Host Checker
Configuration Guide

Overview ............................................................................................................................................. 2

Client Side requirements for Host Checker: .................................................................................... 2
  Qualified platforms:..................................................................................................................... 2
  Compatible platforms:.................................................................................................................. 2
  Windows clients............................................................................................................................ 3
    Installer Package Files and File Location:.................................................................................. 4
    Additional Installer Package Files and File Locations:............................................................. 4
  Files Remaining After Uninstall:.................................................................................................. 5
  Registry Modifications:................................................................................................................. 5
  Log File Locations....................................................................................................................... 6
  Macintosh Clients:....................................................................................................................... 6
    Application and Additional Files Installed by Host Checker:.................................................... 6
    Files Remaining After Uninstall:............................................................................................... 6
    Log files Installed by Host Checker:........................................................................................ 6
  Linux Clients:............................................................................................................................. 6
    Application and Additional Files Installed by Host Checker:.................................................... 6
    Files Remaining After Uninstall:............................................................................................... 7
    Log Files Installed by Host Checker:........................................................................................ 7
  Required rights to run and install applications:............................................................................ 7

Configuring Global Host Checker settings: ..................................................................................... 7
  Perform check every X mins......................................................................................................... 8
  Client-side process, login inactivity timeout.............................................................................. 8
  Auto-upgrade Host Checker........................................................................................................ 8
  Perform dynamic policy reevaluation ......................................................................................... 8
  Create Host Checker Connection Control Policy ....................................................................... 8
  Advanced Endpoint Defense: Malware Protection .................................................................... 9
    Pre 6.5:........................................................................................................................................ 9
    Post 6.5:.................................................................................................................................... 10
  Virus signature version monitoring............................................................................................. 11
  Patch Management Info monitoring:.......................................................................................... 12
  Host Checker policies.................................................................................................................. 12

Configuring a Host Checker policy ................................................................................................ 13
  Predefined Antivirus check........................................................................................................ 13
Predefined Firewall Policy
Predefined Malware policy
Predefined Anti-Spyware policy
Predefined: OS Checks
Custom: 3rd Party NHC Check
Custom: Ports policy
Custom Process policy
Custom File Policy
Custom Registry Settings policy
Custom NetBIOS policy
Custom MAC Address policy
Custom Machine Certificate Policy
Configuring Host Checker Restrictions
If you want to implement Host Checker at the realm level:
If you want to implement Host Checker at the role level:
If you want to create role-mapping rules based on a user’s Host Checker status:
If you want to implement Host Checker at the resource policy level:
Step by Step configuration for a test scenario
Objective:
Configuration:
Overview:

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

The IVE 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.

The IVE 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 Juniper QA department as part of the 6.5 release.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Operating System : list of browsers and Java Environment</th>
</tr>
</thead>
</table>
| Windows  | • XP Professional SP3 32 bit: Internet Explorer 7.0, 8.0 and Firefox 3.0.Sun JRE 6  
          |   • Vista Enterprise SP1 32 bit: Internet Explorer 7.0, 8.0 and Firefox 3.0.Sun JRE 6  
          |   • Windows 7 Enterprise 32 bit: Internet Explorer 8.0 and Firefox 3.5 Sun JRE 6 (6.5R2 and above) |
| Mac      | • Mac OS X 10.5.0, 32 and 64 bit : Safari 3.2.Sun JRE 6  
          |   • Mac OS X 10.4.3, 32 bit only: Safari 2.0. Sun JRE 5 |
| Linux    | • OpenSuse 11, 32 bit only: Firefox 3.0.Sun JRE 6  
          |   • Ubuntu 8.10, 32 bit only: Firefox 3.0.Sun JRE 6 |

Compatible platforms:
The platforms listed in the “compatible” category have not been systematically tested by Juniper QA department in the 6.5 but based on testing in previous releases and knowledge of the platform Juniper expects that the functionality will work and will fully support these platforms.
<table>
<thead>
<tr>
<th>Platform</th>
<th>Operating System</th>
<th>Browsers and Java Environment</th>
</tr>
</thead>
</table>
| Windows    | • Vista Enterprise/Ultimate/Business/Home Basic/Home Premium with Service Pack 1 or 2 on 32 bit or 64 bit platforms  
               • Windows 7 Enterprise/Ultimate/Professional/Home Basic/Home Premium on 32bit or 64 bit platforms (6.5R2 and above)  
               • XP Professional with SP2 or SP3 on 32 bit or 64 bit  
               • 2000 Professional SP4  
               • XP Home SP3  
               • XP Media Center 2005  
               • Windows 2003 server SP2, 32bit and 64 bit | • Internet Explorer 8.0 *  
                                      • Internet Explorer 7.0 *  
                                      • Internet Explorer 6.0 *  
                                      • Firefox 3.5  
                                      • Firefox 3.0  
                                      • Firefox 2.0  
                                      • Sun JRE 5/1.5.07 and above  
                                      • Microsoft JVM – for Windows 2000  
                                      (* Wherever-applicable) |
| Mac        | • Mac OS X 10.6, 32 bit and 64 bit  
               • Mac OS X 10.5.x, 32 bit and 64 bit  
               • Mac OS X 10.4.x, 32 bit only  
               • Mac OS X 10.3.x, 32 bit only | • Safari 1.2 and above  
                                      • Sun JRE 5/1.5.07 and above |
| Linux      | • OpenSuse 10.x, 32 bit only  
               • Ubuntu 7.10, 32 bit only  
               • Red Hat Enterprise Linux 5, 32 bit only | • Firefox 2.0 and above |
| Solaris    | • Solaris 10, 32 bit only | • Mozilla 2.0 and above |

**Windows clients:** To run Host Checker, the IVE downloads the dsHostCheckerSetup.exe.cab 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.cab package after installation is complete.
Installer Package Files and File Location:
Host Checker installs the following CAB file: %TEMP%\dsHostCheckerSetup.exe.cab

Additional Installer Package Files and File Locations:
Host Checker installs the following additional files on the client in C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker:

- CertAuthIMC.dll
- dsHostChecker.exe
- dsHostCheckerProxy.exe
- dsHostCheckerResource_de.dll
- dsHostCheckerResource_en.dll
- dsHostCheckerResource_es.dll
- dsHostCheckerResource_fr.dll
- dsHostCheckerResource_ja.dll
- dsHostCheckerResource_ko.dll
- dsHostCheckerResource_zh.dll
- dsHostCheckerResource_zh_cn.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
• install.log
• JSystemIMC.dll
• msvcp60.dll
• restore_win2k.txt
• restore_win98.txt
• ShavlikIMC.dll
• tnc_config
• uninstall.exe
• versionInfo.ini

In addition, if you implement policies that download or check for third-party software, Host Checker may install additional DLLs in subdirectories of: C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker.

**Files Remaining After Uninstall:**
nprvamgr.sys.

**Registry Modifications:**
Host Checker sets the following registry values:

<table>
<thead>
<tr>
<th>String</th>
<th>Set in</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogFile</td>
<td>HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\Host Checker\Debug\dsHostChecker</td>
</tr>
<tr>
<td>level</td>
<td>HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\Host Checker\Debug\dsHostChecker</td>
</tr>
<tr>
<td>Language</td>
<td>HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\Host Checker</td>
</tr>
<tr>
<td>InstallPath</td>
<td>HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\Host Checker</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayName</td>
<td>“Juniper Networks Host Checker”</td>
</tr>
<tr>
<td>DisplayVersion</td>
<td>current product version number</td>
</tr>
</tbody>
</table>
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\Juniper Networks\Logging\debuglog.log (Windows XP)
- C:\users\username\AppData\Roaming\Juniper Networks\Logging\debuglog.log (Windows Vista and Windows 7)
- C:\Users\Public\Juniper Networks\Logging\debuglog.log (Windows Vista and Windows 7)

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:

~/Library/Application Support/Juniper Networks/tncc.jar

~/Library/Application Support/Juniper Networks/hcport.txt

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:

~/Library/Logs/Juniper Networks

Linux Clients: The following information applies to Linux clients only.

Application and Additional Files Installed by Host Checker

<table>
<thead>
<tr>
<th>Publisher</th>
<th>“Juniper Networks”</th>
</tr>
</thead>
<tbody>
<tr>
<td>QuietUninstallString</td>
<td>“C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker &lt;version number&gt;\uninstall.exe” /S”</td>
</tr>
<tr>
<td>StartupApp</td>
<td>“C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker\dsHostChecker.exe”</td>
</tr>
<tr>
<td>StopApp</td>
<td>“C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker\dsHostChecker.exe -stop”</td>
</tr>
<tr>
<td>UninstallString</td>
<td>“C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker\uninstall.exe”</td>
</tr>
<tr>
<td>URLInfoAbout</td>
<td>“<a href="http://www.juniper.net%E2%80%9D">http://www.juniper.net”</a></td>
</tr>
</tbody>
</table>
Host Checker installs $HOME/.juniper_networks/tncc.jar on the Linux client.

**Files Remaining After Uninstall**
The following files remain on the Linux client after uninstall:

- $HOME/.juniper_networks/dsHCLauncher_linux1.log
- $HOME/.juniper_networks/dsHostChecker_linux1.log

**Log Files Installed by Host Checker**
Host Checker installs the following log files on Linux systems.

- $HOME/.juniper_networks/dsHCLauncher_linux1.log
- $HOME/.juniper_networks/dsHostChecker_linux1.log

**Log Files Installed by Host Checker:**
Host Checker installs the following log files on Linux systems.

- $HOME/.juniper_networks/dsHCLauncher_linux1.log
- $HOME/.juniper_networks/dsHostChecker_linux1.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 the IVE’s ActiveX, ActiveX installer service, and Java mechanisms.

<table>
<thead>
<tr>
<th>Action</th>
<th>ActiveX</th>
<th>ActiveX: Installer Service</th>
<th>Java</th>
<th>Java</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows</td>
<td>Windows</td>
<td>Windows</td>
<td>Mac/Linux</td>
</tr>
<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>
</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>
</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 mins: 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 the IVE 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 the IVE.

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 IVE sign-in page after Host Checker starts running but before signing in to the IVE, 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 the IVE 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 the IVE 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 the IVE.
**Advanced Endpoint Defense: Malware Protection:**

**Pre 6.5:**

In versions prior to 6.4, Host Checker would download and run Whole Security Confidence Online software on your users’ computers. This software scans for malicious programs, including:

- **Trojan horses**—Hackers write trojan horses to remotely administer an infected machine. Trojan horses almost always install themselves on a user’s computer without the authorized user’s knowledge.

- **Key logger software**—Hackers write key logger software to eavesdrop on a user by capturing and logging his typed keystrokes. Key logger software installs itself on a user’s computer without the authorized user’s knowledge.

- **Monitoring applications**—Monitoring applications are end-user software applications that monitor and record user activity. Users typically install this software themselves to monitor the activity of children, spouses, and other users who share their computers.

- **Remote controls**—Remote control applications are commercial applications such as VNC that offer easy remote access to an authorized user for computer administration activities.

Note: Each user’s computer must be able to access the Whole Security site (update.wholesecurity.com) so that Confidence Online can periodically download the latest definition files.

The options here are explained below,

**Enable Silent Enforcement of Signature Scan:** If you do not want Confidence Online to notify users when it blocks trojan horse, key logger software, and other applications that it deems malicious. (Note that Confidence Online accesses a Whole Security server on a daily basis in order to keep its list of malicious applications current.)

**Enable User Control over disabling Behavior Blocker:** If you want to enable users to choose whether or not to block monitoring applications, remote control software, and other potentially legitimate applications. If you select this option, users can view and control blocked applications through a Confidence Online icon in their system trays. (For more information, see the Confidence Online end-user help system.) If you do not select this option, Confidence Online simply blocks these applications without user interaction.

Once you enable these options, Host Checker would automatically create the necessary policies for you. These appear under the User Realms > Select Realm > Authentication Policies > Host Checker and under User Roles > Select Role > Authentication Policies > Host Checker. Below are a list of the policies created by the IVE and their descriptions.
### Advanced Endpoint Defense: Malware Protection

- **Behavior Blocker**—This policy is created by Whole Security. It enables the Confidence Online behavior blocker software to block keystroke logger software, screen capture software, and other applications that try to eavesdrop on user sessions. Only administrators can install and run the behavior blocker feature in Confidence Online. The behavior blocker feature is supported on Windows 2000 and Windows XP systems.

- **Category One Threats (Trojan Horses and Key Loggers)**—This policy is created by Whole Security. It enables the Confidence Online software to block trojan horse programs, spyware, malware, and other malicious applications. Restricted users, power users, and administrators can install and run the scanning feature in Confidence Online. The scanning feature is supported on Windows NT4, Windows 2000, and Windows XP systems.

- **Category Two Threats (Monitoring Applications and Remote Controls)**—This policy is created by Whole Security. It enables the Confidence Online software to block monitoring applications, remote control software, and other potentially legitimate applications. Restricted users, power users, and administrators can install and run the scanning feature in Confidence Online. The scanning feature is supported on Windows NT4, Windows 2000, and Windows XP systems.

### Post 6.5:

From release 6.5 onwards, Host Checker includes integrated antispyware functionality provided by Web Root that can detect and remediate Windows endpoints with spyware and keyloggers. Advanced Endpoint Defense (AED) ensures that malware, spyware, viruses or worms are not present on endpoints that attempt to connect to the IVE, and you can restrict or quarantine these endpoints depending on your Host Checker policy configuration.

This feature uses a signature database that is automatically downloaded from Web Root Spy Sweeper servers on the Internet. You can configure the age of the database on the IVE to determine the frequency of updates. The age of the database is the threshold used to determine if a user can access resources by passing a Host Checker policy.
By default, with the base license, 2 simultaneous endpoints can use this feature. You can purchase a separate license to enable additional users.

Note that if you configure an AED policy for endpoints, a separate installer is downloaded to endpoints. User endpoints are scanned for offending software, and signatures may be automatically installed.

Once you enable these options, Host Checker would automatically create the necessary policies for you. These appear under the User Realms > Select Realm > Authentication Policies > Host Checker and under User Roles > Select Role > Authentication Policies > Host Checker as shown below.

Note: EES log messages are included in the Juniper debug log files on the end-user systems. WebRoot debug logs are located in `<%AllUsersProfile%>Application Data\Webroot\WRSSMini\Logs>`. Only the last three logs are saved to conserve disk space. WebRoot memory dumps are also located in `<%AllUsersProfile%>Application Data\Webroot\WRSSMini\Logs>`.

**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 Juniper Networks staging site at a specified interval, or you can download the files from Juniper and use your own staging server.
The default staging site for Juniper Networks is https://download.juniper.net/software/av/uac/epupdate_hist.xml

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

Note: Please note that all connections towards the “Download path” configured is made from the IVE internal interface ONLY.

**Patch Management Info monitoring:**

Similar to the Virus Signature version monitoring, you could also configure Host Checker to monitor and verify that the operating systems, software versions, and patches installed on client computers are up to date, and remediate those endpoints that do not meet the specified criteria.

You can automatically import the current Patch Management Info Monitoring lists from the Juniper Networks staging site at a specified interval, or you can download the files from Juniper and use your own staging server.

The default URLs are the paths to the Juniper Networks staging site is https://download.juniper.net/software/hc/patchdata/patchupdate.dat. You must enter the credentials for your Juniper Networks Support account.

Note: Please note that all connections towards the “Download path” configured is made from the IVE internal interface ONLY.

**Host Checker policies:**

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

- Go under Authentication > Endpoint Security > Host Checker on the Admin GUI.
- Go under Policies and 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.
• 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 donot 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 Juniper 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 donot find the Antivirus product you are looking for, please open a Support case with Juniper Support.

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, the IVE 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.
• 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, the IVE initiates a new handshake to re-evaluate realm or role assignments.

**Predefined Malware policy**: Select this option to check for the malware protection software you specify.
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.

- 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, the IVE 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.)

**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 the IVE considers the rule met.


**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 the IVE. 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, the IVE 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 the IVE. In the **Processes** 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.
Host Checker How To

- Select **Required** to require that this process is running or **Deny** to require that this process is not running.
- Specify the MD5 checksum value 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 the IVE. 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 **Files** 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 checksum value 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, the IVE 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 the IVE. This rule type ensures that certain registry keys are set on the client machine before the user can access the IVE. You may also use registry checks to evaluate the age of required files and allow or deny access accordingly.

- 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 that you want to require (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.

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. The IVE 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, the IVE 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 the IVE. 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 the IVE. 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 the IVE for validation.

Configuring Host Checker Restrictions

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

- Navigate to:
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 the IVE.

- 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 the IVE to download Host Checker to the client machine. If you choose this option for a realm’s authentication policy, then the IVE 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 on 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 the IVE 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 the IVE 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:

- 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 the IVE 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 donot fulfill the above requirements, they should get an appropriate message informing them of this requirement.

**Configuration:**
- Go under 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 under 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.