



ForeScout

Endpoint Module: HPS Inspection Engine

Configuration Guide

Version 11.1.1



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-06-17 14:15

Table of Contents

About the HPS Inspection Engine	6
Accessing and Managing Endpoints	6
Remote Inspection	7
SecureConnector™	7
HPS Inspection Engine Plugin Requirements	8
Configure the HPS Inspection Engine	9
Configure by Region or Appliance	9
Troubleshooting Configuration	9
Access the HPS Inspection Engine Configuration Pane	9
Remote Inspection	10
Domain Credentials	10
General Remote Inspection Settings	11
SecureConnector	13
Upgrade Mode	14
Actions	14
Detection	15
SecureConnector Password Protection	16
Alternative Appliances	16
Client-Server Connection	16
Windows Updates	17
Distributing Vulnerability Information to Windows Endpoints	18
Using Windows Server Update Services (WSUS) or Windows Update	18
Windows Update Default Settings	19
Classification Utility	19
Forescout Classification Version	20
Nmap Scan Options	21
Tuning	24
Specify Endpoint IP Addresses to Ignore	24
Tune HPS Inspection Engine Processes	24
Tune Nmap Processes	25
Send HTTP Actions on SecureConnector Connect and User Login	26
HTTP Notification Action – Attempt to Open Browser at Endpoint	26
User Name Resolve Priorities	27
Advanced Remote Inspection Configuration	28
Ensure That the HPS Inspection Engine Plugin Is Running	28
Testing and Verifying Connectivity	28
Configuration for an Appliance or Group of Appliances	29
Working with Remote Inspection	30
About MS-WMI	30
About Registry Service and Remote Procedure Calls	31
About SMB	32
Detecting SMB Relay Behavior	32
Working with SMB Signing	33

About Kerberos	33
Detecting Services Available on Endpoints	34
Script Execution Services	35
About Secured Directories and Script Files	36
About fsprocsvc.exe.....	36
Microsoft Task Scheduler	37
Working with SecureConnector	38
How SecureConnector Works	39
Event Driven Monitoring of Host Properties	39
Installing and Running SecureConnector	39
Download or Link to a SecureConnector Installer Package	40
Generate an MSI Installer for SecureConnector	43
The SecureConnector Executable.....	44
The SecureConnector ID	45
Stop SecureConnector	45
Uninstall SecureConnector.....	46
Updating SecureConnector	46
SecureConnector Details	48
Restrict SecureConnector Access to the Appliance	49
Detect NAT Behavior Based on SecureConnector Connections	50
Resolving Dual-homed Endpoints Managed by SecureConnector.....	50
Using Certificates to Authenticate the SecureConnector Connection	51
Certificate-Based Rapid Authentication of Endpoints	52
Endpoint Module Information.....	53
Additional Forescout Documentation.....	53
Documentation Downloads	53
Documentation Portal	54
Forescout Help Tools.....	54
Appendix A: Endpoint Ports and Executable Files Used by HPS Inspection Engine	56
Endpoint Ports	56
Endpoint Executables.....	58
Appendix B: Troubleshooting the HPS Inspection Engine.....	60
Operational Requirements	60
Testing the Domain Credentials.....	61
Test the Credentials on a Desktop Using a Localhost Query	61
Test the Credentials on a Desktop Using Remote Query	61
Port Setup Test	64
NetBIOS over TCP/IP Setup Test	66
Services Test	67
Sharing Test	68
Appendix C: SecureConnector Log Files.....	69

Configure and Retrieve Log files – the fstool sc_config Command 70

Appendix D: Remote Inspection and SecureConnector – Feature Support.. 71

Related Plugins 75

User Accounts to Run Scripts on Managed Endpoints 75

About the HPS Inspection Engine

The HPS (Host Property Scanner) Inspection Engine is a component of the Forescout Endpoint Module. See [Endpoint Module Information](#) for details about the module.


The HPS Inspection Engine allows Forescout eyeSight 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.


Forescout eyeControl uses the HPS Inspection Engine to perform *actions* to manage, remediate or control endpoints.

This document describes how to configure the HPS Inspection Engine and provides other information, including:

- Supported operating systems
- Executables and processes generated by the HPS Inspection Engine
- Troubleshooting issues

 *Some of the functionality and configuration settings described here apply primarily to Windows endpoints. Configure the OS X Plugin and the Linux Plugin to provide parallel functionality for OS X or Linux endpoints.*

Accessing and Managing Endpoints

 *This section contains information common to plugins of the Endpoint Module.*

Endpoint Module plugins access endpoints to learn detailed information about the endpoint, such as file metadata and operating system information. In addition, the plugins run scripts on endpoints and perform other remediation actions.

- The HPS Inspection Engine interacts with Windows endpoints.
- The Linux Plugin interacts with Linux endpoints.
- The OS X Plugin interacts with OS X endpoints.

When you configure these plugins, you determine the methods used to access and manage endpoints. When these access methods are successful, the endpoint is resolved as *Manageable*.

You can use the following methods to access endpoints:

- [Remote Inspection](#)
- [SecureConnector™](#)

Both methods can be deployed together in a single network environment.

Remote Inspection

Remote Inspection uses the SSH communications protocol to query the endpoint, and to run scripts and implement remediation actions on the endpoint.

Agentless

Remote Inspection is *agentless* - The Forescout platform 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 endpoint.

Specify Remote Inspection settings in the Remote Inspection tab of each plugin during plugin configuration.

The following properties indicate whether Remote Inspection is used to access and manage an endpoint:

- For Windows endpoints (supported by the HPS Inspection Engine):
 - Windows Manageable Domain
 - Windows Manageable Domain (Current)
 - Windows Manageable Local
- For Linux endpoints (supported by the Linux Plugin):
 - Linux Manageable (SSH Direct Access)
- For OSX endpoints (supported by the OSX Plugin):
 - Macintosh Manageable (SSH Direct Access)

SecureConnector™

SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information back to Forescout eyeSight, and implements Forescout actions on the endpoint. The *Start SecureConnector* action initiates SecureConnector installation on endpoints.

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:

	Windows Endpoints	Linux Endpoints	OS X Endpoints
SecureConnector installer package provided by:	HPS Inspection Engine	Linux Plugin	OSX Plugin
Can install SecureConnector as a dissolvable utility	✓	✓	✓
Can install SecureConnector as a permanent application	✓	✗	✗

	Windows Endpoints	Linux Endpoints	OS X Endpoints
Can install SecureConnector as a <i>permanent service / system daemon</i>	✓	✓	✓

The following properties indicate whether SecureConnector is used to access and manage an endpoint:

- For Windows endpoints (supported by the HPS Inspection Engine):
 - Windows Manageable SecureConnector
 - Windows Manageable SecureConnector (via any interface)
- For Linux endpoints (supported by the Linux Plugin):
 - Linux Manageable (SecureConnector)
- For OSX endpoints (supported by the OSX Plugin):
 - Macintosh Manageable (SecureConnector)

HPS Inspection Engine Plugin Requirements

This section describes the requirements for configuring and running the Forescout HPS Inspection Engine Plugin.

Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Forescout Endpoint Module 1.2.1 with the HPS Inspection Engine Plugin.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.
- Core Extensions Module version 1.2.1 including the DNS Client Plugin.
- Content Modules:
 - Windows Applications version 20.0.5
 - NIC Vendor DB version 20.0.4
 - Windows Vulnerability DB version 20.0.5

Networking Requirements

SecureConnector creates an encrypted tunnel from the endpoint to the Appliance through TCP port 10003. This port must be open on enterprise firewalls to support communication between SecureConnector and the Appliance.

Supported Windows Operating Systems

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

Configure the HPS Inspection Engine

You can configure the HPS Inspection Engine to:

- Add or update Windows domain credentials
- Define general SecureConnector settings
- Define global options when working with the *Start Windows Updates* action
- Specify resolution methods and default values for various global parameters
- Specify test parameters and test connectivity

Configure 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 HPS Inspection Engine 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 HPS Inspection Engine Configuration Pane

To configure HPS Inspection Engine:

1. In the Forescout Console, select **Options** from the **Tools** menu.
2. Select **Modules > Endpoint > HPS Inspection Engine**. Then select **Configure**.
3. Configure as required. 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, MS-RRP, and other standard protocols to manage Windows endpoints. Use this tab to configure how HPS Inspection Engine performs Remote Inspection.

The screenshot shows the 'Remote Inspection' configuration tab. It includes a 'Domain Credentials' table with columns for 'Domain Administrator', 'DNS Domain Name', and 'Netbios Domain Name'. Below the table are 'Add', 'Edit', and 'Remove' buttons. The 'Endpoint Remote Inspection method' is set to 'Using MS-RRP (Windows Remote Registry Protocol)'. Other settings include 'When Remote Inspection uses MS-WMI, run scripts with: CounterACT (fsprocsvc)', 'When Remote Inspection uses MS-RRP, run scripts with: CounterACT (fsprocsvc)', 'Authentication Method: Kerberos', 'When Authentication Method is Kerberos, resolve hostname using: Netbios name based resolution', and 'Minimum SMB Protocol Version: SMBv1'. A checkbox for 'Require SMB signing' is present with a note: 'When this option is selected, endpoints without SMB signing enabled cannot be managed by Remote Inspection.'

Domain Credentials

Domain credentials are credentials with local machine administrator privileges that are used to connect to network endpoints. Basic configuration of domain credentials is usually performed when setting up the Forescout Console via the Console Initial Setup Wizard. For more information, see the *Forescout 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 that exists in the Local Administrators group of endpoints in the relevant network segment.

At least one set of administrator credentials must be defined.

- Domain credentials defined during initial setup appear in the Domain Credentials table of the *Remote Inspection* tab. See the *Forescout Administration Guide* for details of the Initial Setup Wizard.
- 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 the credentials used by Appliances that monitor a specific network segment or regional subnet. For details, refer to [Configuration for an Appliance or Group of Appliances](#).

To connect to an endpoint, the plugin steps through this list until a set of credentials succeeds.

If you define separate configurations with domain credentials specific to network segments, place the domain credentials most relevant to the segment at the top of the table so that they are tried first. Keep the default domain credentials defined during initial setup at the bottom of the table.

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

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

Domain Administrator	The user name of an administrator account for endpoints that are handled by the HPS Inspection Engine.
DNS Domain Name	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.
NetBIOS Domain Name	(Optional) The NetBIOS domain name of the matching DNS Domain name. This field is optional and may result in better Kerberos authentication.
Domain Password	The password of the administrator account. (CyberArk only) When the Forescout eyeExtend Module (Extended Module) for CyberArk is installed, the Password source field appears. When you select CyberArk as the domain administrator password source, the password is provided by the CyberArk Password Vault. Refer to the Forescout eyeExtend for CyberArk Configuration Guide for more information. See Additional Forescout Documentation for information on how to access the guide.

General Remote Inspection Settings

Define the following general settings:

Endpoint Remote Inspection method

Choose the protocol used to communicate with Windows endpoints. Options include:

- **Using MS-RRP** – The HPS Inspection Engine interacts with the endpoint using remote procedure calls (RPCs) to the Windows Remote Registry Service (MS-RRP) on the endpoint.
- **Using MS-WMI** – The HPS Inspection Engine 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 HPS Inspection Engine first tries to use the Windows Management Instrumentation (WMI) service to interact with each endpoint. If WMI services are not running on an endpoint, HPS Inspection Engine 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 HPS Inspection Engine uses to run scripts on the endpoint.

Options include:

- **MS-WMI** – 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.
- **Forescout fsprocsvc** – fsprocsvc is a proprietary Forescout service utility downloaded by HPS Inspection Engine to endpoints. This utility is able to implement interactive scripts on endpoints.

When Remote Inspection uses MS-RRP, run scripts with

Choose the service HPS Inspection Engine uses to run scripts on the endpoint.

Options include:

- **Forescout fsprocsvc** – A proprietary Forescout service utility downloaded by HPS Inspection Engine to endpoints.
- **Windows Task Scheduler** – This standard service launches scripts and other processes on most Windows machines.


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

Authentication Method

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

- **Kerberos** –use the Kerberos servers installed in domain controllers of your environment. See [About Kerberos](#) for details.
- **NTLMv1 only** – Although this option provides backwards compatibility, it is not recommended for security reasons.
- **NTLMv2 only** – For security reasons, there is no fallback 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.*

When Authentication Method is Kerberos, resolve hostname using

Choose whether Kerberos resolves the hostname using information from the SPNEGO handshake, or using a DNS query.

Minimum SMB Protocol Version

SMB clients and servers negotiate the SMB version they will use. Choose the minimum SMB version that is used 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 in recent Windows versions.

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

SMB Version	Earliest Windows Support
SMB 3.1.1	Windows 10 Windows Server 2016
SMB 3	Windows 8 Windows Server 2012
SMB 2	Windows Vista Windows Server 2008
SMB 1	Previous versions

Require SMB signing

When this option is selected, every new connection to an endpoint requires digitally signed SMB communication. When this option is cleared, SMB signing is supported, but not required.

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 Forescout eyeSight. 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 HPS Inspection Engine configuration screen.

HPS Inspection Engine
Use this pane to configure how the HPS Inspection Engine accesses and manages Windows endpoints.

CounterACT Devices ▾

Default +

Remote Inspection **SecureConnector** Windows Updates Classification Utility Tuning Test

Upgrade Mode

☐ Automatically upgrade Windows endpoints managed by SecureConnector to current SecureConnector version (11.0.00.0089)

Actions

☐ Automatically run SecureConnector when using the Disable External Device action. (Required for this action.)

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

☐ Automatically run SecureConnector when using the Disable Dual Homed action. (Required for this action.)

☒ Show balloon messages at desktop.

Detection

☐ Use SecureConnector to learn MAC addresses from the local ARP table

SecureConnector Password Protection

SecureConnector Password Protection

Retype SecureConnector Password Protection

Alternative Appliances

Additional Appliance Connections

Client-Server Connection

Minimum supported TLS version: TLS version 1.0 ▾

☐ CounterACT server verifies SecureConnector client certificate chain

Check SecureConnector client certificate revocation status Do not check ▾

Additional CDPs for CRL:

☐ Soft-fail OCSP requests

Upgrade Mode

Automatically upgrade Windows endpoints managed by SecureConnector to current SecureConnector version

Use this setting to enable or disable automatic updates of SecureConnector for Windows. For details, see [Updating SecureConnector](#).

Actions

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

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; without SecureConnector, the process is killed once a minute. Select this option to automatically install SecureConnector and increase kill frequency (recommended).

When Kill actions affecting Windows endpoints are first applied to an endpoint, the Console indicates this by reporting that the processes were killed, even if the specified applications are not running on the endpoint. This behavior is functioning as designed.

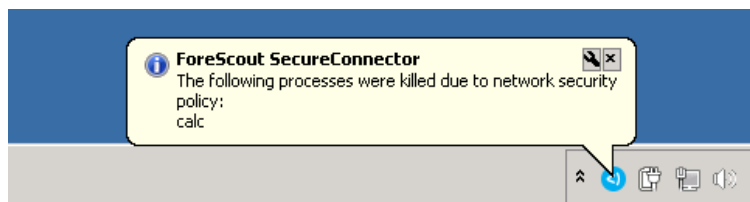
Automatically run SecureConnector when using the Disable Dual Homed action

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 the following messages generated by SecureConnector:

- Messages sent to an endpoint using the **Send Balloon Notification** action.
- Messages appear when the Disable External Devices, Kill Process, Kill Instant Messaging, and Kill Peer-to-peer actions are performed, indicating the impact of the action.



Balloon notifications are displayed only if the SecureConnector icon appears in the endpoint systray. To work with balloon notifications, enable the systray icon when you install SecureConnector. For details, see [Installing and Running SecureConnector](#).

Detection

Use SecureConnector to learn MAC address from local ARP tables

The Switch Plugin queries the ARP table on switches to learn MAC addresses. When you select this option, the HPS Inspection Engine also queries the local ARP table on endpoints managed by SecureConnector. This additional ARP query enables detection of endpoints that may be otherwise unreachable. Local ARP table query is not implemented on SecureConnector instances that are located behind a NAT address.

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.

Alternative Appliances

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. Typically, this list contains other Appliances managed by this Enterprise Manager.

Client-Server Connection

When an endpoint managed by SecureConnector accesses the network, the SecureConnector client on the endpoint connects to the CounterACT Appliance that manages that endpoint. The settings in this section of the tab let you configure the protocols used to establish the client-server connection, and secure the connection using an X.509-compliant public key certificate.

When you use certificates to secure the client-server connection:

- Use the Certificates interface of the Console to import certificates and trust chains. See "Appendix 8: Configuring the Certificate Interface" in the *Forescout Administration Guide*.
- Use your environment's Public Key Infrastructure (PKI) to distribute client-side certificates to endpoints.
- For more information about certificate-based authentication using SecureConnector, see the *SecureConnector Advanced Features How-to Guide*.

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)

CounterACT server verifies SecureConnector client certificate chain

When this option is enabled, SecureConnector clients on Windows endpoints present a certificate when they connect to the Forescout platform. Forescout eyeSight validates the certificate chain. When you select this option, additional required settings are active.

To work with this option, endpoints managed by SecureConnector must have a signed client certificate and trust chain. Your PKI may define several certificates that can be used by SecureConnector, for example, certificates defined by geographical location or endpoint roles and permissions. Use the Trusted Certificates pane of the Console to import the client-side trust chain(s). For details, refer to the *ForeScout Administration Guide*.

Check SecureConnector client certificate revocation status

Check that the client certificate has not been revoked. From the drop-down menu, select how the client certificate revocation status is determined:

- **Using CRL:** Check if the certificate is in the Certificate Revocation List (CRL) of the issuing Certificate Authority.
- **Using OCSP:** Send an Online Certificate Status Protocol (OCSP) request for the certificate revocation status.

Additional CDPs for CRL

Enter a comma-separated list of CRL distribution points that should be queried.

Soft-fail OCSP requests

When no response is received from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.

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.

The screenshot shows the 'Windows Updates' configuration tab within the HPS Inspection Engine console. The interface includes a navigation bar at the top with tabs for 'Remote Inspection', 'SecureConnector', 'Windows Updates' (selected), 'Classification', 'Tuning', and 'Test'. Below the navigation bar, there is a section titled 'Use endpoint's "Windows Updates" settings (WSUS, MS Website) to check for missing updates'. This section contains a table with columns 'From' and 'To', and a list of items. Below the table, there are buttons for 'Add', 'Edit', and 'Remove'. The 'Add' button is highlighted. Below the table, there is a section titled 'WSUS Environment Settings' with two input fields: 'HTTP(S) URL of WSUS server' and 'HTTP(S) URL of report server'. Below this, there is a section titled 'Windows Update Default Settings' with two settings: 'Update method' (set to 'Automatically Download and Notify of Installation') and 'Maximum Concurrent Vulnerability DB File HTTP Uploads' (set to 40).


To update vulnerability information on endpoints, several methods are supported:

- Using the HPS Inspection Engine. The HPS Inspection Engine checks for vulnerability updates on managed endpoints, and downloads latest vulnerability information. See [Distributing Vulnerability Information to Windows Endpoints](#).

- Using WSUS instances or Windows Update. See [Using Windows Server Update Services \(WSUS\) or Windows Update](#).
- When they are available, you may use other methods to distribute the Microsoft Vulnerability CAB file to endpoints in your environment.

Distributing Vulnerability Information to Windows Endpoints

The HPS Inspection Engine looks for the `wsusscn2.cab` file on Windows endpoints. If this file is different from the CAB file provided by the Windows Vulnerability DB, the plugin downloads its own CAB file to the endpoint.

 *Refer to the Windows Vulnerability DB Configuration Guide for details of CAB file distribution.*

Using Windows Server Update Services (WSUS) or Windows Update

It may be more efficient for endpoints to retrieve vulnerability information from WSUS or Windows Update, rather than use the information provided by the Windows 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.

This section describes how to configure handling of vulnerability information retrieved directly from WSUS or Windows Updates.

 *In large, geographically dispersed networks with several WSUS instances, you can define settings for specific Appliances or groups of Appliances. See [Configure by Region or Appliance](#) for details.*

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. Note that:
 - When at least one IPv4 range is defined in the table, Forescout treats all IPv6 subnets covered by this configuration as if they are included in the table. Although they do not appear in the table, IPv6 addressable endpoints use Windows Updates/WSUS.
 - IPv4-only endpoints not included in the specified ranges receive vulnerability information from the Windows Vulnerability DB.
2. To use local WSUS instances, enter the URLs of target WSUS servers and WSUS report servers in the **WSUS Environment Settings** area.

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

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 ForeScout policy conditions. In this case, vulnerabilities of interest are determined at the WSUS, and Forescout policy conditions should detect endpoints with any vulnerability tracked by the WSUS instance. Configure policy conditions as follows:

1. In the Forescout 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 **Check new vulnerabilities automatically**.

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 Utility

This tab contains controls that determine how the HPS Inspection Engine performs endpoint classification.

Remote Inspection	SecureConnector	Windows Updates	Classification Utility	Tuning	Test
<input checked="" type="checkbox"/> Use Nmap Banner Scan					
<input checked="" type="checkbox"/> Use Nmap Fingerprint Scan					
<input checked="" type="checkbox"/> Use Nmap results with low confidence level					

The HPS Inspection Engine powers Forescout tools used for classifying endpoints. These tools attempt to identify the category of network asset to which each endpoint belongs. The Network Function property reports the results, sorting endpoints into categories.


Use classification policy templates and advanced properties to further refine these categories, or to classify devices into groups based on 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 the Forescout platform or switches configured to work with the Forescout platform;

and Nmap scans. Nmap is typically used 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.

Forescout Classification Version

 *This section is only relevant if you upgraded from a previous release.*

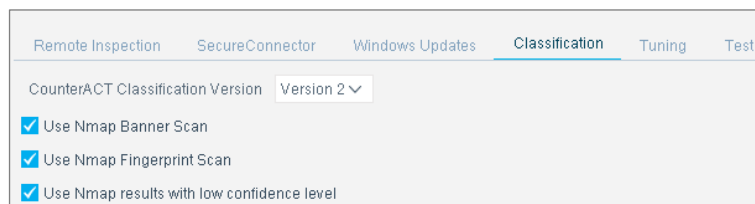
The set of methods used for classification in Forescout evolves over time to include different tools and larger endpoint fingerprint databases.

- Classification Version 3 is the default version and uses Nmap 7.0.1.
- Classification Version 2 uses the same classification algorithms as Version 3 but uses Nmap 5.21.

For new (scratch) installations, or if you previously ran Classification Version 3 before upgrading to this release:

- Classification Version 3 is used for classification.
- The Forescout Classification Version drop-down menu *does not appear in the Classification tab.*

If you were using Classification Version 2 before you upgraded to this release, the Forescout Classification Version drop-down menu is provided to allow you to upgrade. *It is strongly recommended to upgrade to Classification Version 3.* For details, see [Upgrading the Classification Version](#).



 *Even if you continue to use Classification Version 2, Forescout uses Classification Version 3 to classify IPv6 addressable endpoints.*

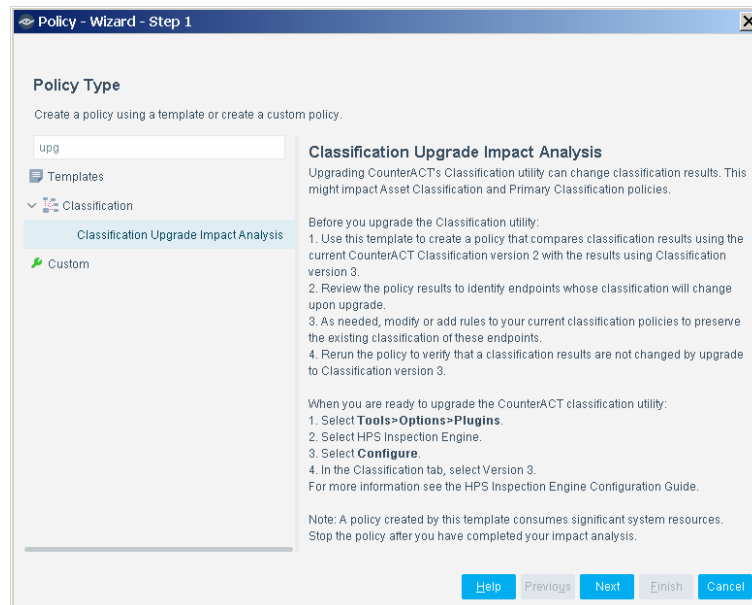
Upgrading the Classification Version

Follow the procedure in this section to upgrade from Classification Version 2 to Classification Version 3. *It is strongly recommended to upgrade to Classification Version 3.*

When you change the set of classification methods, there may be significant changes in the results of HPS Inspection Engine's classification processes. These changes are evident when some endpoints receive new values for the **Function, Operating System, Vendor and Model, 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 Upgrade Impact Analysis 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 this 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 so 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 find that endpoints not accurately classified by classification version 2 are now handled correctly by the improved capabilities of classification version 3. In these cases, remove 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, HPS Inspection Engine 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, HPS Inspection Engine uses Nmap fingerprint scans to resolve the classification properties.

Use Nmap results with low confidence level

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

Nmap Scan Logs

Nmap output is not logged. For troubleshooting purposes, set the following Boolean properties to create log files in the HPS Inspection Engine's log file directory.

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

Property	Equivalent Nmap Flag
config.nmap_log_banners_normal.value	-oN: Enables normal output
config.nmap_log_banners_xml.value	-oX: Enables XML output
config.nmap_log_banners_grepable.value	-oG: Enables grep output
config.nmap_log_banners_all.value	Enables all output formats

To enable logging, log in to the CLI of 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
```

Nmap Scan Commands Used by HPS Inspection Engine

This section describes the parameters used for various Nmap scans.

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 does not yield enough information to classify the device, HPS Inspection Engine repeats the Nmap scan 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

To overwrite the list of ports that is used for any of these scans, log in to the Enterprise Manager and submit the following command:

```
fstool oneach fstool va set_property <scan_config_property> <ports>
```

where

<scan_config_property> is one of the nmap scan properties listed below.

<ports> is a list of port numbers you want to use in this nmap scan.

Nmap Scan Type	Configuration Property	Default Value
Banner Scan	config.nmap_banner_tcp_ports.value	21,22,23,53,80,135,88,1723,3389,5900 ▪ CSV format
Initial Fingerprint Scan	config.nmap_common_ports_fragile.value	80;9100;515 ▪ List items separated by semi-colon character (;).
Full Fingerprintnt Scan	config.nmap_common_ports_robust.value	4,21,22,23,25,79,80,110,111,135,139,220,445,513,631,143,8080,41351,62078 ▪ CSV format

Tuning

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

Specify Endpoint IP Addresses to Ignore

The table lists endpoint IP addresses that are ignored when calculating the Number of IPv4 Addresses host property.

- Select **Add** to add an IPv4 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 **Dynamically scale concurrent HPS Inspection Engine processes based on available memory** 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):

- Clear the **Dynamically scale concurrent HPS Inspection Engine processes based on available memory** checkbox.
 - Enter a value in the **Concurrent RI HPS - Inspection Engine Processes** field to set the maximum number of processes that 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 that communicate with endpoints managed by SecureConnector 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.*
-  *The Technical Support Plugin provided with the Core Extensions Module lets you retrieve detailed logs of SecureConnector and Remote Inspection processes and memory usage. Use this information to monitor HPS Inspection Engine performance on Appliances.*

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. HPS Inspection Engine selects a default value based on total Appliance memory.

Available Memory	Default Concurrent Processes
Up to 1 GB	5
Up to 2 GB	10
Up to 4 GB	20
More than 4 GB	40

To enable automatic tuning:

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


HPS Inspection Engine does not exceed the default maximum concurrent processes on each Appliance.

To customize tuning (for advanced use only):

- Clear 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 **Limit source ports for Nmap scanning**. Nmap fingerprinting processes use source ports higher than 61000.

 *The Technical Support Plugin provided with the Core Extensions Module lets you retrieve detailed logs of module processes and memory usage. Use this information to monitor HPS Inspection Engine performance on Appliances.*

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 when the action is issued, the HTTP message is not displayed. With this option set, the message is 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

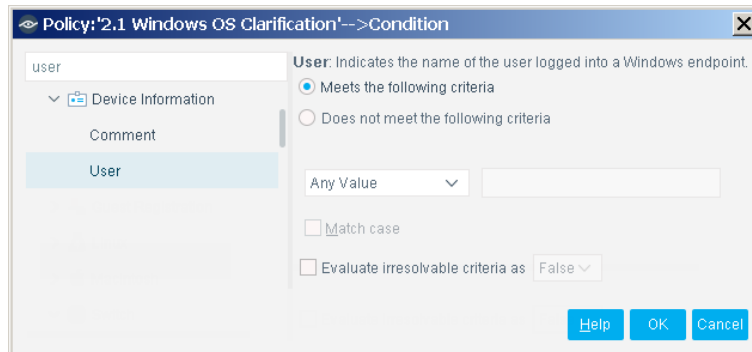
Selecting this option causes the HTTP Notification action to open an Explorer dialog box rather than the default Web browser.

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

To learn endpoint user names, three options are available:

- Always use HTTP login name when available.
The name is 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

Resolve to last known user name when no users are logged in to endpoint

When this option is selected, the last known user name 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.

Use HTTP Login name when Sign In page is closed

Enable this option to use the HTTP login name when the HTTP sign in page is closed.

Remember name for (hours)

Specify 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, the HPS Inspection Engine ignores local user accounts that it 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, HPS Inspection Engine 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 HPS Inspection Engine uses the less secure LMv2 authentication variant. It is recommended to only enable this option if backwards compatibility with LMv2 is required.




Ensure That the HPS Inspection Engine Plugin Is Running

After installing the HPS Inspection Engine Plugin (and configuring it, if necessary), ensure that it is running.

To verify:

1. Select **Tools > Options > Modules**.
2. In the *Modules* pane, hover over the HPS Inspection Engine Plugin name to view a tooltip indicating if it is running on Forescout devices in your deployment.

The name is preceded by one of the following icons:

-  - The HPS Inspection Engine Plugin is stopped on all Forescout devices.
 -  - The HPS Inspection Engine Plugin is stopped on some Forescout devices.
 -  - The HPS Inspection Engine Plugin is running on all Forescout devices.
3. If the HPS Inspection Engine Plugin is not running, select **Start**, and then select the relevant Forescout devices.
 4. Select **OK**.

Testing and Verifying Connectivity

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

Remote Inspection	SecureConnector	Windows Updates	Classification	Tuning	Test
Test Address					
Connectivity Test Type					
(SNMP Test Parameters) OID					
(SNMP Test Parameters) Community					
(SNMP Test Parameters) Extra Parameters					

The following options are available:

Test Address	<p>A test IP address. Depending on the test type, the address can be used to verify:</p> <ul style="list-style-type: none"> ▪ Connectivity to the domain name, administrator and password. ▪ Remote registry connection. ▪ A running Windows service. <p>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.</p>
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	<p>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.</p> <p>Timeout – The number of seconds to wait for a response. The default timeout is 25 seconds.</p> <p>Retry – The number of times to retry sending an SNMP message. The default number of retries is 1. The upper limit is 20.</p> <p>For example, to indicate a timeout of five seconds and three retries, enter the following:</p> <p><code>-t 5 -r 3</code></p>

Configuration for an Appliance or Group of Appliances

You can create and apply 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 **+** 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.

For more information about creating and applying configurations, see the *Forescout Administration Guide*.

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 HPS Inspection Engine, you specify a set of standard protocols that are available in your environment, and are used 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, see [Appendix D: Remote Inspection and SecureConnector – Feature Support](#).

About MS-WMI

Windows Management Instrumentation (WMI) is a Microsoft tool for web-based enterprise management. WMI is used 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. Run the `dcomcnfg` utility and configure the following endpoint permissions:

- Access Permissions: Enable all
- Launch and Activation Permissions: Enable all

3. Run the `wmiimgmt.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 and Remote Procedure Calls

A Remote Procedure Call (RPC) may be submitted to the registry services (MS-RRP) 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 with 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
 - Remote Procedure Call
 - Remote Registry

Remote Procedure Calls include safeguards against SMB Relay behavior. See [Detecting SMB Relay Behavior](#).

About SMB

Server Message Block (SMB) is a protocol for file and resource sharing. This protocol is used 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 with 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.

New RPC connections are tested to determine if the endpoint is a relay. If relay behavior is detected:

- The connection is no longer used by the Forescout platform.
- 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:
 - Most properties in the Windows, Windows Applications, and Windows Security folders of the Condition tree.
 - 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.

Property Name	Property Value
config.verify_smb_relay.value	0 – No testing of RPC connections. 1 – Test every new RPC connection for SMB relay behavior. This is the default value.

Property Name	Property Value
config.response_err_if_smb_relay_value	0 – Resolve properties as for normal endpoints. 1 – Set all RPC related properties to Irresolvable for SMB relay endpoints. This is the default value.

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 helps identify SMB Relay behavior and prevent man-in-the-middle attacks.

Use the **Require SMB Signing** option on the [Remote Inspection](#) tab to configure Forescout to require 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 do so when they communicate with the Forescout platform.

When you require SMB signing, Remote Inspection can no longer be used 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>
- 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 configure Kerberos authentication, the Forescout platform interacts with Kerberos authentication servers deployed in your environment (typically on existing Active Directory instances).

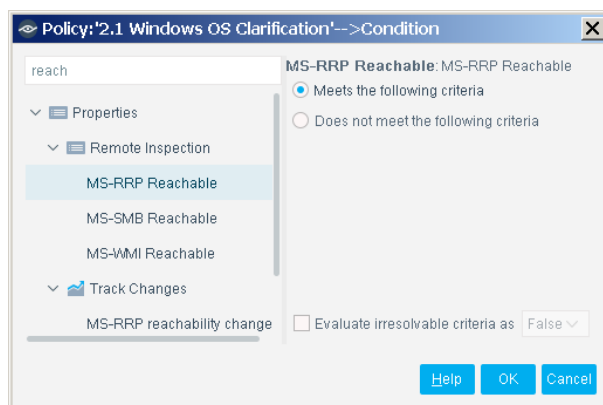
When Kerberos authentication is used for Remote Inspection, a dedicated administrator account should be defined in the domain controller and entered in the [Domain Credentials](#) tab. The HPS Inspection Engine uses this account to interact with Kerberos servers, and to perform Remote Inspection on endpoints.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

The Forescout platform uses hostnames for Kerberos authentication. If an endpoint's hostname is unknown, a reverse DNS query is performed to determine the hostname. When you work with Kerberos authentication, ensure that DNS records are regularly updated in your environment.

Kerberos authentication uses Ticket Granting Tickets (TGTs) with limited validity periods. When the Forescout platform has previously logged in successfully to an endpoint using Kerberos, and the endpoint is removed from the Domain and then rejoins, reconnection to the endpoint is blocked until the domain controller renews the TGT used for Kerberos authentication; typically, the TGT is renewed every 10 hours. During this period, resolution of properties and other Remote Inspection tasks are not performed for the endpoint.

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:

MS-RRP Reachable	Indicates whether the Remote Registry Protocol can be used for Remote Inspection tasks on the endpoint.
MS-SMB Reachable	Indicates whether the Server Message Block protocol can be used for Remote Inspection tasks on the endpoint.
MS-WMI Reachable	Indicates whether Windows Management Instrumentation can be used for Remote Inspection tasks on the endpoint.

These properties do not have an *Irresolvable* state. When HPS Inspection Engine 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 used 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.

- 📖 *PowerShell scripts cannot run 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.

When WMI is used for Remote Inspection:

- Most background scripts are run using WMI.
- WMI does not support interactive scripts (such as scripts that support Guest Registration and other HTTP-based actions) on some Windows endpoints. The `fsprocsvc` service or Microsoft Task Scheduler are used to run interactive scripts on these endpoints.
- 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\`


Use the following property to customize the directory used to download and run scripts: `config.sc_script_run_folder.value`

- 📖 *Use a double backslash (\\) or a single forward-slash (/) as directory separator (The Enterprise Manager reads a single backslash as an escape character). For example, `c:\\Windows\\temp` or `C:/Windows/temp`.*

Required folder permissions: System, admin, and user access.

It is strongly recommended to specify a secured directory.

- 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 details about the Install as system option of the **Start SecureConnector** action, see the Forescout Administration 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\`

Use the following property to customize the directory used to download and run scripts: `config.script_run_folder.value`

-  Use a double backslash (\\) or a single forward-slash (/) as directory separator. The Enterprise Manager reads a single backslash as an escape character. For example, `c:\\Windows\\temp` or `C:/Windows/temp`.

Required folder permissions: System and admin access.

It is strongly recommended to specify a secured directory.

- Interactive scripts are downloaded to and run from the %TEMP% directory of the currently logged in user.

About Secured Directories and Script Files

Because scripts that run on endpoints can be targets for malicious attack, ACL permissions are applied to directories that store scripts. This prevents 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 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>).

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.

Note that:

- The service remains on endpoints when they exit the network.
- Some Antivirus applications may report fsprocsvc as a malicious service. You may need to add this service to whitelists in your environment.

Item	Description
Footprint	<ul style="list-style-type: none"> ▪ Size on disk: Approximately 250KB ▪ Memory acquired during runtime: 2 MB ▪ Runs under: System ▪ Start type: Automatic ▪ After two hours of inactivity, the service stops
Properties requiring the service (with remote inspection, not via SecureConnector)	<ul style="list-style-type: none"> ▪ 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, not via SecureConnector)	<ul style="list-style-type: none"> ▪ 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 Forescout scripts.

Task Scheduler Limitations

Working with the Task Scheduler has the following limitations:

- It 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 selected, 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 *Linux 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. 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). MS-WMI supports event-driven monitoring and other real-time functionality.*

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**
- **Disable Dual Homed**
- **Send Balloon Notification** when the SecureConnector systray icon is visible on the endpoint

SecureConnector improves 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 SecureConnector is installed on the endpoint, 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 Forescout traffic between SecureConnector and the Appliance takes place over 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. This is sometimes referred to as "HPS redirect".

 *In environments that have overlapping IP addresses, the connection is **not** seamlessly re-created. For more information refer to the Working with Overlapping IP Addresses How-to Guide.*

Permanent vs. Dissolvable Deployment

You can configure SecureConnector 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.

Event Driven Monitoring of Host Properties

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

The host properties updated using event-driven monitoring are listed in [Appendix D: Remote Inspection and SecureConnector – Feature Support](#).

Installing and Running SecureConnector

The following methods can be used to install and run SecureConnector on endpoints:

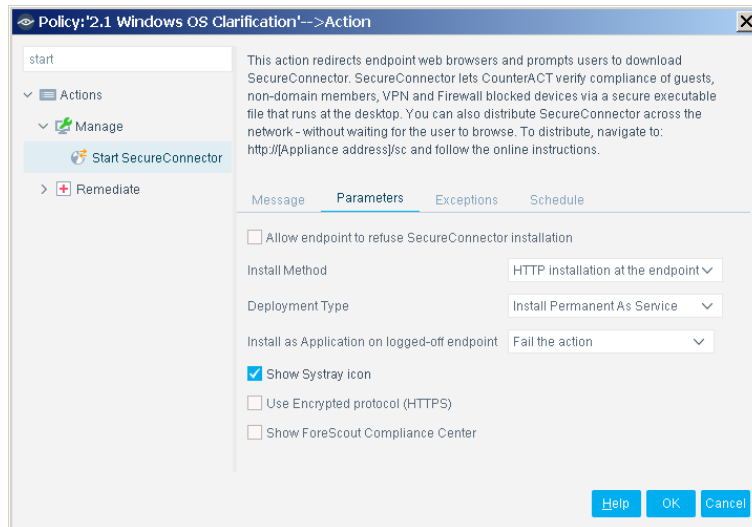
- **Policy-based deployment:** By including the **Start SecureConnector** action in a policy, you can selectively deploy SecureConnector in response to classification or other policy-based evaluation of endpoints.

The **Start SecureConnector** action supports background or interactive installation:

- Background installation connects to endpoints using Remote Inspection.
- Interactive installation redirects endpoint browsers to a download page, from which end users install SecureConnector.

If the SecureConnector package is already installed on an endpoint, applying the **Start SecureConnector** action upgrades and restarts SecureConnector on the endpoint.

For deployment options and additional details, refer to the *Forescout Administration Guide*.



- **Installer-based deployment:** You can deploy SecureConnector on any number of endpoints by downloading an installer package from a CounterACT device, and then distributing the file.

Two types of installers are supported:

- Use the same installer package used by the **Start SecureConnector** action. See [Download or Link to a SecureConnector Installer Package](#).
- Generate an MSI installer package. Your deployment tools use Windows Installer commands to install or uninstall SecureConnector. See [Generate an MSI Installer for SecureConnector](#).



You can use SecureConnector log files to troubleshoot SecureConnector issues. See [Appendix C: SecureConnector Log Files](#).

- For appliances that are configured with overlapping IP addresses, SecureConnector installers are not uniform across the network. In each overlapping site, SecureConnector must be downloaded from an Appliance in the site. SecureConnector can only communicate with this Appliance. For more information, see the Working with Overlapping IP Addresses How-to Guide.

Download or Link to a SecureConnector Installer Package

Distribute SecureConnector to endpoints by downloading an installation file from an Appliance, and then using the following methods to distribute the file:

- Windows login script or domain group policy – an advantage to this method is that installation is silent.


- Any third-party software maintenance tool.
 - Direction installation by IT staff using physical media, such as a USB stick.
-  *It is also possible to deploy SecureConnector as part of a machine image. For details, refer to the Deploying SecureConnector as a Service as Part of a Machine Image How-to Guide.*
- Email distribution of a link to the installer package on a CounterACT device. Users must save and launch the installer.
-  *The Forescout SecureConnector Distribution Tool page used to access these installers is not accessible when HTTP Redirection is disabled (Options > General > Web Server Configuration > Disable Web Portals).*

To distribute SecureConnector via file or link:

1. Browse to the following location:

`https://<Appliance_IP>/sc`

where <Appliance_IP> is the IP address of Enterprise Manager or an Appliance.



2. Define the SecureConnector settings (described above).
 - Whether to place an icon on the endpoint systray.
 - How to install SecureConnector on the endpoint:
 - As a permanent service
 - As a permanent application
 - As a dissolvable utility

3. Select **Submit**.

Forescout Agent Download

Select Version

- ☐ Win32
☒ Win64


Your SecureConnector configuration has been saved and is ready for download. Once downloaded, SecureConnector can be distributed across any network segment using standard distribution methods, for example, you can send the following link via email:

https://10.150.178.42/x64/SC-CqCyKicTqQgZ5PuVMvSYLi9KLdFYe0p91Fc+NMYS06OD0w_cFbAEAAE-.exe

Note: If your environment uses overlapping IP addresses, refer to the [Forescout Working with Overlapping IP Addresses How to Guide](#).

Download

4. Specify whether the SecureConnector agent is for a 32-bit or 64-bit system.

 *To support end users who are redirected to this page, the installer for the browsing machine is selected by default.*

5. 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 path.
6. Send the file or link to endpoints via login script, email, or any other method.
 - If the file is distributed, end users 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 is distributed, instruct end users to select **Run** when prompted.
7. Create a policy that uses the **Windows Manageable (SecureConnector)** property to verify that SecureConnector is installed on target endpoints.

After installation using this method, SecureConnector initially connects to the Appliance from which the installer link or file was copied. SecureConnector is then redirected to the Appliance that manages the endpoint. These initial connections place a momentary load on the Appliance that provides the installer package.

Generate an MSI Installer for SecureConnector

Use this procedure to generate a SecureConnector installer package in .msi format. This installer can be used with Windows Installer tools and commands to deploy and uninstall SecureConnector on Windows endpoints.

The MSI installer installs SecureConnector as a Permanent Service on the endpoint.

To generate an MSI installer for SecureConnector:

1. Browse to the following location:

`https://<EM_IP>/sc-installer`

where <EM_IP> is the IP address of Enterprise Manager.

ForeScout SecureConnector MSI Installer Packages

This download page provides MSI packages that install ForeScout SecureConnector on Windows endpoints. These installers duplicate the functionality of the **Start SecureConnector** action in ForeScout CounterACT. Use these installer packages to distribute SecureConnector to endpoints in your environment using existing MSI tools.

For 32-bit Windows systems use [this MSI package](#).

For 64-bit Windows systems (x64/Intel64/AMD64) use [this MSI package](#).

A typical msi command using these packages takes the following format:
msiexec.exe /i SecureConnectorInstaller.msi MODE=<mode_value>
 The following table shows string values for the MODE parameter that let you specify installation options. When you submit the msi command, use a <mode_value> string from the table below.

	Show SecureConnector icon in System Tray After Installation	Invisible After Installation. No SecureConnector icon in System Tray
Install as Permanent Service. (SecureConnector runs before/after user session)	CisBKicTTXg1TSY0R+EQ5zOjh7DKRmK3f9W_xJdev08f3UVsAOYFAAE-	CisBKicTTXg1TSY0R+EQ5zOjh7DKRmK3f9W_xJdev08f3UVsAOYFAAE-

What happens when the installer runs?

The final step of SecureConnector installation is to establish a connection between the endpoint and the CounterACT device that will manage it.


When these installers run on an endpoint:

1. The installer installs SecureConnector on the endpoint.
2. SecureConnector opens an encrypted, authenticated tunnel to the CounterACT Enterprise Manager (10.43.1.42).
3. The Enterprise Manager redirects the endpoint to its managing CounterACT Appliance for ongoing management.
4. SecureConnector then opens an encrypted, authenticated tunnel to this CounterACT Appliance to initialize the management relationship.

By default, these connections use TCP on Port 10003. Refer to the Endpoint Module Configuration Guide for details of how to change connection defaults.

 *This page is not accessible when HTTP Redirection is disabled (Options > General > Web Server Configuration > Disable Web Portals).*

2. Download the installer for 32-bit or 64-bit machines, as appropriate.
3. When these installers run, they parse the MODE parameter to determine the options used to install SecureConnector. Your Windows Installer statement must specify the MODE parameter, and provide one of the string values shown on the download page.

 *One installer package supports several SecureConnector configurations, depending on the MODE value specified.*

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

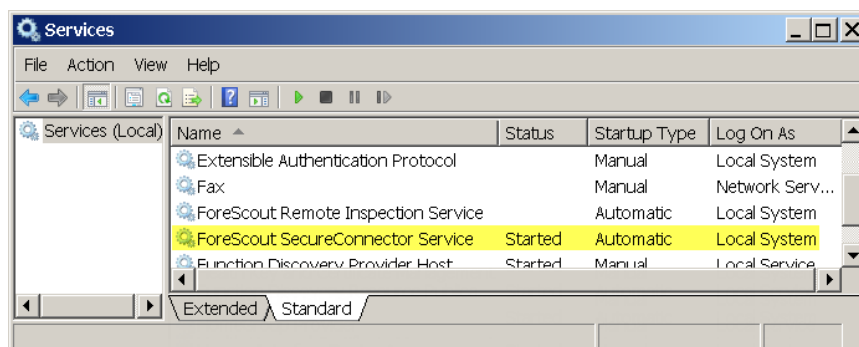
After installation using this method, SecureConnector initially connects to the Enterprise Manager that provided the installer. SecureConnector is then redirected to the Appliance that manages the endpoint. These initial connections place a momentary load on the Enterprise Manager.

The SecureConnector Executable

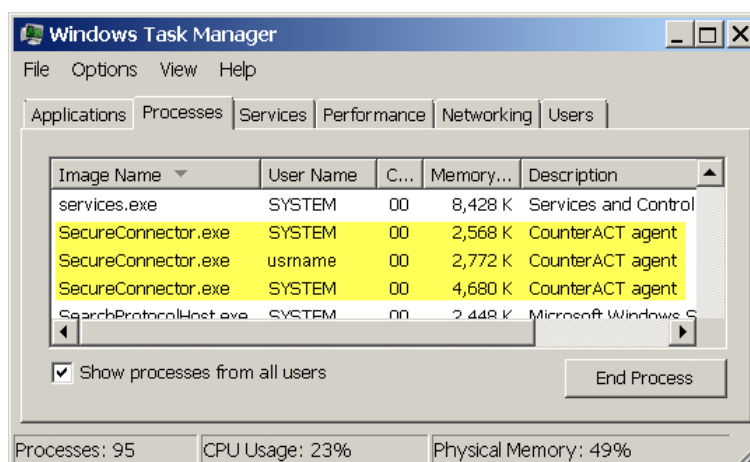
When activated by the HPS Inspection Engine, `SecureConnector.exe` runs on Windows endpoints. Activation occurs when the Start SecureConnector action is selected or when SecureConnector is otherwise installed. See [Appendix C: SecureConnector Log Files](#) for details.

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

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 in 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 in the Task Manager on the endpoint.



In this example, 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 and View Compliance Center).
- One SecureConnector.exe process is the SecureConnector service. (If SecureConnector is installed as an application, 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.*

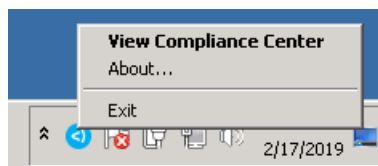
The SecureConnector ID

When SecureConnector connects to the CounterACT Appliance, it sends a unique ID that helps to identify the endpoint. The HPS Inspection Engine may 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, the system concludes this is a new machine, deletes all previous information, and relearns 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, all information learned on the older IP address is moved to the new IP address (the old IP address is changed to the new one).

Stop SecureConnector

When the SecureConnector toolbar icon is visible, end users can stop SecureConnector on their devices by selecting **Exit** from the SecureConnector toolbar menu. SecureConnector stops, *but is not uninstalled*.

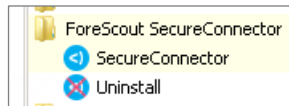


When you [configure the HPS Inspection Engine](#), you can enable password protection for SecureConnector on endpoints. When password protection is enabled, users who try to **Exit** SecureConnector are prompted for a password.

Uninstall SecureConnector

The following methods can be used to stop and uninstall SecureConnector:

- **Policy-based uninstall:** SecureConnector is uninstalled from endpoints that match the conditions in a Forescout policy using the **Stop SecureConnector** action.
- **Interactive uninstall:** End users or IT staff can select the **Uninstall** option from the Forescout SecureConnector folder.



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

- **CLI or script-based uninstall**, using the following command:

```
SecureConnector.exe -uninstall [-silent] [-p <password>]
```

Where

-silent suppresses an on-screen confirmation message

-p <password> is used when SecureConnector is password protected.

- **MSI-based uninstall**, using the packages and parameters described in [Generate an MSI Installer for SecureConnector](#).

If password protection is enabled for SecureConnector, use the PASSWORD parameter in your Windows Installer statement to provide the password string. The password string should be unencrypted (clear text).

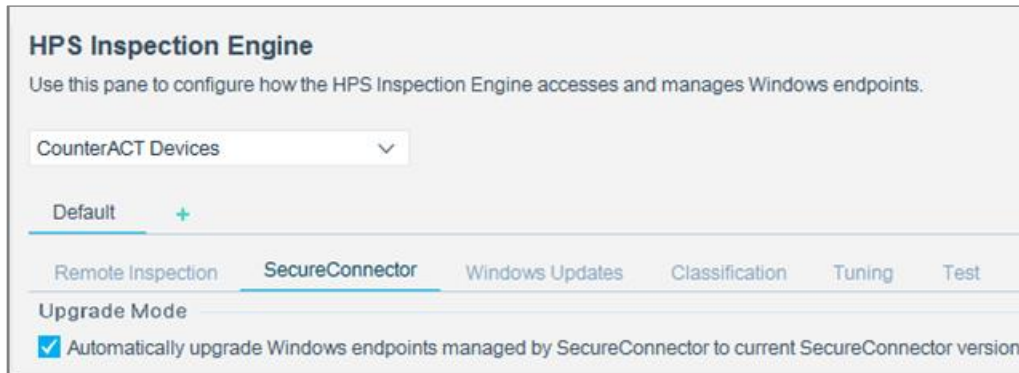
Updating SecureConnector

Several versions of SecureConnector can be present in your environment simultaneously. For example:

- When you upgrade the Endpoint Module, endpoints continue to run the previous version of SecureConnector until you distribute the updated version. New functionality is not yet available.
- New versions of the Endpoint Module may contain updates to SecureConnector. The updated version of SecureConnector is installed on endpoints when you apply the **Start SecureConnector** action, or if you download and distribute an installation package from the Enterprise Manager.
- Similarly, if you roll back the Endpoint Module, endpoints continue to run the SecureConnector version that they received before rollback, which may contain functionality not supported after rollback of the Endpoint Module.
- Endpoints may not be present on the network to receive a SecureConnector update.


This section describes how to distribute updates to SecureConnector on Windows endpoints.

In the SecureConnector tab of the HPS Inspection Engine configuration pane, the **Automatically upgrade Windows endpoints managed by SecureConnector to current SecureConnector version** option indicates the version of SecureConnector for Windows provided by the Endpoint Module.



This option determines how SecureConnector is updated on Windows endpoints:

- Select this option to automatically distribute new versions of SecureConnector to all Windows endpoints managed by SecureConnector. When you upgrade the Endpoint Module, the new version of SecureConnector is automatically downloaded to Windows endpoints that are running SecureConnector.

 *This was the default behavior of the HPS Inspection Engine until this release.*

In networks with large numbers of endpoints managed by SecureConnector, this download behavior can cause a spike in network resource usage.

- Clear this option to disable automatic updates of SecureConnector each time you upgrade the Endpoint Module. Use one or more policies based on the **Windows SecureConnector Update** template to update SecureConnector on endpoints gradually, and with greater control.

When you enable automatic updates, no further configuration is required.

When you disable automatic updates of SecureConnector, use the following tools to manage the versions of SecureConnector for Windows that run in your environment.

- The Windows SecureConnector Version property indicates the SecureConnector version installed on a Windows endpoint.
- The SecureConnector Compatibility property indicates whether the SecureConnector version running on the endpoint is compatible with your Forescout environment. When this property is evaluated as *Partially Compatible*, only functionality common to both the endpoint and Forescout is supported.

- The Update Installed SecureConnector action updates SecureConnector on the endpoint so it is fully compatible with Forescout. This action only affects endpoints that are already running SecureConnector. Depending on the version running on the endpoint, this action either upgrades or rolls back SecureConnector. The update preserves the existing deployment type and other settings. For example, if SecureConnector runs as a permanent service with a visible System Tray icon, these settings are duplicated during update.
- The Windows SecureConnector Update template provides a sample policy for SecureConnector version management. This template uses the SecureConnector Compatibility property to detect Windows endpoints on which SecureConnector must be updated. The policy uses the Update Installed SecureConnector action to update SecureConnector on these endpoints.

To manage SecureConnector versions on Windows endpoints, create one or more policies based on the Windows SecureConnector Update template. Each time an Endpoint Module upgrade includes a new version of SecureConnector for Windows, run these policies to detect endpoints that require SecureConnector update.

- 📄 *To gradually update SecureConnector across your network environment, you can define several policies with different network scopes, or additional policy conditions that detect endpoints based on endpoint type or function.*
- 📄 *To fine-tune update behavior, examine Inventory views for the SecureConnector Compatibility property. Many endpoints may require SecureConnector update when significant new functionality is introduced.*

SecureConnector Details

Item	Description
Size on disk	Approximately 2 MB
Endpoint memory utilization	<p>Process mode:</p> <ul style="list-style-type: none"> ▪ Main process: 3MB – 6MB ▪ Watchdog process: 400kB – 600kB <p>Service mode:</p> <ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Using Remote inspection methods ▪ Browser – Using HTTP redirection. Defined in the Start SecureConnector action. ▪ Browser – Direct setup file download. Described in this guide. See Installing and Running SecureConnector.

Item	Description
SecureConnector privilege level	<p>Ideally, SecureConnector should be installed as a service on corporate endpoints. This ensures that all SecureConnector related features are available irrespective of the user logged on to the machine.</p> <p>When SecureConnector is installed as a service, it runs with Administrator privileges even when the current logged in users are not administrators.</p> <p>When SecureConnector is installed as an application, privileges are determined by the currently logged in user, even if a user with administrator privileges was used to install SecureConnector. The following actions do not work if the currently logged in user does not have administrator privileges:</p> <ul style="list-style-type: none"> ▪ Disable External Devices ▪ Kill Process (for processes that do not belong to the SecureConnector user) ▪ Disable Dual Homed <p>Privilege levels are determined in part by the mode in which SecureConnector is installed. The mode is determined when configuring the Start SecureConnector action.</p> <p>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.</p>
Installation folder when installed permanently	<p>Under %ProgramFiles% if setup runs with Administrator (or SYSTEM) privileges.</p> <p>Under %AppData% when setup runs with non-Administrator privileges or setup is affected by UAC.</p>
Folder used when deployed in dissolvable mode	Under %Temp%.

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:

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.

Detect NAT Behavior Based on SecureConnector Connections

NAT devices can be detected by examining the IP addresses used by endpoints to connect to SecureConnector on Appliances. After an endpoint connects to SecureConnector, the HPS Inspection Engine 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 HPS Inspection Engine instance controls this behavior.

To enable or disable NAT detection:

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

```
fstool va set_property config.report_nat_device_sc.value true
```
3. Repeat this command on all Appliances.
4. From the Console, restart all HPS Inspection Engine instances.
5. To disable NAT detection, submit the following commands, as relevant:

```
fstool va set_property config.report_nat_device_sc.value false
```
6. Repeat this command on all Appliances.
7. From the Console, restart all HPS Inspection Engine instances.

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 the endpoint corresponding to the interface used by SecureConnector is identified as *Managed 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

actions 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.

Using Certificates to Authenticate the SecureConnector Connection

When endpoints managed by SecureConnector access the network, the SecureConnector client on endpoints connects to the CounterACT Appliance that manages the endpoint. Configuration options in the [SecureConnector](#) tab let you secure this client-server connection using an X.509-compliant public key certificate.

Certificate-based authentication is implemented for all SecureConnector deployment types: Permanent as Service, Permanent as Application, and Dissolvable.

Choose one of these authentication methods for SecureConnector connections:

- Use the predefined Forescout self-signed certificate. This is the default server authentication method used by SecureConnector clients. The Appliance presents a pre-existing certificate defined in Forescout eyeSight.
- Use a self-signed or domain validated certificate unique to your network environment. You must import these certificates at the Forescout Console.
- Use a certificate signed by a third party Certificate Authority (CA). You must import these certificates and trust chains at the Forescout Console.

Use the Trusted Certificates and System Certificates panes of the Console to install the required trust chains and certificates in Forescout. Specify the relevant plugins of the Endpoint Module when you configure the Scope/Subsystem fields. For details, refer to the *Forescout Administration Guide*.

About Server Certificates for CounterACT Appliances

In this interaction, the CounterACT Appliance presents a certificate to the SecureConnector client. Note that:

- Trust information is distributed with the SecureConnector client, based on the certificates and trust chains imported into the Console. If no certificates are imported into Forescout eyeSight, the default self-signed certificate provided by eyeSight is used.
- OCSP responders listed in the certificate are queried to verify certificate validity. CRLs and CDPs are not supported.
- When multi-domain certificates are used, SecureConnector authenticates the certificate using the Subject Alternate Name (SAN) extension field in addition to the Subject Common Name field.

To support this authentication interaction:

- Enable the **SecureConnector client verifies CounterACT server certificate chain** option in the [SecureConnector](#) tab.

- To use a certificate unique to your environment, import the certificate and its trust chain into the *System Certificates* tab of the Console's Certificates interface. Select the HPS Inspection Engine in the Scope tab.
- For certificates signed by a CA, use your environment's PKI tools to distribute trust chain information to endpoints.

The server certificate presented by CounterACT Appliances to SecureConnector clients is the default Forescout self-signed certificate, or the certificate you imported into the Forescout Console.

About SecureConnector Client Certificates

When Forescout runs in Certification Compliance mode, optional configuration settings let you require a client-side certificate. When this option is enabled, SecureConnector on endpoints must present a certificate to the CounterACT Appliance. Refer to the *Forescout Installation Guide* for more information about Certification Compliance mode.

Certificate-Based Rapid Authentication of Endpoints

Typically Forescout 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 Forescout eyeSight and eyeControl 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.

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.

The following describes a typical scenario 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 the Forescout platform. Endpoints are granted immediate network access based on a signed X.509 digital certificate. eyeSight continues the compliance checks defined in active policies, and may revoke or change endpoint access if these checks fail.
- A corporate policy may grant limited network access to endpoints without a valid rapid authentication certificate, or with an expired or revoked certificate, or endpoints not managed by SecureConnector, until normal, policy-driven compliance checks are run.

For more information about implementing certificate-based rapid authentication in your environment, refer to the *SecureConnector Advanced Features How-to Guide*.

Endpoint Module Information

The HPS Inspection Engine is installed as part of the Forescout Endpoint Module.

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

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

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

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

Additional Forescout Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 *Software downloads are also available from these portals.*

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend products. The portal also provides additional documentation.

To access the Product Updates Portal:

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

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend products. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

Console Help Buttons

- Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with in the Console.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Product Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

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

Appendix A: Endpoint Ports and Executable Files Used by HPS Inspection Engine

This section gives more detail about how the HPS Inspection Engine interacts with Windows endpoints.

Endpoint Ports

To establish basic connectivity and to determine if an endpoint is manageable, the HPS Inspection Engine attempts to connect to endpoints on certain ports. In addition, certain ports are used to perform nmap scans and to resolve properties such as the **Open Ports** property.

If ICMP is disabled in the network due to Firewall settings, the **Open Ports** property always reports **Open** for UDP ports. UDP does not require a response as part of its protocol. Therefore, if an ICMP unreachable response is received, the Open Ports property is reported as **Closed**. Otherwise, the Open Ports property is reported as **Open**. Without an ICMP response, UDP port scans always report the ports as **Open**. Therefore, policies should not include UDP scans.

Basic Connectivity Tests

The following queries determine connectivity and manageability:

- ICMP Ping test - 3 attempts sending ICMP packets (ICMP_ECHO, ICMP_TSTAMP, ICMP_MASKREQ)
- SYN test – If the ICMP test fails, we scan the following ports using TCP:
80, 21, 22, 23, 25, 113, 31339
- ACK test – If the SYN test fails, we scan the following ports using TCP:
80, 113, 443, 10042

Nmap Scans for Classification

If banner or fingerprint scanning is enabled, these scans use the ports described in [Nmap Scan Commands Used by HPS Inspection Engine](#).

UDP Scans to Resolve Open Ports

To resolve the **Open Ports** property for a UDP port, we confirm connectivity by using UDP to connect to five ports chosen randomly in the range 40000-65535

The following table summarizes ports that may be queried by the HPS Inspection Engine.

Port	Protocol	Basic Connectivity	Nmap Scans
4	TCP		✓
21	TCP	✓	✓
22	TCP	✓	✓
23	TCP	✓	✓

Port	Protocol	Basic Connectivity	Nmap Scans
25	TCP	✓	✓
53	TCP		✓
79	TCP		✓
80	TCP	✓	✓
88	TCP		✓
110	TCP		✓
111	TCP		✓
113	TCP	✓	
135	TCP		✓
139	TCP		✓
143	TCP		✓
220	TCP		✓
443	TCP	✓	
445	TCP		✓
513	TCP		✓
515	TCP		✓
631	TCP		✓
1723	TCP		✓
3389	TCP		✓
5900	TCP		✓
8080	TCP		✓
9100	TCP		✓
10042	TCP	✓	
30339	TCP	✓	
41351	TCP		✓
62078	TCP		✓
N/A	ICMP	✓	

Port	Protocol	Basic Connectivity	Nmap Scans
40000-65535	UDP	✓	

Endpoint Executables

The following executable files may be 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	
Name	Description
fsprocsvc.exe install_fsprocsvc.exe	fsprocsvc.exe runs scripts for several Forescout tasks. The service is similar to Microsoft's PsTools (part of Windows Sysinternals tools: http://technet.microsoft.com/en-us/sysinternals/default.aspx). 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.
SecureConnector.exe	The SecureConnector executable.
fs_DeviceControl.exe	Resolves the <i>External Devices</i> property.
fs_CalcHash.exe	Resolves the Windows File MD5 Signature property.
fs_NBTDomain.exe	Resolves the NetBIOS Domain property
Additional Files	
fs_apps.vbs	Resolves the Windows Applications Installed property.
fs_auto_updates.vbs	Performs the Windows Self-Remediation action.
fs_dot1x.vbs	Resolves host properties provided by the RADIUS Plugin.
fs_http_notify_g4.vbs	Supports the HTTP Notification action.
fs_http_upload.vbs	Resolves the Microsoft Security > Vulnerabilities property.
fs_kb.vbs	Resolves the Microsoft Security > Vulnerabilities property.

fs_kill_proc.vbs	Kills local processes to support Kill... actions.
fs_reg_edit.vbs	Performs the Set Registry Key on Windows action.
fs_sched_task_rm.vbs	Utility for running scripts with Task Scheduler.
fs_user.vbs	Supports the User property.
fs_wmi.vbs	Resolves the Windows Security Center Antivirus Status property.
fs_workgroup.vbs	Resolves the Device Information > User property for endpoints running Vista on WORKGROUP.
fs_wua_full.vbs	Performs the <i>Start Windows Updates</i> action.
fs_wua_search.vbs	Used for Microsoft Security > Vulnerabilities properties.

HPS Inspection Engine 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 [Networking Requirements](#).
- 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 Remote Inspection can be performed on these machines. This means that you should have access to 445/TCP or 139/TCP to retrieve Windows-related information. By default, these ports are open on Windows 2000 machines.*
- Access to the endpoint's file system. If RRP is used for Remote Inspection, the remote registry must also be accessible. Refer to the *Forescout Administration Guide* 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

To test the domain credentials:

1. Log on to a desktop machine using the Forescout user name and password. If this fails, check the Forescout user settings on the Domain Controller.
2. Check that the desktop machine is a member of the Domain and authenticates against the Domain Controller.
3. Check that the login uses Domain, rather than localhost credentials.

Test the Credentials on a Desktop Using a Localhost Query

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

To perform this test:

1. Log on to a desktop machine using any credentials other than the **Forescout** 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 Forescout.
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. It might need to be more fully qualified. For example, DOMAIN, DOMAIN.COM or HQ.DOMAIN.COM
- Check the credentials on the Domain Controller.

Test the Credentials on a Desktop Using Remote Query

To perform this test:

1. Log on to 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 **Forescout** user

<domain> is the fully qualified domain name of the network

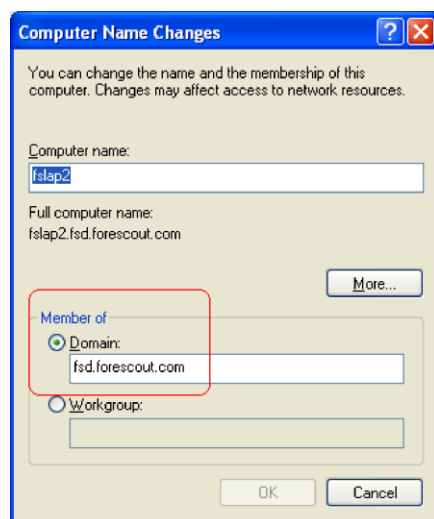
<username> is the user account defined in Forescout

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 > Panel > System**. In 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 configuration screen. Run 'nbtstat -n' to see the following output.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\gil>nbtstat -n

Wireless Network Connection 5:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Local Area Connection:
Node IpAddress: [10.0.0.50] Scope Id: []

        NetBIOS Local Name Table

        Name                Type             Status
        ----                -
        FSLAP2               <00>             UNIQUE          Registered
        FSLAP2               <20>             UNIQUE          Registered
        FSD                   <00>             GROUP           Registered
        FSD                   <1E>             GROUP           Registered

C:\Documents and Settings\gil>_

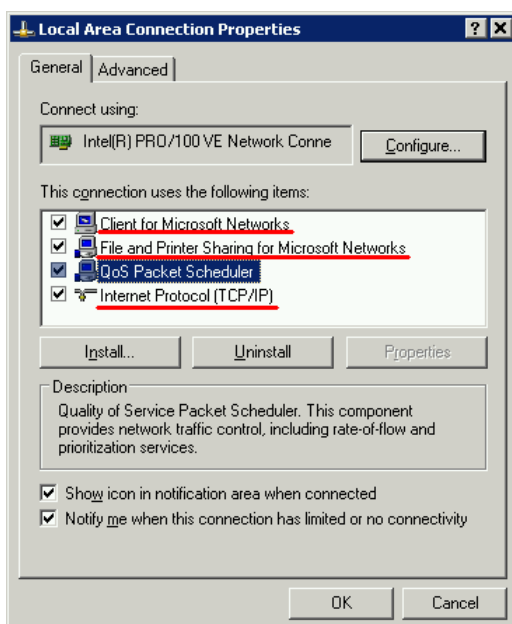
```

TCP/IP Configuration Test

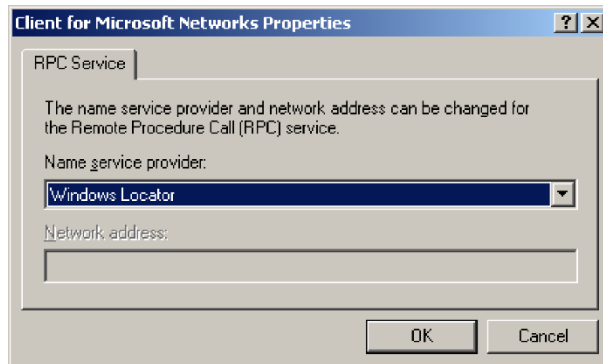
Open the properties dialog box of the relevant network connection.

To view the network connection properties:

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



3. Verify that the Client for Microsoft Networks is configured as follows:



Port Setup Test

Depending on the Remote Inspection method used and the Windows versions running on target endpoints, TCP ports 445 and 139 should be accessible.

Group Policy Test

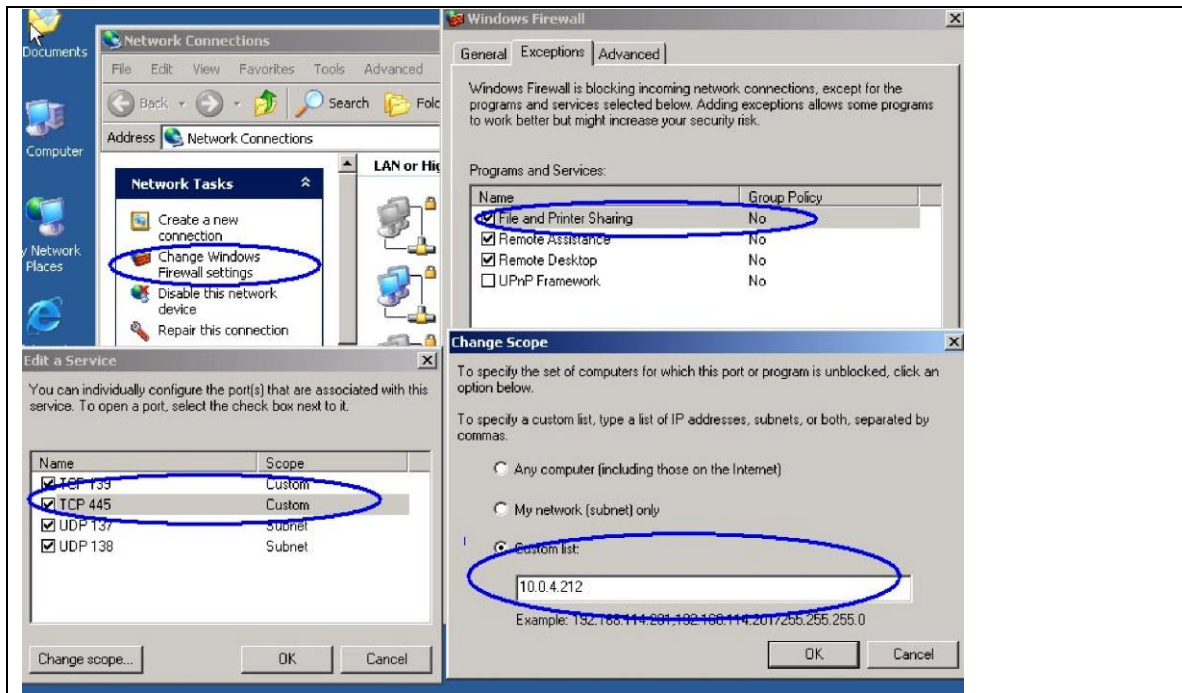
In a Windows XP group policy, the domain can be configured to set the end-system's Windows Firewall settings. Refer to "Working with Windows XP SP2 Machines" in the *Forescout Administration Guide* for more information.

Local Configuration of Windows Firewall

You can configure Windows Firewall to allow incoming network connections on TCP ports 445 and 139.

To allow incoming network connections:

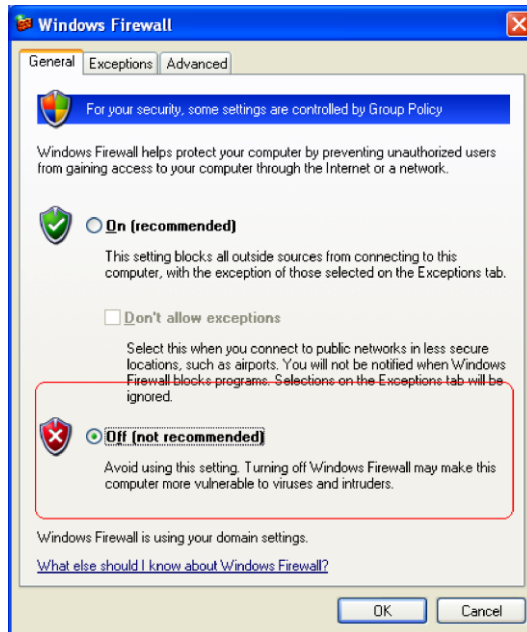
1. Select **Start > Settings > Control Panel > Windows Firewall** to display the Windows Firewall dialog box.



2. Select the **Exceptions** tab and then select **File and Printer sharing**.
3. Verify that the TCP 445 and TCP 139 ports are selected in the Edit a Service dialog box.
4. Choose **Change Scope** for each port and add the Forescout IP address in the Custom List.

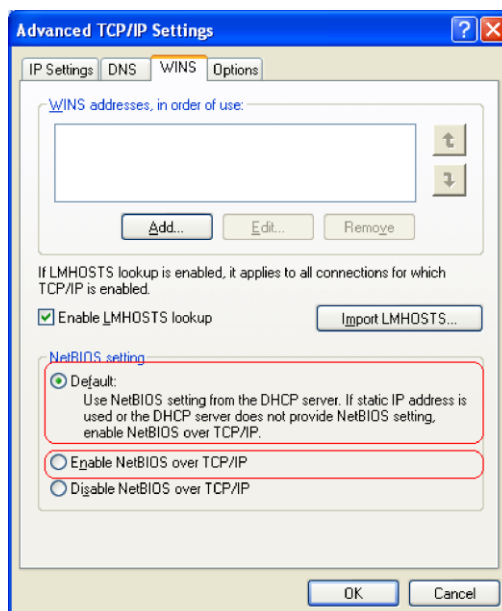
Disabling Windows Firewall

For testing purposes, you can disable the Windows Firewall from the Windows Firewall dialog box.



NetBIOS over TCP/IP Setup Test

You can enable NetBIOS over TCP/IP directly or from the DHCP server by selecting the **Default** option or the **Enable NetBIOS over TCP/IP** option in the Advanced TCP/IP Settings.



Services Test

Verify that the required services are running.

To verify the services are running:

1. Open the services view by selecting **Start > Control Panel > Administrative Tools > Services**.
2. Verify that the following services are running:
 - ServerWhen RRP is used for Remote Inspection:
 - Remote Procedure Call (RPC)
 - Remote Registry ServiceWhen 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 the services are running, but Forescout eyeSight reports that services are not running, for example:

`rpc_service_server_down:err`

There may be a memory related issue on the endpoint that is preventing Windows from properly using those services.

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

<https://support.microsoft.com/en-us/kb/2404366>

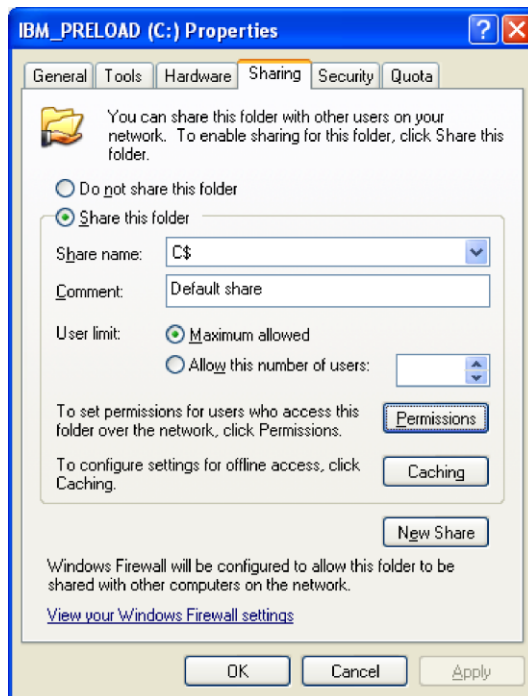
<https://support.microsoft.com/en-us/kb/981314>

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. Select the Sharing tab, and verify the following configuration:



Disable the "Use simple file sharing" Option

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

To disable simple file sharing:

- Select **My computer > Tools > Folder Options**, select the View tab, and 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 40 M. When the active log file `sc.log` reaches this size limit, it is saved as a timestamped archive file. The timestamp indicates the date and time range of events recorded in the file. By default, two archive files are retained in addition to the active log file. For example, the following files 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 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 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 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, two files are retained. Each archived log file is 40 M 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.

```
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 command:

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

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

```
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 Forescout features that are supported by Remote Inspection and/or by SecureConnector and provides information about the benefits of using SecureConnector.



A green checkmark indicates the feature is supported.



A red x indicates a feature is not supported.



A yellow checkmark indicates the feature is supported, but requires the fsprocsvc.exe service.

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

Feature	Type	Technology			Benefits of SecureConnector
		RI WMI	RI RRP	Secure Connector	
Assign to VLAN	Action	✗	✗	✓	Can assign an endpoint behind VoIP to VLAN without bouncing switch port
Device Interfaces	Property	✓	✓	✓	
Disable Dual Homed	Action	✗	✗	✓	
Disable External Device	Action	✗	✗	✓	
External Devices	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
HTTP Redirection to URL (If Attempt to open a browser at the detected endpoint is selected)	Action	✓	✓	✓	
Intranet WSUS Server	Property	✓	✓	✓	
Kill Process on Windows	Action	✓	✓	✓	Process is killed every second instead of every minute
MAC Address	Property	✗	✗	✓	
Microsoft Applications Installed	Property	✓	✓	✓	Event-driven real-time resolution instead of polling

Feature	Type	Technology			Benefits of SecureConnector
		RI WMI	RI RRP	Secure Connector	
Microsoft Vulnerabilities	Property	✓	✓	✓	
Microsoft Vulnerabilities Fine-tuned	Property	✓	✓	✓	
MS-RRP Reachable	Property	✓	✓	✓	Can be resolved by SecureConnector, but not relevant for endpoints managed by SecureConnector.
MS-SMB Reachable	Property	✓	✓	✓	Can be resolved by SecureConnector, but not relevant for endpoints managed by SecureConnector.
MS-WMI Reachable	Property	✓	✓	✓	Can be resolved by SecureConnector, but not relevant for endpoints managed by SecureConnector.
NetBIOS Domain	Property	✓	✓	✓	
NetBIOS Hostname	Property	✓	✓	✓	
NetBIOS Membership Type (Domain or Workgroup)	Property	✓	✓	✓	
Network Adapters	Property	✓	✓	✓	
Number of IPv4 Addresses Number of IPv6 Addresses	Property	✓	✓	✓	
Run Script On Windows (non-interactive)	Action	✓	✓	✓	
Run Script On Windows (interactive)	Action	✓	✓	✓	
Send Balloon Notification	Action	✗	✗	✓	
Set Registry Key on Windows	Action	✓	✓	✓	
SMB Relay	Property	✓	✓	✓	
SMB Signing	Property	✓	✓	✓	

Feature	Type	Technology			Benefits of SecureConnector
		RI WMI	RI RRP	Secure Connector	
Start Windows Updates	Action	✓	✓	✓	
User	Property	✓	✓	✓	
Windows Applications Installed	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows Domain Member	Property	✓	✓	✓	
Windows Expected Script Result (non-interactive)	Property	✓	✓	✓	
Windows Expected Script Result (interactive)	Property	✓	✓	✓	
Windows File Date	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows File Exists	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows File MD5 Signature	Property	✓	✓	✓	
Windows File Size	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows File Version	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows File Version Comparison	Property	✓	✓	✓	
Windows Hotfix Installed	Property	✓	✓	✓	
Windows Is Behind NAT	Property	✓	✓	✓	
Windows Last Login Event	Property	✗	✗	✓	Requires SecureConnector installed as a service
Windows Logged On	Property	✓	✓	✓	
Windows Manageable Domain	Property	✓	✓	N/A	
Windows Manageable Domain (Current)	Property	✓	✓	N/A	

Feature	Type	Technology			Benefits of SecureConnector
		RI WMI	RI RRP	Secure Connector	
Windows Manageable Local	Property	✓	✓	N/A	
Windows Manageable SecureConnector	Property	N/A	N/A	✓	
Windows Processes Running	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows Registry Key Exists	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows Registry Value	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows Registry Value Exists	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows SecureConnector Deployment Type	Property	N/A	N/A	✓	
Windows SecureConnector Connection Encryption	Property	N/A	N/A	✓	
Windows SecureConnector Systray Display	Property	N/A	N/A	✓	
Windows Services Installed	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows Services Running	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows Shared Folders	Property	✓	✓	✓	Event-driven real-time resolution instead of polling
Windows Update Agent Installed	Property	✓	✓	✓	
Windows Updates Installed – Reboot Required	Property	✓	✓	✓	

Related Plugins

SecureConnector and Remote Inspection both support the properties and actions provided by other components, such as the NIC Vendor DB Content Module.

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

User Accounts to Run Scripts on Managed Endpoints

This table summarizes the user accounts that are used by processes and scripts on managed endpoints to resolve host properties and implement actions.

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

Method Used to Run Scripts	Non Interactive Scripts Run As	Interactive Scripts Run As
fsprocsvc.exe	System user	Current logged-in user
WMI	User configured in HPS Inspection Engine	(Not Available with WMI)
Task Scheduler	User configured in HPS Inspection Engine	Current logged-in user
SecureConnector installed as service	System user	Current logged-in user
SecureConnector installed as application	Current logged-in user	Current logged-in user