timeout requests. You may need to use this to handle SNMP timeout problems. These problems may occur if the network is extremely busy.

- **Timeout** – The number of seconds to wait for a response. The default timeout is 25 seconds.
- **Retry** – The number of times to retry sending an SNMP message. The default number of retries is 1. The upper limit is 20.

For example, to indicate a timeout of five seconds and three retries, enter the following:

- \( t \ 5 \ -r \ 3 \)

### Configuration for an Appliance or Group of Appliances

You can create and apply plugin configurations for individual Appliances, or for a group of Appliances.

Configurations are organized using a row of tabs. *Each tab duplicates all the configuration fields in the pane.*

Initially, only the Default tab is present. In the following example, an additional tab has been added, with the configuration for a specific Appliance.

Use the following controls to create and manage configurations:

- Select the Plus-sign tab to create a new configuration.
- When there are several configurations, it may be difficult to locate the configuration that applies to a specific device. Select the device from the CounterACT Devices drop-down. The configuration that applies to that device is highlighted for editing.
Apply Uniform Configuration Settings to All Appliances

The settings of the Default tab apply to all CounterACT devices that are not included in other configurations. If you do not create other configurations, these settings apply to all CounterACT devices.

Define a Configuration for a Single Device or Group of Devices

Use this procedure to define configuration settings that apply to a specified CounterACT device or group of devices.

To create a configuration for a device or group of devices:

1. Select the Plus-sign tab. The Select CounterACT devices to configure dialog box opens.

2. Select the CounterACT devices to which this configuration will apply.

3. (Optional) Specify a text label for this configuration in the Name (Optional) field.

4. Select OK. A new tab appears in the pane.

Configuration settings you define while this tab is selected apply only to the CounterACT devices you selected in step 2.

To modify the scope of a configuration:

1. Select the Edit icon on a tab. The Edit devices to configure dialog opens.

2. Edit the devices to which this configuration applies:
   - Select devices to add to the configuration.
   - Clear selected devices to remove them from the configuration.

3. (Optional) Modify the text label of the configuration.
4. Select **OK** to save changes to the configuration.

**To delete a configuration:**

1. Select the Delete icon × on a tab.
2. Select **Yes** to confirm deletion.

   The configuration tab is removed from the pane.

> Settings of the Default tab now apply to all devices that were in the scope of the deleted configuration.

---

**Working with Remote Inspection**

Remote Inspection uses WMI and other standard domain/host management protocols to query the endpoint, and to run scripts.

Support for WMI and other protocols can vary depending on how they are implemented in the general network environment. When you configure the plugin, you specify a set of standard protocols that are available in your environment, and CounterACT uses these to support detailed inspection and to run scripts.

Individual endpoints may not support some features, or may require additional configuration steps due to their operating system or other configuration settings.

This section describes the Windows protocols and services that support Remote Inspection. For an overview of features supported by Remote Inspection and SecureConnector, see Appendix D: Remote Inspection and SecureConnector – Feature Support.

**About MS-WMI**

Windows Management Instrumentation is a Microsoft tool for web based enterprise management. CounterACT can use WMI to inspect endpoints, and to run background scripts on endpoints.

**Basic Requirements**

To use WMI on a Windows endpoint, verify the following settings:

- Port 135/TCP must be available for WMI communication.
- The following services should be running:
  - Server
  - Windows Management Instrumentation (WMI)
- WMI communication must be enabled in network firewalls.
Additional Configuration/Troubleshooting Options

Verify/implement the following configuration settings to work with WMI.

1. Configure the following Active Directory settings. You can configure some of these settings on endpoints using a Group Policy.
   - Member of Domain Administrators or Local Administrators group
   - Member of the following domain groups:
     - Performance Log Users
     - Distributed COM Users
   - Member of a group with the following permissions:
     - Act as part of Operating System
     - Log on as a batch job
     - Log on as a service
     - Replace a process

2. If the CounterACT fsprocsvc utility will be used to run scripts on endpoints, the Windows Remote Registry Service must be running on endpoints.

3. Run the dcomcnfg utility and configure the following endpoint permissions:
   - Access Permissions: Enable all
   - Launch and Activation Permissions: Enable all

4. Run the wmic.msc utility and configure WMI namespace security settings.
   Assign permissions to the following namespaces:
   - root\CIMv2
   - root\Default
   - root\SecurityCenter
   - root\SecurityCenter2
   Assign the following permissions to each of the namespaces:
   - Execute Methods
   - Enable Account
   - Remote Enable
   - Read Security

About Registry Service (MS-RRP) and Remote Procedure Calls (RPCs)

CounterACT can submit a Remote Procedure Call (RPC) to the registry services of a Windows machine to inspect the endpoint, or to run scripts. To use RPCs on a Windows endpoint, verify the following settings:

- On endpoints running Windows 7 and above, Port 445/TCP must be available. On earlier versions of Windows, port 139/TCP must also be available.
- The following services should be running:
  - Server
CounterACT® HPS Inspection Engine  Configuration Guide

− Remote Procedure Call
− Remote Registry

CounterACT provides safeguards against SMB Relay behavior in Remote Procedure Calls. See Detecting SMB Relay Behavior.

About SMB

Server Message Block (SMB) is a protocol for file and resource sharing. CounterACT uses this protocol with WMI or RPC methods to inspect and manage endpoints. This protocol must be available to perform the following:

- Resolve file-related properties
- Resolve script properties
- Run script actions

To use SMB on a Windows endpoint, verify the following settings:

- On endpoints running Windows 7 and above, Port 445/TCP must be available. On earlier versions of Windows, port 139/TCP must also be available.
- The Server service must be running.
- Local hard drives must be shared: file and printer sharing must be enabled for the network adapter.

Detecting SMB Relay Behavior

SMB relay attacks exploit challenge-response authentication of the SMB protocol to allow an endpoint to capture authentication information. This method of attack is similar to Pass-the-Hash and other Man-in-the-Middle attacks.

When CounterACT establishes a new RPC connection to an endpoint, it performs tests to determine if the endpoint is a relay. If relay behavior is detected:

- The connection is no longer used by CounterACT.
- The **SMB Relay** property is set to **True**.
- The **Windows Manageable Domain** and **Windows Manageable Domain (Current)** properties are set to **False**.
- Host properties that are resolved using RPC are set to **Irresolvable**. This includes the following properties:
  - Several properties in the Device Information folder of the Condition tree.
  - Related properties in the Track Changes folder of the Condition tree.
To modify handling of SMB relays:

1. Log in to the Appliance and submit the following command:

   `fstool va set_property <property_name> <property_value>
   
   Where <property_name> and <property_value> are taken from the following table, as desired.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Property Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>config.verify_smb_relay.value</td>
<td>0 - No testing of RPC connections.</td>
</tr>
<tr>
<td></td>
<td>1 – (default) CounterACT tests every new RPC connection for SMB relay behavior.</td>
</tr>
<tr>
<td>config.response_err_if_smb_relay.value</td>
<td>0 - Resolve properties as for normal endpoints.</td>
</tr>
<tr>
<td></td>
<td>1 – (default) Set all RPC related properties to Irresolvable for SMB relay endpoints.</td>
</tr>
</tbody>
</table>

2. Restart the HPS Inspection Engine.

3. Repeat this procedure on each Appliance.

Working with SMB Signing

SMB Signing is an optional feature that secures SMB communication with a digital signature. SMB Signing is useful to help identify SMB Relay behavior and prevent man-in-the-middle attacks.

Use the **Require SMB Signing** option on the **Remote Inspection** tab to configure whether CounterACT requires SMB signing for communication with endpoints.

SMB signing is supported by most Windows endpoints; Microsoft has issued patches that support SMB signing on most legacy Windows versions. It is strongly recommended to enable this option to secure Remote Inspection interactions.

When you enable this option, an endpoint that can perform SMB signing will use SMB signing when they communicate with CounterACT.

When you require SMB signing, CounterACT can no longer use Remote Inspection to manage endpoints that cannot work with SMB signing, for example:

- Old Windows XP / Server 2003 systems that are not patched/up to date
- Endpoints behind WAN optimization devices that require unsigned SMB packets.

Create a policy that uses the **SMB Signing** host property to detect these endpoints and remediate them. Remediation options include:

- (Recommended) Enable SMB signing on all endpoints. Use Group Policies to configure SMB signing as described by the following Microsoft support article: [https://support.microsoft.com/en-us/kb/887429](https://support.microsoft.com/en-us/kb/887429)
- Use the **Start SecureConnector** action to install SecureConnector on endpoints that do not support SMB signing.
About Kerberos

Kerberos is a network authentication protocol that uses secret-key cryptography. When you choose Kerberos authentication, CounterACT interacts with Kerberos authentication servers deployed in your environment (typically on existing Active Directory instances).

When CounterACT uses Kerberos authentication for Remote Inspection, a dedicated administrator account should be defined in the domain controller and entered in the **Domain Credentials** tab. The HPS Inspection Engine uses this account to interact with Kerberos servers, and to perform Remote Inspection on endpoints. In accordance with Kerberos best practices, delegation permissions should be disabled for this user.

CounterACT uses hostnames for Kerberos authentication. To use Kerberos to authenticate endpoints, verify that:

- All Domain Credentials defined in the Remote Inspection tab are defined using their FQDN (Fully Qualified Domain Name).
- CounterACT is able to perform forward and reverse DNS resolutions of Windows endpoints. If an endpoint’s hostname is unknown, CounterACT performs a reverse DNS query to determine the hostname.
  
  Similarly, ensure that DNS records are regularly updated in your environment to support DNS queries.

Verify Managed Endpoints

Use the following command at the CounterACT Appliance command line interface to verify that an endpoint is properly responding to remote inspection methods.

```
fstool va_test -h <host_ip> -c manage
```

For a managed endpoint, the test response should resemble the following example.

```
# fstool va_test -h 10.0.0.123 -c manage
Testing host[10.0.0.123] cmd[manage]
  Testing user[counteract] domain[FSD]
  wmi_success[1]
```

Detecting Services Available on Endpoints

The following host properties provide detailed information about the Remote Inspection methods available on an endpoint.
The following Boolean properties are listed in the Properties tree under the Remote Inspection folder:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-RRP Reachable</td>
<td>Indicates whether CounterACT can use the Remote Registry Protocol for Remote Inspection tasks on the endpoint.</td>
</tr>
<tr>
<td>MS-SMB Reachable</td>
<td>Indicates whether CounterACT can use the SAMBA protocol for Remote Inspection tasks on the endpoint.</td>
</tr>
<tr>
<td>MS-WMI Reachable</td>
<td>Indicates whether CounterACT can use the Windows Management Interface for Remote Inspection tasks on the endpoint. In previous releases, this property was named Windows Manageable Domain by WMI.</td>
</tr>
</tbody>
</table>

These properties do not have an *Irresolvable* state. When the plugin cannot establish connection with the service, the property value is *False*. Do not use the **Evaluate Irresolvable Criteria as** option with these properties.

The following corresponding Track Changes policies are listed under the Track Changes folder:

- MS-RRP reachability changed
- MS-SMB reachability changed
- MS-WMI reachability changed

## Script Execution Services

This section describes the services that CounterACT uses to execute scripts on endpoints. PowerShell scripts and all common script file types are supported. The prefix `cscript` is added to files with the `.vbs` file extension.

- *CounterACT cannot run PowerShell scripts when the PowerShell Execution Policy is set to Restricted on the endpoint. See PowerShell documentation.*
- *When SecureConnector is installed on an endpoint, it is used to run scripts.*
- *If you choose to use WMI for Remote Inspection, CounterACT runs most background scripts run using WMI. However, WMI does not support interactive scripts (such as scripts that support Guest Registration and other HTTP-based actions) on all Windows endpoints. CounterACT uses the services described here to run these interactive scripts.*
When WMI is used for Remote Inspection, scripts that reside at another network location cannot be run on endpoints due to Windows security features.

By default, scripts are downloaded to and run from the following locations on Windows endpoints:

- On endpoints managed by SecureConnector:
  - When SecureConnector is deployed as a Service, all scripts are downloaded to and run from the following secured directory:
    \%TEMP\fstmpsc\%
    Typically \%TEMP\ is c:\windows\temp\%
  - When SecureConnector is deployed as a Dissolvable or Permanent Application, all scripts are downloaded to and run from the \%TEMP\ directory of the currently logged in user.

  If the **Start SecureConnector** action was used to install SecureConnector when no user was logged in, SecureConnector initially runs in the system context, and scripts are downloaded and run as described for deployment as a Service. For SecureConnector deployed as a Permanent Application, the next time SecureConnector is run, it runs from the logged-in user context, and scripts are downloaded to and run from the \%TEMP\ directory. For more information about the Install as system option of the **Start SecureConnector** action, see the Console User Guide.

- On endpoints managed by Remote Inspection:
  - Non-interactive scripts are downloaded to and run from the following secured directory:
    \%TEMP\fstmp\%
    Typically \%TEMP\ is c:\windows\temp\%
  - Interactive scripts are downloaded to and run from the \%TEMP\ directory of the currently logged in user.

You can use the following configuration property to customize the directory used to download and run scripts:

```plaintext
cfg.config.script_run_folder.value
```

It is strongly recommended to specify a secured directory.

**About Secured Directories and Script Files**

Because scripts that run on endpoints can be targets for malicious attack, CounterACT creates the /fstmp and /fstmpsc directories it creates with ACL permissions that prevent unauthorized modification of script files. When scripts run in the user context, or when you customize the target directory, scripts may be vulnerable to attack. It is recommended to specify a folder with secured access.

You can add an additional layer of security by applying ACL permissions to the script file itself to prevent unauthorized modification.
About fsprocsvc.exe

The fsprocsvc.exe service, installed on endpoints by the HPS Inspection Engine, is used to run interactive scripts for several CounterACT tasks. It is a ForeScout service similar to Microsoft's PsTools (Part of Windows Sysinternals tools: http://technet.microsoft.com/en-us/sysinternals/default.aspx).

To download and run this service, the Windows Remote Registry Service must be running on the endpoint.

The service is downloaded to, and runs from, the folder used by the HPS Inspection Engine to run scripts.

The service does not open any new network connection or generate traffic. Communication is carried out over Microsoft's SMB/RPC (445/TCP and 139/TCP) and the authentication is performed with the domain credentials. If there is no request to run a new command within two hours, the service stops automatically.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Footprint | • Size on disk: Approximately 250KB  
• Memory acquired during runtime: 2 MB  
• Runs under: System  
• Start type: Automatic  
• After 2 hours of inactivity the service stops |

Properties requiring the service (With remote inspection, i.e. not via SecureConnector)

- Windows Expected Script Result
- Device Interfaces
- Number of IP Addresses
- External Devices
- Windows File MD5 Signature
- Windows Is Behind NAT
- Microsoft Vulnerabilities

Actions requiring the service (With remote inspection, i.e. not via SecureConnector)

- Run Script On Windows
- HTTP Redirection to URL (If Attempt to open a browser at the detected endpoint is selected)
- Start SecureConnector
- Set Windows Registry Key
- Start Antivirus
- Update Antivirus
- Start Windows Updates
- Kill Process on Windows, Kill Instant Messaging, Kill Peer-to-peer

Microsoft Task Scheduler

An option is available to work with Microsoft Task Scheduler, rather than with fsprocsvc.exe.

Task Scheduler is a component of Microsoft Windows that lets user schedule the launch of programs or scripts at pre-defined times or after specified time intervals. This utility can be used to run CounterACT scripts.
Task Scheduler Limitations

- Requires the relevant service to be started on the endpoint.
- Interactive tasks do not work on Windows Vista and Windows 7 if the remote process is triggered from Task Scheduler.
- The *Update Antivirus* action does not work on Windows Vista and Windows 7 if the HPS remote inspection is configured to work as a "Scheduled Task".
- Opening a browser window does not work on Windows Vista and Windows 7 if the HPS remote inspection is configured to work as a "Scheduled Task". When redirected with this option checked, the browser does not open automatically and relies on the packet engine seeing this traffic.
- On Windows Vista and Windows 7 configurations, SecureConnector via remote inspection is invisibly installed if the HPS remote inspection is configured to work as a *Scheduled Task* and SecureConnector is set to be visible.

Working with SecureConnector

SecureConnector is a light footprint executable that runs on the endpoint to make endpoints manageable, and to perform or optimize certain actions.

SecureConnector is also available when working with Mac OS X and Linux endpoints. Refer to the *Macintosh/Linux Property Scanner Plugin Configuration Guide* and the *OS X Plugin Configuration Guide* for details.

Making Windows Endpoints Manageable

You can use SecureConnector to access Windows endpoints and make them manageable for deep inspection. In general, Windows endpoints are unmanageable if their remote registry or file system cannot be accessed by CounterACT. This is typical for:

- Machines that are guests on the network
- Endpoints that are not part of the domain

Several policy properties are available for detecting *unmanageable* endpoints.

To work with SecureConnector, Windows endpoints must be running MS-WMI (Windows Management Instrumentation).

Performing or Optimizing Certain Actions

SecureConnector is required to perform the following actions on endpoints:

- **Assign to VLAN** behind VoIP devices without resetting port
- **Disable External Device**
- **Send Balloon Notification**
- **Disable Dual Homed**
SecureConnector can be used to improve kill frequency when working with the following actions:

- **Kill Cloud Storage on Windows**
- **Kill Instant Messaging on Windows**
- **Kill Peer-to-peer on Windows**
- **Kill Process on Windows**

These actions detect and halt specific Windows processes. If the endpoint has SecureConnector installed the actions run once per second; if not, the actions run once per minute.

**How SecureConnector Works**

SecureConnector creates a secure (encrypted TLS) connection to the Appliance through port 10003. SecureConnector receives inspection and action requests and responds to them via this connection; all CounterACT traffic between SecureConnector and the Appliance goes via the secure connection.

When an endpoint is reassigned to another Appliance, the secure connection is seamlessly re-created between the endpoint and the newly assigned Appliance.

**Permanent vs. Dissolvable Deployment**

SecureConnector can be configured to run once and terminate itself upon user logout, reboot, or disconnection from the network, and then reopen at reconnection to the network and readmission to the relevant policy. This is called *dissolvable* installation.

Alternatively, it can be configured to install permanently so that it remains at reboot or disconnection; in this case it can be removed via the uninstall option in the Windows **Start>Programs** menu.
Event Driven Monitoring of Host Properties

When SecureConnector is installed on a host, it continuously monitors host properties and only reports changes to CounterACT. Event driven monitoring significantly reduces network traffic, and provides the most updated information without policy rechecks.

Host properties that are updated using event-driven monitoring are listed in Appendix D: Remote Inspection and SecureConnector – Feature Support.

Activating SecureConnector

SecureConnector is powered by the HPS Inspection Engine, but downloaded to endpoints using the Start SecureConnector action. Installation, visibility and other options can be configured when defining the action. Navigate to the Working with Actions page in the online Help for details.

In addition, you can distribute SecureConnector to endpoints by downloading an installation file from an Appliance, and then distributing the file. See SecureConnector Installation for details.

You can use SecureConnector log files to troubleshoot SecureConnector issues. See Appendix C: SecureConnector Log Files.

SecureConnector Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size on disk</td>
<td>Approximately 2 MB</td>
</tr>
</tbody>
</table>
| Endpoint memory utilization | **Process mode:**
  ▪ Main process: 3MB – 6MB
  ▪ Watchdog process: 400kB – 600kB
  **Service mode:**
  ▪ Agent process: 3 MB – 5 MB
  ▪ Performer process: 4 MB – 6 MB
  ▪ Service: 3 MB – 5 MB |
| Deployment type             | Permanent or dissolvable. Defined in the Start SecureConnector action.       |
| Visibility options          | Visible (Icon in System tray) or non-visible Defined in the Start SecureConnector action |
| Installation methods        | ▪ Using Remote inspection methods
  ▪ Browser – direct setup file download. Described in this guide. See Activating SecureConnector. |
<p>| SecureConnector privilege level | Ideally, SecureConnector should be installed as a service on corporate endpoints. This ensures that all SecureConnector related features will be available irrespective of the user logged on to the machine. |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When SecureConnector is installed as a service, it runs with Administrator privileges even when the current logged in users are not administrators. When SecureConnector is installed as an application, privileges are determined by the user currently logged in, even if a user with administrator privileges was used to install SecureConnector. The following actions will not work if the user currently logged in does not have administrator privileges:</td>
<td></td>
</tr>
<tr>
<td>‣ Disable External Devices</td>
<td></td>
</tr>
<tr>
<td>‣ Kill Process (for processes that do not belong to the SecureConnector user)</td>
<td></td>
</tr>
<tr>
<td>‣ Disable Dual Homed</td>
<td></td>
</tr>
<tr>
<td>Privilege levels are determined in part by the mode in which SecureConnector is installed. The mode is determined when configuring the Start SecureConnector action. When User Account Control (UAC) is active, it prevents SecureConnector installation from modifying specific system critical folders such as Program Files. However, SecureConnector can be installed to the user home folder, where it has all user privileges.</td>
<td></td>
</tr>
<tr>
<td>Installation folder when installed permanently</td>
<td></td>
</tr>
<tr>
<td>%ProgramFiles% if setup runs with Administrator (or SYSTEM) privileges. %USERPROFILE%\Application Data if setup runs with non-Administrator privileges or setup is affected by UAC.</td>
<td></td>
</tr>
<tr>
<td>Folder used when deployed in dissolvable mode</td>
<td></td>
</tr>
<tr>
<td>%Temp% if runs with Administrator (or SYSTEM) privileges %USERPROFILE%\local settings\Temp if setup runs with non-Administrator privileges or setup is affected by UAC.</td>
<td></td>
</tr>
</tbody>
</table>

### Running the SecureConnector Executable

SecureConnector.exe, activated by the HPS Inspection Engine, runs on Windows endpoints. Activation occurs when the Start SecureConnector action is chosen or when SecureConnector is otherwise installed. See Appendix C: SecureConnector Log Files for details.

Changes to the executable are reported in the release notes for this plugin.

SecureConnector can run as an application or as a service, depending on how it is installed. Installation options are defined when running the Start SecureConnector action. When run as a service, the ForeScout SecureConnector service appears at the endpoint’s Services window. The service is started in automatic mode.
When SecureConnector is installed as a service, several processes run and can be seen from the endpoint Task Manager.

In the example shown above there are three SecureConnector.exe processes:

- One SecureConnector.exe process manages communication with the CounterACT Appliance.
- One SecureConnector.exe process is responsible for the user interface (such as Systray icon, View Compliance Center).
- One SecureConnector.exe process is the SecureConnector service. (If SecureConnector is installed as an application then this process does not appear and SecureConnector only uses two processes.)

The fsprocsvc.exe process may appear briefly in Task Manager when it is used to install SecureConnector.

**SecureConnector ID**

When SecureConnector connects to the CounterACT Appliance, it sends CounterACT a unique ID. This ID is used to help identify the endpoint and may cause CounterACT to perform an identity change if one of the following events occurs:
The current IP address was used by another machine – This occurs if another SecureConnector ID was learned for this IP address. If another endpoint with SecureConnector previously used the same IP address, then the system will conclude this is a new machine, will delete all previous information and will relearn the properties from the new machine.

The current machine previously used another IP address – This occurs if this SecureConnector ID was learned on another IP address. If this endpoint previously used another IP address then all the information learned on the older IP address will be moved to the new IP address (The old IP address will be changed to the new one).

SecureConnector Installation

You can distribute SecureConnector to endpoints by downloading an installation file from an Appliance, and then distributing the file via:

- Wide, automatic distribution via Windows login script or domain group policy – an advantage to this method is that installation is silent.
- Distribution to specific endpoints via a link in email.
- Distribution to specific endpoints via a file on a USB stick.
- Any third-party distribution tool.

You can also obtain a link from an Appliance and send that via email or another method to specific endpoints; when a user clicks the link, a SecureConnector installation file is automatically downloaded to the endpoint.

Each endpoint automatically connects to the Appliance to which it is assigned, even if the installation file is downloaded from a different Appliance. However, the initial connection will always go via the Appliance that the file was downloaded from thus placing a momentary load on that Appliance.

After distribution, it is recommended to set up a policy to verify that SecureConnector installation was successful at the intended endpoints.

In addition to the standard file distribution method described here, the Start SecureConnector action can be used to install SecureConnector on endpoints selected by policy conditions.

To distribute SecureConnector via file or link to endpoints:

1. Browse to the following location:

   http://<Appliance_IP>/sc

   where <Appliance_IP> is the IP address of Enterprise Manager or an Appliance. The ForeScout SecureConnector Distribution Tool page opens.
2. Define SecureConnector settings (described above).
   - Whether to place an icon on the endpoint systray.
   - How to install SecureConnector on the endpoint:
     - As a dissolvable utility
     - As a permanent application
     - As a permanent service

4. Specify whether the SecureConnector agent is for 32-bit or 64-bit system. Select **Download** to download the SecureConnector installation file, or copy the link at the bottom of the window. Do not change the file name or the link path.

5. Send the file or link to desired endpoints via login script, email or any other method.
   - If the file method is used, instruct the user to double-click the file to install.
     When SecureConnector is installed as a *Permanent Service* or a *Permanent Application*, a popup notification message indicates installation success or failure.
   - If the link method is used, instruct the user to select **Run** when prompted, so that the installation file will automatically download and run.

6. Create a policy that uses the **Windows Manageable (SecureConnector)** property to verify that SecureConnector is installed on target endpoints.

**Stopping SecureConnector From the Endpoint**

By default, end users can stop SecureConnector on their devices by doing one of the following:

- Open a command-line window and issue the following command:
  
  ```
  SecureConnector.exe -uninstall
  ```
  A message box indicates successful uninstall. To suppress this message, use this form of the command:
  
  ```
  SecureConnector.exe -uninstall -silent
  ```

- When the SecureConnector toolbar icon is visible, right-click the icon, then select **Exit**. SecureConnector stops, but is not uninstalled.

![View Compliance Center](image)

When you [configure the plugin](#) you can enable password protection for SecureConnector on endpoints. When password protection is enabled, users who try to **Exit** SecureConnector are prompted for a password.

![ForeScout SecureConnector](image)
Restrict SecureConnector Access to the Appliance

By default, all endpoints with the SecureConnector executable connect to their managing Appliance using SecureConnector, and are managed by SecureConnector. You can configure the Appliance to only accept a SecureConnector connection from specified ranges of endpoints – thereby forcing management of all other endpoints by Remote Inspection, even if they have the SecureConnector executable.

To restrict access to the SecureConnector service by IP address

1. Log in to the Appliance.
2. Issue the following command:
   
   `fstool va set_property config.va_port_val.value "<IPs>"`

   where `<IPs>` is a comma-separated list of individual IPv4 addresses or subnet/masks that can access the SecureConnector service on the Appliance. For example, the following command limits SecureConnector access to subnets of two Class C addresses:

   `fstool va set_property config.va_port_val.value "192.185.100.1/20, 192.180.100.1/255.255.255.0"`

3. Restart the HPS Inspection Engine.
4. Repeat this procedure on each Appliance to restrict access to its SecureConnector service.

Detecting NAT Behavior Based on SecureConnector Connections

To detect endpoints that are NAT devices, CounterACT can examine the IP addresses used by endpoints to connect to SecureConnector on Appliances. After an endpoint connects to SecureConnector the plugin uses SecureConnector to learn the IP address of the endpoint. If the IP address found by SecureConnector does not match the IP address at the source of the TCP socket connection, the Device is NAT host property is resolved as True for the endpoint.

By default, this check is not enabled. The `conf.report_nat_device_sc.value` property of the relevant plugin controls this behavior.

To enable or disable NAT detection in SecureConnector connections:

1. Log in to the Enterprise Manager as root.
2. To enable NAT detection, submit the following commands:

   `fstool va set_property config.report_nat_device_sc.value true`
   `fstool oneach fstool va set_property config.report_nat_device_sc.value true`

   From the Console, restart all instances of the plugin.
3. To disable NAT detection, submit the following commands, as relevant:

```
fstool va set_property config.report_nat_device_sc.value false
fstool oneach fstool va set_property
config.report_nat_device_sc.value false
```

From the Console, restart all instances of the plugin.

**Resolving Dual-homed Endpoints Managed by SecureConnector**

When a device has multiple network interfaces (such as wired and wireless NICs) each NIC is detected and listed in the Console as a separate endpoint.

When such a device is managed with SecureConnector, only one of the endpoints listed in the Console for this device is identified as *Managed by SecureConnector* - the endpoint corresponding to the interface used by SecureConnector. The other NICs are listed in the Console as endpoints *Not Managed by SecureConnector*. This means that network access policies can apply restrictive action to secondary NICs of a device that is managed by SecureConnector through another NIC.

When the Advanced Tools Plugin is installed, the optional *Windows Manageable SecureConnector (via any interface)* property can be used to resolve a secondary (unmanaged) interface on the device as *Managed* when another NIC on the endpoint is already managed by SecureConnector. Refer to the *Advanced Tools Plugin Configuration Guide* for details.

**Certificate Based Rapid Authentication of Endpoints**

Typically CounterACT endpoint detection capabilities are combined with endpoint authentication and compliance policies to enforce network access control: Upon connection, network access of endpoints is restricted (typically to the DHCP and DNS servers and to CounterACT for detection and remediation interactions) until the user/endpoint is authenticated and compliance is proven. Only then is the necessary network access granted. However, authenticating endpoints and verifying compliance can cause a delay during which even legitimate endpoints have only restricted access. If complex compliance policies are in place, this delay in network access may be noticeable, resulting in an unsatisfactory user experience for corporate users.

An alternative access control method for initial connection is to give all endpoints full access by default for a limited period of time. During this time, the endpoint is authenticated and compliance checks are performed in the background. If authentication and/or compliance is not achieved within this ‘grace period’ access is restricted. This provides an improved user experience, but also opens a window during which a rogue user may freely access the network.

Authenticating endpoints can be quite challenging, and often this step is either omitted altogether, or a weak authentication check is performed (such as ensuring manageability). A strong endpoint authentication mechanism supports more immediate network access based on authentication alone, without the need to rely on potentially lengthy compliance checks.
Certificate based rapid authentication provides a strong, secure and extremely fast endpoint authentication mechanism. It uses your corporate PKI (Public Key Infrastructure) to provide immediate, authenticated network access for corporate users and other known endpoints, while providing greater security than the ‘grace period’ access approach.

When endpoints connect to the network:

- Corporate endpoints and other trusted endpoints managed by SecureConnector immediately initiate certificate-based authentication as part of SecureConnector’s TLS interaction with CounterACT. Endpoints are granted immediate network access based on a signed X.509 digital certificate. CounterACT continues the compliance checks defined in active policies, and may revoke or change endpoint access if these checks fail.

- Endpoints without a valid rapid authentication certificate, or with an expired or revoked certificate, or endpoints not managed by SecureConnector, are granted limited network access until normal, policy-driven compliance checks are run.

For more information about implementing certificate-based rapid authentication in your environment, see the SecureConnector Advanced Features How-to Guide.
## Appendix A: Executable Files Used by the Plugin

The following executable files are installed on endpoints by the HPS Inspection Engine. Refer to the *HPS Inspection Engine Release Notes* for information regarding changes made to these files.

### EXE files

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fsprocsvc.exe</td>
<td>fsprocsvc.exe runs scripts for several CounterACT tasks. The service is similar to Microsoft’s PsTools (part of Windows Sysinternals tools: <a href="http://technet.microsoft.com/en-us/sysinternals/default.aspx">http://technet.microsoft.com/en-us/sysinternals/default.aspx</a>). The service does not open new network connections or generate traffic. The connection uses Microsoft SMB/RPC/WMI (445/TCP and 139/TCP) and is authenticated with domain credentials. If there is no request to run a new command within two hours, the service stops automatically.</td>
</tr>
<tr>
<td>SecureConnector.exe</td>
<td>The SecureConnector executable.</td>
</tr>
<tr>
<td>fs_DeviceControl.exe</td>
<td>Resolves the <em>External Devices</em> property.</td>
</tr>
<tr>
<td>fs_md5.exe</td>
<td>Resolves the <em>Windows File MD5 Signature</em> property.</td>
</tr>
<tr>
<td>fs_NBTDomain.exe</td>
<td>Resolves the <em>NetBIOS Domain</em> property</td>
</tr>
</tbody>
</table>

### Additional Files

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs_apps.vbs</td>
<td>Resolves the <em>Windows Applications Installed</em> property.</td>
</tr>
<tr>
<td>fs_auto_updates.vbs</td>
<td>Performs the <em>Windows Self Remediation</em> action.</td>
</tr>
<tr>
<td>fs_dot1x.vbs</td>
<td>Resolves host properties provided by the 802.1x Plugin.</td>
</tr>
<tr>
<td>fs_http_notify_g4.vbs</td>
<td>Supports the <em>HTTP Notification</em> action.</td>
</tr>
<tr>
<td>fs_http_upload.vbs</td>
<td>Resolves the <em>Microsoft Security &gt;Vulnerabilities</em> property.</td>
</tr>
<tr>
<td>fs_kb.vbs</td>
<td>Resolves the <em>Microsoft Security &gt;Vulnerabilities</em> property.</td>
</tr>
<tr>
<td>fs_kill_proc.vbs</td>
<td>Kills local processes to support <em>Kill...</em> actions.</td>
</tr>
<tr>
<td>Script Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fs_reg_edit.vbs</td>
<td>Performs the Set Registry Key on Windows action.</td>
</tr>
<tr>
<td>fs_sched_task_rm.vbs</td>
<td>Utility for running scripts with Task Scheduler.</td>
</tr>
<tr>
<td>fs_user.vbs</td>
<td>Supports the User property.</td>
</tr>
<tr>
<td>fs_wmi.vbs</td>
<td>Resolves the Windows Security Center Antivirus Status property.</td>
</tr>
<tr>
<td>fs_workgroup.vbs</td>
<td>Resolves the Device Information&gt;User property for endpoints running Vista on WORKGROUP.</td>
</tr>
<tr>
<td>fs_wua_full.vbs</td>
<td>Performs the Start Windows Updates action.</td>
</tr>
<tr>
<td>fs_wua_search.vbs</td>
<td>Used for Microsoft Security &gt;Vulnerabilities properties.</td>
</tr>
</tbody>
</table>

The plugin sometimes uses other methods to perform some of the tasks supported by these scripts. For example, SecureConnector can directly implement some of these tasks.

## Appendix B: Troubleshooting the HPS Inspection Engine

This section describes troubleshooting procedures if the HPS Inspection Engine test fails. The following categories are available:

- **Operational Requirements**
- **Testing the Domain Credentials**

### Operational Requirements

If the HPS Inspection Engine is not operating effectively, you should verify that the following requirements are met:

- Endpoints are running supported versions of Windows. See [Supported Windows Operating Systems](#).
- Endpoints are running services required for remote inspection and to run scripts. See [Working with Remote Inspection](#).
- You have domain-level administrator privileges on each computer being scanned or it is a member of the Domain Admins group. This group allows writing to the file system but not to the Windows Registry.
- On endpoints running Windows 7 and above, Port 445/TCP must be available. On earlier versions of Windows, port 139/TCP must also be available.
If your network includes endpoints that run under Windows XP SP2, you changed the Windows Firewall Settings so that CounterACT can perform remote inspection on these machines. This means that you should have access to 445/TCP or 139/TCP. Allowing access means CounterACT can retrieve Windows-related information. By default, these ports are open on Windows 2000 machines.

- CounterACT has access to the endpoint’s file system. If RRP is used for Remote Inspection, CounterACT must also access the remote registry. Refer to the CounterACT User Manual for more information about verifying this information.

- (For XP systems only) You have cleared Use Simple File Sharing for the endpoint.

To clear Simple File Sharing on Windows XP:

1. Double click the My Computer icon on your desktop.
2. Select Folder Options from the Tools menu.
3. Select the View tab.
4. Clear Use Simple File Sharing and select OK.

Testing the Domain Credentials

Perform the following steps to test the domain credentials.

1. Log onto a desktop machine using the CounterACT username and password. If this fails, check the counteract user settings on the Domain Controller.
2. Check that the desktop machine is a member of the Domain and is authenticating against the Domain Controller.
3. Check that the login is using the Domain, rather than localhost credentials.

Testing the Credentials on a Desktop Using a Localhost Query

This test ensures that a query can be performed using the domain credentials.

1. Log on to a desktop machine using any credentials other than the counteract user. This desktop should be a member of the domain.
2. Open a command window (Start>Run>cmd).
3. Run the following command:
   ```
   net use \127.0.0.1\C$ /USER:<domain>\<username>
   ```
4. Where <domain> is the fully qualified domain name of the network and <username> is the user account defined in CounterACT.
5. If the command completes successfully, it should return the following:
   ```
   Local name
   Remote name \\127.0.0.1\C$
   ```
Resource type: Disk
Status: OK
# Opens: 0
# Connections: 1

If this test fails:
- Check the domain syntax. Perhaps it needs to be more fully qualified. For example DOMAIN, DOMAIN.COM or HQ.DOMAIN.COM
- Check the credentials on the Domain Controller.

**Testing the Credentials on a Desktop Using Remote Query**

1. Log onto another desktop machine that is also a member of the domain.
2. Open a command window (Start>Run>cmd).
3. Run the command:
   ```
   net use \<IP> \c$ <password> /USER:<domain><username>
   ```
   Where
   - `<IP>` is the IP address of the target machine
   - `<password>` is the password for the `counteract` user
   - `<domain>` is the fully qualified domain name of the network
   - `<username>` is the user account defined in CounterACT

   If this fails, check the following:
   - [Domain Configuration Test](#)
   - [TCP/IP Configuration Test](#)
   - [Port Setup Test](#)
   - [NetBIOS over TCP/IP Setup Test](#)
   - [Services Test](#)
   - [Sharing Test](#)

**Domain Configuration Test**

**To perform a domain configuration test:**

1. Open the System dialog box. Select Start>Control Panel>System. See the domain configuration – in the Computer Name tab, select Change. Verify that the machine is a member of the domain and that the domain is spelled correctly.
2. Verify that the NetBIOS domain name is identical to the one configured in the Host Properties Scanner Plugin configuration screen. This is done by running ‘nbtstat –n’, see the following output.

**TCP/IP Configuration Test**

Open the properties dialog box of the relevant network connection.

**To open the dialog box:**

1. Select **Start>Settings>Control Panel>Network Connections**.
2. Right-click the network connection and select **Properties**. The following components should be installed (marked in red in the figure below):
   - **Client for Microsoft Networks**
   - **File and Printer Sharing for Microsoft Networks**
   - **Internet Protocol (TCP/IP)**
3. **Client for Microsoft Networks** should be configured as follows:

**Port Setup Test**

Depending on the Remote Inspection method that is used, and the Windows versions running on target endpoints, CounterACT should have access to ports 445/TCP and 139/TCP.

**Group Policy Test**

In a Windows XP group policy, the domain can be configured to set the end-system’s Windows Firewall settings. Refer to *Appendix 3: Remote Access to Network Hosts > Working with Windows XP SP2 Machines* in the Console User Manual for more information.

**Local Configuration of Windows Firewall**

**To allow incoming network connections:**

1. Select **Start>Settings>Control Panel>Windows Firewall>Exceptions>File and Printer sharing**. Ports 445/TCP and 139/TCP should be selected.
2. Choose **Change Scope** for each port and in the Custom List add the CounterACT IP address.

**Disabling Windows Firewall**

For testing purposes Windows Firewall can be disabled.
NetBIOS over TCP/IP Setup Test

NetBIOS over TCP/IP should be enabled either directly or from the DHCP server. One of the options in red below should be enabled:

![Advanced TCP/IP Settings](image)

Services Test

Verify that required services are running.

To verify:

1. Open the services view by selecting **Start**>**Control Panel**>**Administrative Tools**>**Services**.

2. Verify that the following services are running:
   
   - Server
     
     When RRP is used for Remote Inspection:
     
     - Remote Procedure Call (RPC).
     
     - Remote Registry Service
     
     When WMI is used for Remote Inspection:
     
     - Windows Management Instrumentation

3. If a service is not running:
   
   a. Start the service (right-click and select **Start**).
   
   b. Configure the service to automatically run on startup.

4. If services are running, but CounterACT reports that services are not running, for example:
   
   ```
   rpc_service_server_down:err
   ```
There may be a memory related issue on the endpoint which is preventing Windows from properly using those services.

**a.** Run the following command on the managing Appliance from the `/usr/local/forescout/` folder:

```
./bin/fs_smbclient -U `<username>` -W `<domain>` \\\`<ip>`\c$ -s
./plugin/va/smb.conf.NTLMv2 > & /tmp/smb.log
```

Where `<username>` `<domain>` and `<ip>` are values of the endpoint.

**b.** Open the event viewer on the endpoint and check for an event with ID 2017. This indicates a memory issue. If this event is found, start the regedit utility and modify the following registry keys:

- `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache`
  - Change this key value from 0 to 1.
- `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Siz e`
  - Change this key value from 1 to 3.
  - Restart the endpoint.

For more information on memory related issues in Windows, see:

- [https://support.microsoft.com/en-us/kb/2404366](https://support.microsoft.com/en-us/kb/2404366)
- [https://support.microsoft.com/en-us/kb/981314](https://support.microsoft.com/en-us/kb/981314)

**Sharing Test**

Verify the default C$ share exists.

**To verify C$ on endpoints running Windows XP or Windows 2000:**

1. From My computer, right-click drive C and select **Properties**.
2. In the Sharing tab, the following should be configured:
Disable the "Use simple file sharing" Option

In some rare incidents, this option prevents endpoints running Windows XP or Windows 2000 from performing remote inquiries.

**To disable simple file sharing:**

- From **My computer > Tools > Folder Options**, select the View tab, disable the **Use simple file sharing** option.

Appendix C: SecureConnector Log Files

SecureConnector creates log files on a continuous basis. Crash dump diagnostics are generated only when the SecureConnector application crashes. Log and crash dump files are created and stored at the following locations:

- On endpoints running Vista and later Windows releases:
  
  %ALLUSERSPROFILE%\ForeScout SecureConnector\Logs
  
  %ALLUSERSPROFILE%\ForeScout SecureConnector\Dump
  
- On endpoints running Windows XP:
  
  %ALLUSERSPROFILE%\Application Data\ForeScout SecureConnector\Logs
  
  %ALLUSERSPROFILE%\Application Data\ForeScout SecureConnector\Dump

Where %ALLUSERSPROFILE% is the pathname specified in the AllUsersProfile Windows environment variable.

**Log Files** - Individual log files can have a maximum size of 40M. When the active log file sc.log reaches this size limit, it is saved as a time stamped archive file. The
timestamp indicates the date and time range of events recorded in the file. By default 2 archive files are retained, in addition to the active log file. For example, the following files may typically appear in the \Logs directory:

sc.log
sc_2013-12-11_121052_2013-12-19_214626.log

The timestamp indicates the date and time range of events recorded in the file. The archive file in the example shown above covers the period from 12:10:25 AM on December 11 to 09:46:26 PM on December 19, 2013.

You can configure the number of log files that are retained on each endpoint, and other log settings.

**Crash Dump Files** – SecureConnector crash dump information is written to the \Dump directory. This directory is only created if a crash occurs. The contents of the \Dump directory are packaged as an archive named Dump.zip, which is placed in the parent \ForeScout SecureConnector directory.

**Configure and Retrieve Log files – the fstool sc_config Command**

The **fstool sc_config** command lets you configure log settings on any endpoint, and retrieve log and crash dump files from any endpoint.

**Configure Logging on an Endpoint**

To configure logging behavior on an endpoint, use the following form of the command:

```
fstool sc_config <ip> -log_level <lvl> -max_logs_number <max> -timespan_minutes <min>
```

where

- `<ip>` is the IP address of the endpoint
- `<lvl>` is the severity level of events that should be recorded in the log. By default events up to severity level 4 are logged. In some cases, ForeScout support staff may ask you to use severity level 5 to capture additional events.
- `<max>` is the maximum number of log files that are retained, including the current open log file. By default 2 files are retained. Each archived log file is 40M in size. When the active log file reaches 40 M it is archived, and the oldest archived file is deleted to keep the total number of files within the specified limit.
- `<min>` is the time interval for which the settings specified in the command are applied. When this term is omitted, settings are permanent on the endpoint until the next sc_config command.

The following example applies the highest log level for a 12-hour period. Events at all severity levels are recorded in the log file during the next 12 hours. After 12 hours, the log level returns to the previous setting.

```
fstool sc_config 100.10.10.01 -log_level 5 -timespan_minutes 720
```
The following example permanently limits the number of log files on the endpoint to three.

```bash
fstool sc_config 100.10.10.01 -max_logs_number 3
```

**Retrieve Files from an Endpoint**

To retrieve log files from an endpoint, use the following form of the command:

```bash
fstool sc_config <ip> -get_logs <CT_path>
```

To retrieve crash dump files from an endpoint, use the following form of the command:

```bash
fstool sc_config <ip> -get_dump <CT_path>
```

where

- `<ip>` is the IP address of the endpoint
- `<CT_path>` is the pathname on the CounterACT Appliance to which files are copied.

---

**Appendix D: Remote Inspection and SecureConnector – Feature Support**

This table summarizes Windows-related CounterACT features that are supported by Remote Inspection and/or by SecureConnector and provides information about the benefits of using SecureConnector.

- ✓ a green checkmark indicates supported
- ✗ a red x indicates not supported
- ✓ a yellow checkmark indicates supported but requires the fsprocsvc.exe service.

SecureConnector supports event-driven real-time resolution of host properties. See [Event Driven Monitoring of Host Properties](#).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Type</th>
<th>Technology</th>
<th>Benefits of SecureConnector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to VLAN</td>
<td>Action</td>
<td>RI WMI</td>
<td>✗</td>
</tr>
<tr>
<td>Windows Applications Installed</td>
<td>Property</td>
<td>RI RRP</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Device Interfaces</td>
<td>Property</td>
<td>Secure Connector</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Disable Dual Homed</td>
<td>Action</td>
<td>Secure Connector</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Feature</td>
<td>Type</td>
<td>Technology</td>
<td>Benefits of SecureConnector</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------</td>
<td>------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><img src="265x644" alt="Image" /> Disable External Device</td>
<td>Action</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="301x644" alt="Image" /> Windows Domain Member</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="336x644" alt="Image" /> Windows Expected Script Result (non-interactive)</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows Expected Script Result (interactive)</td>
<td>Property</td>
<td>RRP</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="209x682" alt="Image" /> External Devices</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows File Date</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows File Exists</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows File MD5 Signature</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows File Size</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows File Version</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows File Version Comparison</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows Hotfix Installed</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> HTTP Redirection to URL (If Attempt to open a browser at the detected endpoint is selected)</td>
<td>Action</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Intranet WSUS Server</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows Is Behind NAT</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Kill Process on Windows</td>
<td>Action</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows Last Login Event</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector installed as a service</td>
</tr>
<tr>
<td><img src="266x668" alt="Image" /> Windows Logged On</td>
<td>Property</td>
<td>RI</td>
<td>Secure Connector</td>
</tr>
<tr>
<td>Feature</td>
<td>Type</td>
<td>Technology</td>
<td>Benefits of SecureConnector</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------</td>
<td>---------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RI WMI</td>
<td>RI RRP</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Property</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Microsoft Applications Installed</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Vulnerabilities</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Microsoft Vulnerabilities Fine-tuned</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MS-RRP Reachable</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-SMB Reachable</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-WMI Reachable</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS Domain</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NetBIOS Hostname</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NetBIOS Membership Type (Domain or Workgroup)</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Number of IP Addresses</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows Registry Key Exists</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Registry Value</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Registry Value Exists</td>
<td>Property</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run Script On Windows (non-interactive)</td>
<td>Action</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Feature</td>
<td>Type</td>
<td>Technology</td>
<td>Benefits of SecureConnector</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Run Script On Windows (interactive)</td>
<td>Action</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
<tr>
<td>Windows SecureConnector Deployment Type</td>
<td>Property</td>
<td>N/A, N/A</td>
<td>✓</td>
</tr>
<tr>
<td>Windows SecureConnector Connection Encryption</td>
<td>Property</td>
<td>N/A, N/A</td>
<td>✓</td>
</tr>
<tr>
<td>Windows SecureConnector Systray Display</td>
<td>Property</td>
<td>N/A, N/A</td>
<td>✓</td>
</tr>
<tr>
<td>Send Balloon Notification</td>
<td>Action</td>
<td>✗, ✗, ✓</td>
<td></td>
</tr>
<tr>
<td>Set Registry Key on Windows</td>
<td>Action</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
<tr>
<td>Windows Shared Folders</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td>Event-driven real-time resolution instead of polling</td>
</tr>
<tr>
<td>SMB Relay</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
<tr>
<td>SMB Signing</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
<tr>
<td>Start Windows Updates</td>
<td>Action</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
<tr>
<td>Windows Updates Installed – Reboot Required</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
<tr>
<td>User currently logged on</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
<tr>
<td>Windows Manageable Domain</td>
<td>Property</td>
<td>✓, ✓, N/A</td>
<td></td>
</tr>
<tr>
<td>Windows Manageable Domain (Current)</td>
<td>Property</td>
<td>✓, ✓, N/A</td>
<td></td>
</tr>
<tr>
<td>Windows Manageable Local</td>
<td>Property</td>
<td>✓, ✓, N/A</td>
<td></td>
</tr>
<tr>
<td>Windows Manageable SecureConnector</td>
<td>Property</td>
<td>N/A, N/A</td>
<td>✓</td>
</tr>
<tr>
<td>Windows Processes Running</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td>Event-driven real-time resolution instead of polling</td>
</tr>
<tr>
<td>Windows Services Installed</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td>Event-driven real-time resolution instead of polling</td>
</tr>
<tr>
<td>Windows Services Running</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td>Event-driven real-time resolution instead of polling</td>
</tr>
<tr>
<td>Windows Update Agent Installed</td>
<td>Property</td>
<td>✓, ✓, ✓</td>
<td></td>
</tr>
</tbody>
</table>
## Related Plugins

SecureConnector and Remote Inspection both support the properties and actions provided by other HPS Inspection Engines such as the HPS NIC Vendor DB.

SecureConnector and Remote Inspection both support all the properties and actions provided by the HPS Applications Plugin. However, SecureConnector supports event-driven reporting of properties which detect the presence and running state of third-party applications.

## User Accounts to Run Scripts on Managed Endpoints

CounterACT runs processes and scripts on managed endpoints to resolve host properties and implement actions. This table summarizes the user accounts that are used by these processes when different Remote Inspection methods are used and when SecureConnector is installed on the endpoint.

Refer to relevant sections of this guide for details of endpoint management functionality supported by each of these methods.

<table>
<thead>
<tr>
<th>Method Used to Run Scripts</th>
<th>Non Interactive Scripts Run As</th>
<th>Interactive Scripts Run As</th>
</tr>
</thead>
<tbody>
<tr>
<td>fsprocsvc.exe</td>
<td>System user</td>
<td>Current logged-in user</td>
</tr>
<tr>
<td>WMI</td>
<td>User configured in HPS Inspection Engine</td>
<td>(Not Available with WMI)</td>
</tr>
<tr>
<td>Task Scheduler</td>
<td>User configured in HPS Inspection Engine</td>
<td>Current logged-in user</td>
</tr>
<tr>
<td>SecureConnector installed as service</td>
<td>System user</td>
<td>Current logged-in user</td>
</tr>
<tr>
<td>SecureConnector installed as application</td>
<td>Current logged-in user</td>
<td>Current logged-in user</td>
</tr>
</tbody>
</table>
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
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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

To access the Documentation Portal:

4. Use your customer support credentials to log in.
5. Select the CounterACT version you want to discover.

Customer Support Portal

The Customer Support 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 Customer Support Portal:

7. 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**

8. After the plugin is installed, select Options from the Tools menu and then select Plugins.

9. Select the plugin and then select Help.

**Documentation Portal**

Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-02-28 12:25