Host Checker
Deployment Guide
Host Checker Deployment Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
Contents

Overview.................................................................................................................................................. 5
Client-side Requirements for Host Checker ................................................................................................. 5
  Qualified Platforms.................................................................................................................................. 5
  Compatible Platforms............................................................................................................................... 5
Windows Clients ........................................................................................................................................... 6
  Installer Package Files and File Location.................................................................................................. 6
  Additional Installer Package Files and File Locations ............................................................................. 6
  Files Remaining After Uninstall ............................................................................................................ 8
  Registry Modifications ............................................................................................................................. 8
Macintosh Clients ........................................................................................................................................ 9
  Application and Additional Files Installed by Host Checker ................................................................. 9
  Files Remaining After Uninstall ............................................................................................................ 9
  Log files Installed by Host Checker ...................................................................................................... 10
Linux Clients ............................................................................................................................................... 10
  Files Created by Host Checker After Installation and Connection Establishment ................................ 10
  Files Remaining After Uninstall ............................................................................................................ 10
  Log Files Installed by Host Checker ...................................................................................................... 10
Required Rights to Run and Install Applications ...................................................................................... 11
Configuring Global Host Checker Settings .............................................................................................. 12
  Perform Check Every X Minutes ............................................................................................................ 12
  Client-side Process, Login Inactivity Timeout ....................................................................................... 12
  Auto-upgrade Host Checker ................................................................................................................... 13
  Perform Dynamic Policy Reevaluation ................................................................................................. 13
  Create Host Checker Connection Control Policy ................................................................................... 13
  Virus Signature Version Monitoring .................................................................................................... 13
  Host Checker Policies .............................................................................................................................. 14
Configuring a Host Checker Policy ........................................................................................................... 16
  Predefined Antivirus Check ................................................................................................................... 16
  Predefined Firewall Policy ..................................................................................................................... 17
  Predefined Anti-Spyware Policy ............................................................................................................. 19
  Predefined: OS Checks ........................................................................................................................... 19
  Predefined: Hard Disk Encryption ......................................................................................................... 21
  Predefined: Patch Management ............................................................................................................ 22
  Custom 3rd Party NHC Check ............................................................................................................. 23
  Custom Ports Policy .............................................................................................................................. 23
  Custom Process Policy ........................................................................................................................... 24
  Custom File Policy ................................................................................................................................. 25
Custom Registry Settings Policy ................................................................. 26
Custom NetBIOS Policy .............................................................................. 27
Custom MAC Address Policy ................................................................. 28
Custom Machine Certificate Policy ......................................................... 29
Custom Advanced Host Checking ........................................................ 30
Custom Statement of Health .................................................................. 31
Custom Remote IMV ............................................................................... 32
Configuring Host Checker Restrictions ................................................. 33
Step by Step Configuration for a Test Scenario ..................................... 35
  Objective ............................................................................................... 35
  Configuration ....................................................................................... 36
Overview

Host Checker is a client-side agent that performs endpoint checks on hosts that connect to Pulse Connect Secure. You can invoke Host Checker before displaying an Pulse Connect Secure sign-in page to a user and when evaluating a role mapping rule or resource policy.

Pulse Connect Secure and Host Checker comply with the standards produced by the Trusted Network Connect (TNC) subgroup of the Trusted Computing Group. For more information about IMVs and IMCs, see www.trustedcomputinggroup.org.

Pulse Connect Secure can check hosts for endpoint properties using a variety of rule types, including rules that check for and install advanced malware protection; predefined rules that check for antivirus software, firewalls, malware, spyware, specific operating systems, third party DLLs, ports, processes, files, registry key settings, and the NetBIOS name, MAC address, or certificate of the client machine.

Client-side Requirements for Host Checker

Qualified Platforms

The platforms listed in the “qualified” category have been systematically tested by Pulse Secure QA department as part of the Pulse Connect Secure 8.3R3 release.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Operating System, List of Browsers and Java Environment</th>
</tr>
</thead>
</table>
| Windows  | • Windows 10 RedStone-2 Enterprise/Pro/Home Version 1703 build 10.0.15063.332, 64-bit, Internet Explorer 11, Edge, Google Chrome & Firefox 52 ESR, Oracle JRE 8 update 131  
  • Windows 10 Enterprise/Pro/Home, Internet Explorer 11, Edge, Google Chrome & Firefox 52 ESR, Oracle JRE 8  
  • Windows 8.1 Update/Professional Enterprise 64-bit, Internet Explorer 11, Google Chrome & Firefox 52 ESR, Oracle JRE 8  
  • Windows 7 Enterprise SP1 64-bit, Internet Explorer 11, Google Chrome & Firefox 52 ESR, Oracle JRE 8 |
| Mac      | Mac OS X 10.12, Safari 10.1, Safari 9.0 Oracle JRE 8 |
| Linux    | Ubuntu 14.04 LTS, Firefox 52, ESR, 64-bit |
| Solaris  | Agentless host check is supported on Solaris 10, 32-bit, using Firefox 24 ESR |

Compatible Platforms

The platforms listed in the “compatible” category have not been systematically tested by Pulse Secure QA department in Pulse Connect Secure 8.3R3 release but based on testing in previous releases and knowledge of the platform Pulse Secure expects that the functionality will work and will fully support these platforms.
### Platform Operating System, List of Browsers and Java Environment

#### Windows
- Windows-10 Redstone 3 Version 1709 OS Build 16299.15 64-bit, Internet Explorer 11, Edge, Google Chrome 61, Firefox 52 ESR, Oracle JRE 8 update 144
- Windows 8.1 Update/Professional/Enterprise 32-bit, Internet Explorer 11, Google Chrome & Firefox 38 ESR, Oracle JRE 8
- Windows 8 Basic edition/Professional/Home Basic/Home 32-bit or 64-bit Windows 7 Enterprise (32-bit), Internet Explorer 11, Google Chrome & Firefox 31 and later, Oracle JRE 7 and later

#### Mac
- Mac OS High Sierra Version 10.13, Safari 11.0 Oracle JRE/JDK 8
- Mac OS X 10.10, 10.11, Safari 10.1, Safari 8.0 Oracle JRE 8
- Mac OS X 10.9, Safari 9.1.3, Safari 9.0, Safari 7.0 Oracle JRE 8
- Mac OS X 10.8, Safari 6.2.8, Safari 6.0 Oracle JRE 8

#### Linux
- openSUSE 12.1, Firefox 38 ESR
- openSUSE 12.1, Firefox 52 ESR, 32-bit
- openSUSE 11.x, 10.x, Oracle JRE 8
- Ubuntu 16.04 LTS, Firefox 52, ESR, 64-bit
- Ubuntu 15.04, Firefox 52, ESR, 64-bit
- Ubuntu 12.04 LTS, 11.x, 10.x, 9.10, Oracle JRE 7 and later
- RHEL 5, Firefox 52 ESR, 32-bit
- RHEL 7, Firefox 52 ESR, 64-bit
- Fedora 23 (32 bit), Firefox 52 ESR 32-bit
- Fedora 23 (64 bit), Firefox 52 ESR 64-bit
- CentOS 6.4, Firefox 52, 32-bit/64-bit

---

### Windows Clients

To run Host Checker, Pulse Connect Secure downloads the dsHostCheckerSetup.exe package to the user's client. This package is responsible for downloading additional files to the user's system in order to run Host Checker. Host Checker deletes the dsHostCheckerSetup.exe package after installation is complete.

**Installer Package Files and File Location**

Host Checker installs the following file: `%TEMP%\dsHostCheckerSetup.exe`

**Additional Installer Package Files and File Locations**

Host Checker installs the following additional files on the client in `<% APPDATA %>\Roaming\Pulse Secure\Host Checker`: 
- AdvancedIMC.dll
- CertAuthIMC.dll
- dsHostChecker.exe
- dsHostCheckerProxy.exe
- dsHostCheckerResource_de.dll
- dsHostCheckerResource_en.dll
- dsHostCheckerResource_es.dll
- dsHostCheckerResource_fr.dll
- dsHostCheckerResourceja.dll
- dsHostCheckerResource_ko.dll
- dsHostCheckerResource_zh.dll
- dsHostCheckerResource_zh_cn.dll
- dsInstallerClient.dll
- dsnsisdll.dll
- dsWinClient.dll
- dsWinClientResource_DE.dll
- dsWinClientResource_EN.dll
- dsWinClientResource_ES.dll
- dsWinClientResource_FR.dll
- dsWinClientResource_JA.dll
- dsWinClientResource_KO.dll
- dsWinClientResource_ZH.dll
- dsWinClientResource_ZH_CN.dll
- EPCheck.dll
- hcimc.dll
- hcUtils.dll
- install.log
- JSystemIMC.dll
- libeay32.dll
- msvcp60.dll
- OpsiwatIMC.dll
- restore_win2k.txt
- restore_win98.txt
- salib_OSSL.dll
- SoHIMC.dll
- ssleay32.dll
- tnc_config
- uninstall.exe
- versionInfo.ini
- Microsoft.VC80.CRT/Microsoft.VC80.CRT.manifest
- Microsoft.VC80.CRT/msvcp80.dll
- Microsoft.VC80.CRT/msvcr80.dll
In addition, if you implement policies that download or check for third-party software, Host Checker may install additional DLLs in subdirectories of: `<% APPDATA %>`\`Pulse Secure`\Host Checker.

**Files Remaining After Uninstall**

`<% APPDATA %>`\`Pulse Secure`\Host Checker`\install.log`

**Registry Modifications**

Host Checker sets the following registry values:

<table>
<thead>
<tr>
<th>String</th>
<th>Set in</th>
</tr>
</thead>
<tbody>
<tr>
<td>browserType</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Host Checker\browserType</td>
</tr>
<tr>
<td>Device Identifier</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Device Id\DeviceId</td>
</tr>
<tr>
<td>EnableLogging</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Host Checker\EnableLogging</td>
</tr>
<tr>
<td>InstallPath</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Host Checker\InstallPath</td>
</tr>
<tr>
<td>Language</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Host Checker\Language</td>
</tr>
<tr>
<td>level</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Host Checker\Debug\dsHostChecker\level</td>
</tr>
<tr>
<td>LogFile</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Host Checker\Debug\dsHostChecker\LogFile</td>
</tr>
<tr>
<td>Product Type</td>
<td>HKEY_CURRENT_USER\Software\Pulse Secure\Device Id\SA</td>
</tr>
</tbody>
</table>

Additionally, Host Checker sets the following values in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\PulseSecure_Host_Checker:

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayIcon</td>
<td><code>&quot;&lt;%APPDATA%&gt;</code>`Pulse Secure`\Host Checker\dsHostChecker.exe&quot;</td>
</tr>
<tr>
<td>DisplayName</td>
<td>&quot;Pulse Secure Host Checker&quot;</td>
</tr>
<tr>
<td>DisplayVersion</td>
<td>current product version number</td>
</tr>
<tr>
<td>Publisher</td>
<td>&quot;Pulse Secure, LLC&quot;</td>
</tr>
</tbody>
</table>
QuietUninstallString = "<%APPDATA%>\Pulse Secure\Host Checker\uninstall.exe" /S"

StartupScript = "<%APPDATA%>\Pulse Secure\Host Checker\dsHostChecker.exe"

StopApp = "<%APPDATA%>\Pulse Secure\Host Checker\dsHostChecker.exe" -stop"

UninstallString = "<%APPDATA%>\Pulse Secure\Host Checker\uninstall.exe"

URLInfoAbout = "https://www.pulsesecure.net/"

<%APPDATA%> mentioned in above paths expands to various directories based on OS.
In Windows 7, Windows 8.1, Windows 10, C:\Users\<UserName>\AppData\Roaming

Log File Locations
You can enable or disable client-side logs through the System > Log/Monitoring > Client Logs > Settings tab of the Web console. When you enable logging, Host Checker adds log files to the following locations:

- C:\Documents and Settings\All Users\Application Data\Pulse Secure\Logging\debuglog.log (Windows XP)
- C:\Users\username\AppData\Roaming\Pulse Secure\Logging\debuglog.log (Windows Vista and Windows 7)
- C:\Users\Public\Pulse Secure\Logging\debuglog.log (Windows Vista and Windows 7)
- C:\Users\<UserName>\AppData\Roaming (Windows 8.1 and Windows 10)
- C:\ProgramData\Pulse Secure\Logging when the client has Pulse Client installed

Macintosh Clients
The following information applies to Macintosh clients only.

Application and Additional Files Installed by Host Checker
Host Checker installs the following files on the Macintosh client:
$HOME/Library/Application Support/Pulse Secure/HostChecker.app
$HOME/Library/Application Support/Pulse Secure/DeviceId

Files Remaining After Uninstall
There is no Host Checker uninstall on the Macintosh client.
Log files Installed by Host Checker

Host Checker stores the log files in the following location on the Macintosh client:
/var/log/Pulse Secure/Logging/debuglog.log

Linux Clients

The following information applies to Linux clients only.
The Linux client installation creates files and folders that are necessary for Host Checker.

Files Created by Host Checker After Installation and Connection Establishment

Host Checker creates the following files under $HOME/.pulse_secure folder:
- $HOME/.pulse_secure/pulse/libpulseui.so
- $HOME/.pulse_secure/pulse/PulseClient_x86_64.sh
- $HOME/.pulse_secure/pulse/pulsesvc
- $HOME/.pulse_secure/pulse/pulse.tgz
- $HOME/.pulse_secure/pulse/pulseUi
- $HOME/.pulse_secure/pulse/pulseutil
- $HOME/.pulse_secure/pulse/certificates/<some certificate>.pem
- $HOME/.pulse_secure/pulse/.pulse_Connections.txt
- $HOME/.pulse_secure/pulse/pulsesvc_handle
- $HOME/.pulse_secure/pulse/pulseUi.lock

Files Remaining After Uninstall

The following files remain on the Linux client after uninstall:
- $HOME/.pulse_secure/pulse/pulsesvc.log

Log Files Installed by Host Checker

Host Checker does not install a separate log file. Log content of the Host Checker is logged in the following file:
- $HOME/.pulse_secure/pulse/pulsesvc.log
- $HOME/.pulse_secure/pulse/postinstall.log
## Required Rights to Run and Install Applications

The following table outlines the rights that are required to install and run the Host Checker client-side components using Pulse Connect Secure’s ActiveX, ActiveX installer service, Java and PSAL mechanisms.

<table>
<thead>
<tr>
<th>Action</th>
<th>ActiveX</th>
<th>ActiveX: Installer Service</th>
<th>Java</th>
<th>Java</th>
<th>PSAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Restricted, Power User or Admin</td>
<td>Restricted, Power User or Admin</td>
<td>Restricted, Power User or Admin</td>
<td>Not Applicable</td>
<td>Restricted, Power User or Admin</td>
</tr>
<tr>
<td>Run</td>
<td>Restricted, Power User or Admin</td>
<td>Restricted, Power User or Admin</td>
<td>Restricted, Power User or Admin</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
Configuring Global Host Checker Settings

Below is a brief of the various options available in the Host Checker configuration page.

**Perform Check Every X Minutes**

Specify the interval at which you want Host Checker to perform policy evaluation on a client machine. If the client machine fails to meet the requirements of the Host Checker policies required by a role or resource policy, then Pulse Connect Secure denies the associated user requests.

*Note: If you enter a value of zero, Host Checker only runs on the client machine when the user first signs into Pulse Connect Secure server.*

**Client-side Process, Login Inactivity Timeout**

This option specifies an interval to control timing out in the following situations:

- If the user navigates away from the Pulse Connect Secure sign-in page after Host Checker starts running but before signing in to Pulse Connect Secure, Host Checker continues to run on the user’s machine for the interval you specify.
- If the user is downloading Host Checker over a slow connection, increase the interval to allow enough time for the download to complete.
Auto-upgrade Host Checker

Allows you to automatically upgrade the Host Checker component on the client machines once Pulse Connect Secure software is upgraded.

Perform Dynamic Policy Reevaluation

This option allows you to automatically refresh the roles of individual users by enabling dynamic policy evaluation for Host Checker. Host Checker can trigger Pulse Connect Secure to evaluate resource policies whenever a user’s Host Checker status changes.

Create Host Checker Connection Control Policy

This policy prevents attacks on Windows client computers from other infected computers on the same physical network. The Host Checker connection control policy blocks all incoming TCP connections. This policy allows all outgoing TCP and Network Connect traffic, as well as all connections to DNS servers, WINS servers, DHCP servers, proxy servers, and Pulse Connect Secure server.

Virus Signature Version Monitoring

You can configure Host Checker to monitor and verify that the virus signatures installed on client computers are up-to-date and remediate those endpoints that do not meet the specified criteria. Host Checker uses the current virus signatures versions from the vendor(s) you specify for pre-defined rules in a Host Checker policy.

You can automatically import the current Virus signature version monitoring lists from the Pulse Secure Networks staging site at a specified interval, or you can download the files from Pulse Secure and use your own staging server.

The default staging site for Pulse Secure Networks is https://www.pulsesecure.net/download

To access the Pulse Secure staging site for updates, you must enter the credentials for your Pulse Secure Support account.

Note: Please note that all connections towards the “Download path” configured is made from the Pulse Connect Secure’s Internal interface ONLY.
**Host Checker Policies**

Below is a description of the various endpoint checks supported by Host Checker on various OS platforms.

<table>
<thead>
<tr>
<th>Windows</th>
<th>Mac</th>
<th>Linux</th>
<th>Solaris</th>
<th>Windows Mobile and Chrome OS</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined: Antivirus</td>
<td>Predefined: Antivirus</td>
<td>Custom: Ports</td>
<td>Custom: Ports</td>
<td>Predefined: OS Checks</td>
<td>OS Checks</td>
<td>OS Checks</td>
</tr>
<tr>
<td>Predefined: HardDisk Encryption</td>
<td>Predefined: HardDisk Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Predefined: Patch Management</td>
<td>Predefined: Patch Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Predefined: OS Checks</td>
<td>Predefined: OS Checks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom: 3rd Party NHC Check</td>
<td>Custom: Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom: Ports</td>
<td>Custom: Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom: Process</td>
<td>Custom: File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom: File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom: Registry Setting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom: NetBIOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Custom: MAC Address

Custom: Machine Certificate

Custom: Advanced Host Checking

Custom: Statement of Health

Custom: Remote IMV
Configuring a Host Checker Policy

- Navigate to Authentication > Endpoint Security > Host Checker on the Admin GUI.
- Under Policies, click on New.
- Choose the appropriate OS you require to configure the checks for.
- Select the appropriate Rule Type. Below is a brief on how to configure the various Rule Types.

Predefined Antivirus Check

This check helps you configure checks for Antivirus products on the client machine.

In the **Antivirus** configuration page:
- Enter a name for this antivirus rule.
- To determine if your software vendor’s product is supported for the System Scan check, click **these Antivirus products**. A new window will open with a list of all of the products that support the feature.
- Select or clear the check box next to **Successful System Scan must have been performed in the last** *days* and enter the number of days in the field.
If you select this check box, a new option appears. If the remediation action to start an antivirus scan has been successfully begun, you can override the previous check.

- Select or clear the check box next to **Consider this rule as passed if ‘Full System Scan’ was started successfully as remediation.**
- Select or clear the check box next to **Virus definition files should not be older than_updates.** Enter a number between 1 and 10. If you enter 1, the client must have the latest update. You must import the virus signature list for the supported vendor.

Select your antivirus vendor(s) and product(s) by using either the **Require any supported product** or **Require specific products/vendors** option buttons.

Note: In case you do not see the Antivirus product you wish to check for listed, please make sure that you are running the latest ESAP version. You could check the Pulse Secure Support portal for the latest version of ESAP along with the documentation showing all the supported products on this ESAP version. In case you still do not find the Antivirus product you are looking for, please open a Support case with Pulse Secure Global Support Center.

Require any supported product allows you to check for any product (rather than requiring you to select every product separately). This option button reveals a list of products in the remediation section to allow you to enable remediation options which are product specific.

Require specific products/vendors allows you to define compliance by allowing any product by a specific vendor (for example, any Symantec product).

Require specific products provides functionality that allows you to select individual products to define compliance.

After you select your vendor(s) and product(s), remediation options will appear on the page.

For each of the following remediation actions:

- **Download latest virus definition files**—obtains the latest available file for the specified vendor from the vendor’s website
- **Turn on Real Time Protection**—launches the virus scanning mechanism for the specified vendor
- **Start Antivirus Scan**—performs a real-time virus scan for the specified vendor the check box is active (clickable) if the action is supported for your product.

If your antivirus product is not supported, you can click the remediation column headers to determine what vendors and products are supported.

Under **Optional**, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Pulse Connect Secure initiates a new handshake to re-evaluate realm or role assignments.

**Predefined Firewall Policy**

You can configure firewall remediation actions with Host Checker after you create a Host Checker firewall rule that requires the endpoint to have a specific firewall installed and running prior to connecting to the network.

After you enforce the Host Checker rule with firewall remediation actions, if an endpoint attempts to log in without the required firewall running, Host Checker can attempt to enable the firewall on the client machine.

The remediation option is not supported for all firewall products. All available products are displayed by using the **Require any supported product or Require specific products/vendors option buttons.**
In the **Firewall** configuration page:

- Enter a name for the firewall rule.
- Select your firewall vendor(s) and product(s) by using either the **Require any supported product** or **Require specific products/vendors** option buttons.

Require any supported product allows you to check for any product (rather than requiring you to select every product separately). This option button reveals a list of products in the remediation section to allow you to enable remediation options which are product specific.

When you add an available product to Selected Products, the remediation option appears, and you can determine if the remediation option is available for your selected firewall.

Require specific products/vendors allows you to define compliance by allowing any product by a specific vendor (for example, any Symantec product).

Require specific products provides functionality that allows you to select individual products to define compliance.

After you select your vendor(s) and product(s), the remediation options on will appear on the page. The Turn on Firewall check box is active (clickable) if the action is supported for your product.

- If your firewall is supported, select the check box to **Turn on Firewall**.
- Under **Optional**, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Pulse Connect Secure initiates a new handshake to re-evaluate realm or role assignments.
Predefined Anti-Spyware Policy

You can configure Host Checker to check for installed spyware on endpoints. After you enforce the Host Checker rule, if an endpoint attempts to log in without the required spyware, the Host Checker rule will fail. The option is not supported for all spyware products. All available products are displayed by using the Require any supported product or Require specific products/vendors option buttons.

In the Antispyware configuration page:

- Enter a name for the firewall rule.
- Select one of the following options:
  - Select the Require any supported product option button to check for any product (rather than requiring you to select every product separately).
  - Select the Require specific products/vendors option button to specify the spyware that you want to check for.
  - Choose either the Require any supported product from a specific vendor or Require specific products to select your spyware.

Add your available spyware from Available Products to Selected Products.

- Under Optional, select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Pulse Connect Secure initiates a new handshake to re-evaluate realm or role assignments.

Predefined: OS Checks

Select this option to create a rule that checks for the Windows operating systems and minimum service pack versions that you specify. (Any service pack whose version is greater than or equal to the version you specify satisfies the policy.)
### Host Checker Deployment Guide

#### Add Predefined Rule: OS Checks

**Rule Type:** OS Checks  
**Rule Name:**

#### Criteria

- **Windows 10**
  - Minimum Service Pack/Version: Ignore
- **Windows 10-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows 2000**
  - Minimum Service Pack/Version: Ignore
- **Windows 2003**
  - Minimum Service Pack/Version: Ignore
- **Windows 2003-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows 2008**
  - Minimum Service Pack/Version: Ignore
- **Windows 2008-R2-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows 7**
  - Minimum Service Pack/Version: Ignore
- **Windows 7-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows 8**
  - Minimum Service Pack/Version: Ignore
- **Windows 8-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows 8.1**
  - Minimum Service Pack/Version: Ignore
- **Windows 8.1-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows Universal App**
  - Minimum Service Pack/Version: Ignore
- **Windows Universal App-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows Universal App ARM**
  - Minimum Service Pack/Version: Ignore
- **Windows VPN Plugin**
  - Minimum Service Pack/Version: Ignore
- **Windows VPN Plugin-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows VPN Plugin-ARM**
  - Minimum Service Pack/Version: Ignore
- **Windows Vista**
  - Minimum Service Pack/Version: Ignore
- **Windows Vista-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows Vista-64-Bit**
  - Minimum Service Pack/Version: Ignore
- **Windows XP**
  - Minimum Service Pack/Version: Ignore
- **Windows XP-64-Bit**
  - Minimum Service Pack/Version: Ignore

**Save Changes**  **Cancel**
Predefined: Hard Disk Encryption

Select this option to create a rule that checks for the hard disk encryption status.

In the **Hard Disk Encryption** configuration page:

- Enter a name for the hard disk encryption rule.
- Select your hard disk vendor(s) and product(s) by using either the **Require any supported product** or **Require specific products/vendors** option buttons.
- Choose either the **Require any supported product from a specific vendor** or **Require specific products** to select your hard disk.

In the **Drive Configuration Details**, select one of the following to check the encryption status:

- Select the **All Drives** option to check all the drives in the system.
- Select the **Specific Drives** option and enter the drive names, example: C,D,E
- Select the **Consider policy as passed if the drives are not detected** option to consider policy as passed if the drives are not detected
Predefined: Patch Management

Patch management software detects patch status based on the configured rules on corresponding patch management server. Select this option to create a rule that detects the severity of various patch updates of the software products.

In the **Patch Management** configuration page:

- Enter a name for the patch management rule.
- From the Criteria, select the Patch Management Software to be installed on the endpoint.
- Select the **Severity** and **Category** details of the patches to be evaluated.

**Note:** For patch management products that do not provide "Severity" and "Category" details, administrator can choose the "Unknown" options so that all the reported missing patches are considered in policy evaluation.

If you want to do remediation, under the Remediation section, select **Enable Automatic Patch Deployment**.

**Note:** Patch remediation support is only through SMS/SCCM patch deployment method. If the system is configured for the SMS/SCCM method for patch deployment, the client machine should have the SMS/SCCM client already installed in the machine for deployment to begin and the SMS/SCCM server should be reachable from the client machine, otherwise remediation fails.
Custom 3rd Party NHC Check

Host Checker has the ability to call the NHC implementation of a supported endpoint security application or a custom DLL that implements NHC. Use this rule type to specify the location of a custom DLL. Host Checker calls the DLL to perform customized client-side checks. If the DLL returns a success value to Host Checker, then Pulse Connect Secure considers the rule met.

Please go through the Endpoint Defense Integration Guide available at the Pulse Secure Support Portal (http://www.pulsesecure.net/techpubs/) to understand the configurations for 3rd Party NHC Checks.

Custom Ports Policy

Use this rule type to control the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access Pulse Connect Secure server.

In the Ports configuration page:

- Enter a name for the port rule.
- Enter a comma delimited list (without spaces) of ports or port ranges, such as: 1234,11000-11999,1235.
- Select Required to require that these ports are open on the client machine or Deny to require that they are closed.
- Under Optional, select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Pulse Connect Secure initiates a new handshake to re-evaluate realm or role assignments.
Custom Process Policy

Use this rule type to control the software that a client may run during a session. This rule type ensures that certain processes are running or not running on the client machine before the user can access resources protected by Pulse Connect Secure.

In the **Process** configuration page:

- Enter a name for the process rule.
- Enter the name of a process (executable file), such as: good-app.exe. You can use a wildcard character to specify the process name. For example: good*.exe
- Select **Required** to require that this process is running or **Deny** to require that this process is not running.
- Specify the MD5 checksum and SHA256 checksum values of each executable file to which you want the policy to apply (optional). For example, an executable may have different MD5 checksum values on a desktop, laptop, or different operating systems. On a system with OpenSSL installed—many Macintosh, Linux and Solaris systems have OpenSSL installed by default—you can determine the MD5 checksum by using this command: openssl md5 <processFilePath>

**Note:** For Linux, Macintosh and Solaris systems, the process that is being detected must be started using an absolute path.
Custom File Policy

Use this rule type to ensure that certain files are present or not present on the client machine before the user can access Pulse Connect Secure. You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly.

In the File configuration page:

- Enter a name for the file rule.
- Enter the name of a file (any file type), such as: c:\temp\bad-file.txt or /temp/bad-file.txt. You can use a wildcard character to specify the file name. For example: *.txt
- You can also use an environment variable to specify the directory path to the file. (You cannot use a wildcard character in the directory path.) Enclose the variable between the <\% and \%> characters. For example: <\%windir\%>\bad-file.txt

- Select Required to require that this file is present on the client machine or Deny to require that this file is not present.
- Specify the minimum version of the file (optional). For example, if you require notepad.exe to be present on the client, you can enter 5.0 in the field. Host Checker accepts version 5.0 and above, of notepad.exe.
- Specify the maximum age (File modified less than n days) (in days) for a file (optional). If the file is older than the specified number of days, then the client does not meet the attribute check requirement.
- Specify the MD5 Checksums and SHA256 Checksums values of each file to which you want the policy
to apply (optional). On Macintosh, Linux and Solaris, you can determine the MD5 checksum by using this command: openssl md5 <filePath>

- Select **Monitor this rule for change** in result to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Pulse Connect Secure initiates a new handshake to re-evaluate realm or role assignments.

## Custom Registry Settings Policy

Use this rule type to control the corporate PC images, system configurations, and software settings that a client must have to access Pulse Connect Secure server. This rule type ensures that certain registry keys are set on the client machine before the user can access Pulse Connect Secure server. You may also use registry checks to evaluate the age of required files and allow or deny access accordingly:

In the **Registry Setting** configuration page:

- Enter a name for the registry setting rule.
- Select a root key from the drop-down list.
- Enter the path to the application folder for the registry subkey.
- Enter the name of the key's value (optional). This name appears in the **Name** column of the Registry Editor.
- Select the key value's type (**String**, **Binary**, or **DWORD**) from the drop-down list (optional). This type appears in the **Type** column of the Registry Editor.
- Specify the required registry key value (optional). This information appears in the **Data** column of the
Registry Editor.

- **Check for 64-bit registry**: This option is applicable only for 64-bit versions of Windows. By default, Host Checker checks only 32-bit registry.

If the key value represents an application version, select **Minimum version** to allow the specified version or newer versions of the application. For example, you can use this option to specify version information for an antivirus application to make sure that the client antivirus software is current. Pulse Connect Secure uses lexical sorting to determine if the client contains the specified version or higher. For example: 3.3.3 is newer than 3.3, 4.0 is newer than 3.3

- Under **Optional**, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Pulse Connect Secure initiates a new handshake to re-evaluate realm or role assignments.

You can configure registry setting remediation actions with Host Checker. If a client attempts to login, and the client machine does not meet the requirements you specify, Host Checker can attempt to correct the discrepancies to allow the client to login.

- Select the check box for **Set Registry value specified in criteria**.

*Note*: If you specify only the key and subkey, Host Checker simply verifies the existence of the subkey folder in the registry.

**Custom NetBIOS Policy**

Use this rule type to check the NetBIOS name of the client machine before the user can access Pulse Connect Secure server.

In the **NetBIOS** configuration page:

- Enter a name for the NetBIOS rule.
- Enter a comma-delimited list (without spaces) of NetBIOS names. The name can be up to 15 characters in length.
- You can use wildcard characters in the name and it is not case-sensitive. For example, md*, m*xp and *xp all match MDXP.
- Select **Required** to require that NETBIOS name of the client machine match one of the names you specify or **Deny** to require that the name does not match any name.

### Custom MAC Address Policy

Use this rule type to check the MAC addresses of the client machine before the user can access Pulse Connect Secure server.

![MAC Address Policy Configuration](image)

In the **MAC Address** configuration page:

- Enter a name for the MAC address rule.
- Enter a comma-delimited list (without spaces) of MAC addresses in the form XX:XX:XX:XX:XX:XX where the X's are hexadecimal numbers. For example: 00:0e:1b:04:40:29

You can use a * wildcard character to represent a two-character section of the address. For example, you can use a * to represent the “04“, “40“, and “29“ sections of the previous example address:

00:0e:1b:*:*:*

But you cannot use a * to represent a single character. For example, the * in the following address is not allowed:

00:0e:1b:04:40:*9

- Select **Required** to require that a MAC address of the client machine matches any of the addresses you specify, or **Deny** to require that the all addresses do not match. A client machine will have at least one MAC address for each network connection, such as Ethernet, wireless, and VPN. This rule's requirement is met if there is a match between any of the addresses you specify and any MAC address on the client machine.
Custom Machine Certificate Policy

Use this rule type to check that the client machine is permitted access by validating the machine certificate stored on the client machine.

In the Machine Certificate configuration page:

- Enter a name for the machine certificate rule.
- From the Select Issuer Certificate list, select the certificate that you want to retrieve from the user's machine and validate. Or, select Any Certificate to skip the issuer check and only validate the machine certificate based on the optional criteria that you specify below.
- From the Optional fields (Certificate field and Expected value), specify any additional criteria that Host Checker should use when verifying the machine certificate.

Note: If more than one certificate is installed on the client machine that matches the specified criteria, the Host Checker client passes the first certificate it finds to Pulse Connect Secure for validation.
Custom Advanced Host Checking

Use this rule type to combine multiple policies for performing advanced host checking. The supported policy types are ports, process, file, registry setting, NETBIOS, MAC address and machine certificate. It allows Administrator to dynamically configure the expected values from registry locations on the endpoint for evaluating the policies.

**Note:** This feature is supported only on Windows platform.

In the **Advanced Host Checking** page:

- Enter a name for the Advanced Host Checking rule.
- Under Criteria:
  - Select a root key from the drop-down list.
  - Enter the path to the application folder for the registry subkey.
  - Enter the name of the key's value (optional). This name appears in the Name column of the Registry Editor.
  - Select the key value's type (String, Binary, or DWORD) from the drop-down list (optional). This type appears in the Type column of the Registry Editor.
  - Specify the required registry key value (optional). This information appears in the Data column of the Registry Editor.
  - Check for 64-bit registry: This option is applicable only for 64-bit versions of Windows. By default, Host Checker checks only 32-bit registry.
Note: You can similarly add the check type for Process/File/NETBIOS/MAC Address. The port number/process name/file path/NETBIOS name/MAC address is obtained from the Registry setting. For more details, refer to the Host Checker section in Pulse Policy Secure Administration Guide.

Custom Statement of Health

The State of Health architecture provides a set of components that evaluates an endpoint’s state of health and makes policy decisions for network access based on the result of the health check.

In the **Statement of Health** configuration page:

- Enter a name for the Statement of Health rule.
- Under **Criteria**, select the SOH policy options from the following types to associate with the rule and click **Save Changes**:
  - Antivirus Enabled
  - Antivirus up to date
  - Antispyware enabled
  - Antispyware up to date
  - Firewall Enabled
  - Automatic Updating Enabled
Custom Remote IMV

The third-party IMVs are installed on the remote IMV server and not on PPS and then obtain a server certificate for the remote IMV server. Import the trusted root CA certificate of the CA that generated the server certificate to PPS. PPS then authenticates with the remote IMV server through the certificate. If you do not have a CA, install and use OpenSSL to generate a CA certificate.

- Enter a name to identify Remote IMV rule.
- Under Criteria, select the third-party IMV to associate with this rule.
Configuring Host Checker Restrictions

If you want to implement Host Checker at the realm level:

- Navigate to:
  - Admin Realms > Select Realm > Authentication Policy > Host Checker (for Admin Realms)
  - Users > User Realms > Select Realm > Authentication Policy > Host Checker (for User Realms)

- Choose one of the following options for either all available policies or for individual policies listed in the Available Policies column:
  - Evaluate Policies—Evaluates without enforcing the policy on the client and allows user-access. This option does not require Host Checker to be installed during the evaluation process; however, Host Checker is installed once the user signs in to Pulse Connect Secure server.
  - Require and Enforce—Requires and enforces the policy on the client in order for the user to log in to the specified realm. Requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement. Requires Pulse Connect Secure to download Host Checker to the client machine. If you choose this option for a realm’s authentication policy, then Pulse Connect Secure downloads Host Checker to the client machine after the user is authenticated and before the user is mapped to any roles in the system. Selecting this option automatically enables the Evaluate Policies option.

- Select the Allow access to realm if any ONE of the selected “Require and Enforce” policies is passed check box if you do not want to require users to meet all of the requirements in all of the selected policies. Instead, the user can access the realm if he meets the requirements of any one of the selected Host Checker policies.
If you want to implement Host Checker at the role level:

- Navigate to:
  - Administrators > Admin Roles > Select Role > General > Restrictions > Host Checker (for Admin Roles)
  - Users > User Roles > Select Role > General > Restrictions > Host Checker (for User Roles)
- Choose one of the following options:
  - Allow all users — Does not require Host Checker to be installed in order for the user to meet the access requirement.
  - Allow only users whose workstations meet the requirements specified by these Host Checker policies — Requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement.
- Select the Allow access to role if any ONE of the selected “Require and Enforce” policies is passed check box if you do not want to require users to meet all of the requirements in all of the selected policies. Instead, the user can access the role if he meets the requirements of any one of the selected Host Checker policies.

If you want to create role-mapping rules based on a user’s Host Checker status:

- Navigate to: Users > User Realms > Select Realm > Role Mapping.
- Click New Rule, select Custom Expressions from the Rule based list, and click Update. Or, to update an existing rule, select it from the When users meet these conditions list.
- Click Expressions
- Write a custom expression for the role mapping rule to evaluate Host Checker’s status using the hostCheckerPolicy variable. For help writing the custom expressions, use tips in the Expressions
Dictionary. Or, see Custom Expressions.

- In the **then assign these roles** section, select the roles that Pulse Connect Secure should map users to when they meet the requirements specified in the custom expression and click **Add**.

- Select the **Stop processing rules when this rule matches** if you want Pulse Connect Secure to stop evaluating role mapping rules if the user successfully meets the requirements defined in this rule.

If you want to implement Host Checker at the resource policy level:

- Navigate to: **Users > Resource Policies > Select Resource > Select Policy > Detailed Rules**.

- Click **New Rule** or select an existing rule from the **Detailed Rules** list.

- Write a custom expression for the detailed rule to evaluate Host Checker's status using the **hostCheckerPolicy** variable. For help writing the custom expressions, use tips in the **Conditions Dictionary**. Or, see Custom Expressions.

**Step by Step Configuration for a Test Scenario**

**Objective**

All users connecting to Pulse Connect Secure should have the Norton Antivirus 10 installed and running with the AV updates not older than 3 on their machines. If the end user machines do not fulfill the above requirements, they should get an appropriate message informing them of this requirement.
Configuration

• Navigate to Authentication > Endpoint Security > Host Checker.

• Create a New Policy. Provide a policy name (say “Policy AV”) and click Continue.

• Under the Rule Type, select Predefined Antivirus and click Add.

• Provide a Rule Name (say Norton).

• Choose the option “Require specific product/vendors” and “Require specific products”.

• Under Available Products, choose Norton AntiVirus (10.x).

• Under the Optional section, choose the option “Virus Definition files should not be older than 3 updates” and save changes. Save changes on the next page as well.

• Now go to User Realms > Select Realm > Authentication Policies > Host Checker. Enable the Require and Enforce option and save changes.
The above steps would ensure that users would be able to only login from machines which has the Norton Antivirus 10 installed/running with updates not older than 3.