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 http://www.pulsesecure.net/support/eula. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
# Table of Contents

About the Documentation ............................................................................................................. ix
  Documentation and Release Notes ............................................................................................. ix
  Supported Platforms ................................................................................................................... ix
  Documentation Conventions ....................................................................................................... ix
  Documentation Feedback ............................................................................................................ xi
  Requesting Technical Support .................................................................................................... xii
    Self-Help Online Tools and Resources ..................................................................................... xii
  Opening a Case with JTAC .......................................................................................................... xii

## Part 1  Overview

**Chapter 1**  
Host Checker .................................................................................................................................. 3
  Host Checker and Trusted Network Computing ........................................................................ 3
    Host Checker Compatibility ...................................................................................................... 4
  Host Checker Overview .............................................................................................................. 5
    Upgrading the Software Version .............................................................................................. 6
  Understanding Host Checker Policy Remediation ..................................................................... 6
    Remediation Options ................................................................................................................ 6
    Remediation User Experience .................................................................................................. 7

**Chapter 2**  
Machine Accounts .................................................................................................................. 9
  Using Host Checker for Machine Account Logins .................................................................... 9

**Chapter 3**  
Anti-Malware Checks .............................................................................................................. 11
  Using the Predefined Enhanced Endpoint Security Option ..................................................... 11
    Enhanced Endpoint Security Option Overview ....................................................................... 11
    Enhanced Endpoint Security User Experience ....................................................................... 12
  Enabling the Enhanced Endpoint Security Option .................................................................. 13

**Chapter 4**  
Wildcard or Environment Variable .......................................................................................... 15
  Using a Wildcard or Environment Variable in a Host Checker Rule .......................................... 15

**Chapter 5**  
Patch Management ................................................................................................................... 17
  Patch Management Info Monitoring and Patch Deployment .................................................... 17
    Configuration and Migration Options for Deprecated Custom: Patch Assessment Rules .......... 17
    Using a System Management Server ...................................................................................... 18

**Chapter 6**  
Third Parties ............................................................................................................................ 19
  Using Third-Party Integrity Measurement Verifiers ................................................................... 19

**Chapter 7**  
Statement of Health .................................................................................................................. 21
  Using Statement of Health Integration Host Checker Policies .................................................. 21
## Part 2  Installation

### Chapter 8  Host Checker

- Specifying Host Checker Installation Options .................................................. 27
- Installing Host Checker Automatically or Manually ............................................ 28

## Part 3  Configuration

### Chapter 9  Host Checker

- Task Summary: Configuring Host Checker ............................................................ 33
- Configuring Host Checker Restrictions ............................................................... 35
- Configuring General Host Checker Remediation ............................................... 37
- Configuring Virus Signature Version Monitoring .............................................. 38

### Chapter 10  Predefined Rules

- Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh) ................................................................. 41
- Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh) ................................................................. 43
- Configuring a Predefined AntiSpyware Rule (Windows and Macintosh) ............ 45
- Configuring a Predefined Host Checker Patch Management Rule ...................... 46
- Configuring a Predefined Host Checker Rule for Hard Disk Encryption (Windows and Macintosh) ................................................................. 48

### Chapter 11  Third Parties

- Configuring a Remote IMV Server ........................................................................ 53

### Chapter 12  Statement of Health

- Configuring a Statement of Health Host Checker Policy ...................................... 59

## Part 4  Administration

### Chapter 13  Host Checker

- Creating Global Host Checker Policies ............................................................... 65
- Implementing Host Checker Policies .................................................................... 66
- Executing Host Checker Policies ......................................................................... 67
- Specifying General Host Checker Options ......................................................... 68

### Chapter 14  Third Parties and Plug-Ins

- Checking for Third-Party Applications Using Predefined Rules ......................... 71
- Implementing a Third-Party IMV Policy ............................................................... 71
- Upgrading the Endpoint Security Assessment Plug-In ......................................... 73

### Chapter 15  Customized Requirements

- Specifying Customized Requirements Using Custom Rules ............................ 77

## Part 5  Troubleshooting

### Chapter 16  Host Checker

- Using Host Checker Logs .................................................................................... 87
## List of Figures

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 5</td>
<td>Patch Management ................................................................. 17</td>
</tr>
<tr>
<td>Figure 1: Delete or Convert the Deprecated Patch Assessment Rules .......................... 18</td>
<td></td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Statement of Health .................................................................. 21</td>
</tr>
<tr>
<td>Figure 2: SOH Integration with a Network Policy Server ........................................ 22</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 3</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 10</td>
<td>Predefined Rules ................................................................. 41</td>
</tr>
<tr>
<td>Figure 3: Rule Settings for Host Checker Policy .................................................... 46</td>
<td></td>
</tr>
<tr>
<td>Figure 4: Patch Management ........................................................................... 47</td>
<td></td>
</tr>
<tr>
<td>Figure 5: Patch Management ........................................................................... 48</td>
<td></td>
</tr>
<tr>
<td>Figure 6: Rule Settings for Host Checker Policy .................................................... 49</td>
<td></td>
</tr>
<tr>
<td>Figure 7: HardDisk Encryption ......................................................................... 50</td>
<td></td>
</tr>
</tbody>
</table>
# List of Tables

About the Documentation................................................................. ix

Table 1: Notice Icons ........................................................................ x
Table 2: Text and Syntax Conventions ............................................... x

## Part 1  Overview

### Chapter 4  Wildcard or Environment Variable
Table 3: Wildcard Characters for Specifying a File Name or Process Name ............................................................................. 15
Table 4: Environment Variables for Specifying a Directory Path on Windows ................................................................. 15
Table 5: Environment Variables for Specifying a Directory Path on Macintosh, Linux and Solaris ........................................................................ 16

## Part 3  Configuration

### Chapter 10  Predefined Rules
Table 6: HardDisk Encryption Settings .............................................. 50
About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Documentation Conventions on page ix
- Requesting Technical Support on page xii

Documentation and Release Notes

To obtain the latest version of Pulse Secure technical documentation, see the product documentation page at http://www.juniper.net/techpubs/.

Supported Platforms

For the features described in this document, the following platforms are supported:

- IC4500
- IC6500 FIPS
- IC6500
- MAG Series

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.
### Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>‼️</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>🚨</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>🌟</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td>🧠</td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td>🌟</td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

Table 2 on page x defines the text and syntax conventions used in this guide.

### Table 2: Text and Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold text like this</td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the configure command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user@host&gt; configure</td>
</tr>
<tr>
<td>Fixed-width text like this</td>
<td>Represents output that appears on the terminal screen.</td>
<td>user@host&gt; show chassis alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No alarms currently active</td>
</tr>
<tr>
<td>Italic text like this</td>
<td>• Introduces or emphasizes important new terms.</td>
<td>• A policy <em>term</em> is a named structure that defines match conditions and actions.</td>
</tr>
<tr>
<td></td>
<td>• Identifies guide names.</td>
<td>• <em>Junos OS CLI User Guide</em></td>
</tr>
<tr>
<td></td>
<td>• Identifies RFC and Internet draft titles.</td>
<td>• RFC 1997, <em>BGP Communities Attribute</em></td>
</tr>
<tr>
<td>Italic text like this</td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine’s domain name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[edit] root@# set system domain-name domain-name</td>
</tr>
</tbody>
</table>
Table 2: Text and Syntax Conventions *(continued)*

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Text like this           | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | • To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.  
• The console port is labeled CONSOLE. |
| < > (angle brackets)     | Encloses optional keywords or variables.                                                                                                  | stub <default-metric metric>;                                                               |
| | (pipe symbol)           | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | broadcast | multicast  
(string1 | string2 | string3) |
| # (pound sign)           | Indicates a comment specified on the same line as the configuration statement to which it applies.                                           | rsvp (# Required for dynamic MPLS only |
| [] (square brackets)     | Encloses a variable for which you can substitute one or more values.                                                                       | community name members [community-ids]                                                       |
| Indention and braces()   | Identifies a level in the configuration hierarchy.                                                                                         | [edit] routing-options {  
   static {  
     route default {  
       nexthop address;  
       retain;  
     }  
   }  
}                                                                                       |
| ; (semicolon)            | Identifies a leaf statement at a configuration hierarchy level.                                                                             |                                                                                               |
| GUI Conventions          |                                                                                                                                             |                                                                                               |
| Bold text like this      | Represents graphical user interface (GUI) items you click or select.                                                                        | • In the Logical Interfaces box, select All Interfaces.  
• To cancel the configuration, click Cancel.                                                   |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections.                                                                                   | In the configuration editor hierarchy, select Protocols>Osfp.                                     |
Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you are a customer with an active support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with PSGSC.

- Product warranties—For product warranty information, visit http://www.pulsesecure.net/support

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure has designed an online self-service portal called the Pulse Secure Global Support Center (PSGSC) that provides you with the following features:

- Find CSC offerings: http://www.pulsesecure.net/support
- Search for known bugs: http://www.pulsesecure.net/support
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://www.pulsesecure.net/support
- Download the latest versions of software and review release notes: http://www.pulsesecure.net/support/
- Search technical bulletins for relevant hardware and software notifications: http://www.pulsesecure.net/support
- Open a case online in the CSC Case Management tool: http://www.pulsesecure.net/support

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: http://www.pulsesecure.net/support

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.pulsesecure.net/support.
- Call 1-888-314-5822 (toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.pulsesecure.net/support.
PART 1

Overview

- Host Checker on page 3
- Machine Accounts on page 9
- Anti-Malware Checks on page 11
- Wildcard or Environment Variable on page 15
- Patch Management on page 17
- Third Parties on page 19
- Statement of Health on page 21
CHAPTER 1

Host Checker

- Host Checker and Trusted Network Computing on page 3
- Host Checker Overview on page 5
- Understanding Host Checker Policy Remediation on page 6

Host Checker and Trusted Network Computing

Host Checker is a client-side agent that performs endpoint health and security checks for hosts that attempt to connect to Policy Secure. Host Checker is based on open standards defined by the Trusted Computing Group (TCG). Trusted Network Connect (TNC) is a subgroup of the TCG that created an architecture and set of standards for verifying endpoint integrity and policy compliance during or after a network access request. Many of the TCG members participated in the definition and specification of the TNC architecture. The TNC defined several standard interfaces that enable components from different vendors to securely operate together. The TNC architecture is designed to build on established standards and technologies, such as 802 1X, RADIUS, IPsec, EAP, and TLS/SSL. For more information about TNC, see www.trustedcomputinggroup.org. Using technology based on the TNC architecture and standards, the Host Checker component of the Unified Access Control solution provides a comprehensive approach to assess the trustworthiness of endpoints.

You can use Host Checker to perform health and security evaluations on endpoints before allowing them to connect to the network and to access protected resources. Host Checker can check for third-party applications, files, process, ports, registry keys, and custom DLLs on hosts. Based on the results of the checks, Host Checker can deny or allow access to protected resources. For example, you can check for virus detection software before allowing a user access to a realm. You can configure policies that launch the software on the user’s system, map the user to roles based on individual policies defined in your own DLL, and then further restrict access to individual resources based on the existence of spyware detection software. When a user’s computer does not meet the requirements you specify, you can configure options that display remediation instructions to users so they can bring their computers into compliance.
NOTE: If you configure a large number of Host Checker policies, and the system is under a heavy load, the server process inside the device could get overloaded. When this happens, a message appears in the event log (Log/Monitoring > Events > Log).

Policy Secure and Host Checker manage the flow of information between the corresponding pairs of IMCs and IMVs. Each IMV on Policy Secure works with the corresponding IMC on the client machine to verify that the client meets the Host Checker rules.

You can also configure Host Checker to monitor third-party IMCs installed on client computers by using third-party IMVs that can be installed on a remote IMV server.

Host Checker supports TNC-based integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs). IMCs are software modules that run on the host and collect information such as antivirus, antispyware, patch management, firewall, and other configuration and security information about the host. IMVs are software modules that run on Policy Secure and verify a particular aspect of a host’s integrity. Each IMV on Policy Secure works with the corresponding IMC on the host to verify that the host meets the requirements of the integrity measurement custom rules that you configure. IMCs scan the client machine frequently for changes in security status. For example, if the user turns off virus checking, the IMC can detect this and then trigger a new check to make sure the modified system complies with the requirements of the Host Checker policy. You can configure Host Checker to monitor third-party IMCs installed on client computers by using third-party IMVs that are installed on a remote IMV server.

You can invoke Host Checker at the role level or the realm level to specify access requirements for endpoints seeking authentication. Host Checker policies that are implemented at the realm level occur before the user is authenticated. Host Checker policies at the role level are implemented after authentication but before the user is permitted to access protected resources.

The Host Checker component is built into OAC, Pulse, and the Java agent. A client-side Host Checker application is downloaded for agentless access. Non-UAC agent clients (the Windows native supplicant) can take advantage of Host Checker’s Statement of Health (SOH) integration feature.

There is no functional difference between OAC or Pulse TNC Host Checker component and the Windows agentless Host Checker. OAC and Pulse Host Checker are included with the installer, and agentless protection is installed through browser access.

Host Checker functionality for Macintosh (with or without OAC), Linux, and Solaris platforms is limited.

Host Checker Compatibility

The TNC integrity measurement rules apply to Windows and Macintosh client machines that are running either OAC or Host Checker (agentless), Windows machines with Pulse, Macintosh with the Safari browser, and Linux and Solaris platforms using Firefox browser with Java support. Windows and Macintosh Java Host Checker is not supported.
Chapter 1: Host Checker

Host Checker runs on agentless and Java agent endpoints, and OAC and Pulse include a built-in Host Checker component. In this chapter, the name Host Checker refers to the software that runs on agentless and Java agent endpoints and the built-in Host Checker component that runs as part of OAC and Pulse.

You configure agentless Host Checker policies for guest access.

**NOTE:** To use Host Checker with Linux or Solaris, you must use the Firefox browser.

You can also configure Statement of Health Host Checker policies to protect Windows 802.1X supplicants (Vista, XP with Service Pack 3, and Windows 7) that are authenticated through 802.1X.

**NOTE:** Some Host Checker processes can take a long time. On Windows endpoints, the user can view Host Checker progress.

You can see the Host Checker status for each active user on the Status > Active Users page.

**Related Documentation**

- Host Checker Overview on page 5
- Creating Global Host Checker Policies on page 65
- Task Summary: Configuring Host Checker on page 33

**Host Checker Overview**

The Policy Secure can check hosts for endpoint properties using a variety of rule types, including:

- Predefined rules that check for antivirus software and up-to-date virus signatures, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders.
- Predefined rules that check for hard disk encryption and patch management.
- (Windows machines only) Custom rules that use IMCs and IMVs to perform customized client-side checks.
- (Windows machines only) Custom rules that check for third party DLLs that perform customized client-side checks.
- (Windows machines only) Custom rules that check for ports, processes, files, registry key settings, and the NetBIOS name, MAC addresses or certificate of the client machine.
- On Macintosh, Linux, and Solaris systems you can check for ports, processes, and files.

If the user’s computer does not meet Host Checker policy requirements, you can display a custom remediation page to the user. This page can include specific instructions and links to resources that can help the user bring the endpoint into compliance with the Host Checker policy.
Upgrading the Software Version

If you upgraded UAC from a previous version, ensure that existing endpoints are upgraded to the current version of the UAC agent before you configure Host Checker policies that implement new features. Because the agent is required to connect and establish a session with the server to perform an agent-based upgrade, the client must pass any Host Checker restrictions required for a realm and roles to gain access.

If an endpoint with an older version of the UAC agent attempts to log in with a new Host Checker feature implemented at the realm level, the user's authentication fails, and the endpoint cannot upgrade to the latest version of the client.

If you implement new features before endpoints are upgraded, you must create a remediation role that does not require any of the new features to allow users to authenticate and download the current version of the client.

To ensure that endpoints are using the latest client, click Maintenance > System > Options and then select either Enable automatic upgrade of Pulse Secure clients or Enable automatic upgrade of Odyssey Access Clients.

Related Documentation

- Creating Global Host Checker Policies on page 65
- Task Summary: Configuring Host Checker on page 33

Understanding Host Checker Policy Remediation

This topic describes Host Checker policy remediation. It includes the following information:

- Remediation Options on page 6
- Remediation User Experience on page 7

Remediation Options

You can specify general remediation actions for Host Checker to take if an endpoint does not meet the requirements of a policy. For example, you can display a remediation page to the user that contains specific instructions and links to resources to help the user bring their endpoint into compliance with Host Checker policy requirements.

You can also include a message to users (called a reason string) that is returned by Host Checker or an IMV and that explains why the client machine does not meet the Host Checker policy requirements.

For example, the user might see a remediation page that contains the following custom instructions, a link to resources, and reason strings:

Your computer's security is unsatisfactory.
Your computer does not meet the following security requirements. Follow the instructions below to fix these problems. When you are done click Try Again. If you Continue without fixing these problems, you may not have access to all of your intranet servers.

1. Symantec

Instructions: You do not have the latest signature files. Click here to download the latest signature files. Reasons: The AntiVirus Product Version is too low.

The age of the Virus Definitions is not acceptable.

For each Host Checker policy, you can configure two types of remediation actions:

- **User-driven**—Using custom instructions and reason strings, you can inform the user about the failed policy and how to make his computer conform. The user must take action to successfully re-evaluate the failed policy unless you configure an IMV to automatically remediate his computer. For instance, you can create a custom page that is linked to a policy server or Web page and enables the user to bring his computer into compliance.

- **Automatic (system-driven)**—You can configure Host Checker to automatically remediate the user’s computer. For example, when the initial policy fails, you can kill processes, delete files, or allow automatic remediation by an antivirus rule, a firewall rule, or a registry setting rule. Host Checker does not inform users when performing automatic actions. (You could, however, include information in your custom instructions about the automatic actions.)

**Remediation User Experience**

Users might see a remediation page in the following situations:

- **Before the user signs in:**
  - If you enable custom instructions or reason strings for a policy that fails, the system displays the remediation page. The user has two choices:
    - Take the appropriate actions to make the endpoint conform to the policy and then click Try Again on the remediation page. Host Checker checks the user’s computer again for compliance with the policy.
    - Leave the endpoint in its current state and click Continue to sign in. The user cannot access the realm, role, or resource that requires compliance with the failed policy.

      - If you do not configure the system with at least one realm that allows access without enforcing a Host Checker policy, the user must bring the endpoint into compliance before signing in.

      - If you do not enable custom instructions or reason strings for a policy that fails, Host Checker does not display the remediation page. Instead, a message displays telling the user that no additional information has been provided and to contact the system administrator. The system does not assign the user a role that allows access to protected resources.

  - After the user signs in:
• OAC—During a session, if a user’s computer becomes noncompliant with the requirements of a Host Checker policy, a pop-up message is displayed briefly in the system tray that informs the user of the noncompliance. The user can display the remediation page by right-clicking the OAC icon in the system tray, choosing OAC Manager from the context menu, and then clicking the How do I resolve this problem link in the status section of OAC window.

• Pulse—During a session, if a user’s computer becomes noncompliant with the Host Checker policy, a message is displayed briefly in the system tray that informs the user of the noncompliance. The remediation page is displayed on the client.

• Agentless—During a session, if a user’s agentless computer becomes noncompliant with the Host Checker policy, the system displays the remediation page to inform the user of the noncompliance. On Windows agentless computers, Host Checker displays a bubble and tray icon if the endpoint becomes noncompliant. The user must click the bubble or tray icon to open a browser window that contains the remediation instructions. On Macintosh, Linux or Solaris agentless computers, Host Checker automatically opens a browser window that contains the remediation instructions as soon as the endpoint is noncompliant.

Related Documentation

• Configuring General Host Checker Remediation on page 37

• Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh) on page 41

• Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh) on page 43

• Specifying Customized Requirements Using Custom Rules on page 77
CHAPTER 2

Machine Accounts

- Using Host Checker for Machine Account Logins on page 9

Using Host Checker for Machine Account Logins

With OAC or Pulse, you can use a machine account configuration to authenticate a physical machine, rather than a user. This type of configuration uses either a statically defined user account or the machine credentials that were created when the machine account was set up in Active Directory. For more information, see http://www.juniper.net/techpubs/en_US/release-independent/aaa-802/information-products/pathway-pages/oac/product/or the Pulse Secure documentation.

If you use the machine account feature, do not configure restrictive Host Checker policies that require human interaction for remediation, because these policies will fail. Instead, configure a separate default role for machine accounts that fail Host Checker policies.

To allow the machine account to log in, you configure a special role for machines. You can create a role-mapping policy that maps all machine roles to a realm that automatically accepts your domain with a wildcard as a username (for example, “QA\*$”).

Related Documentation
- Host Checker and Trusted Network Computing on page 3
- Creating Global Host Checker Policies on page 65
- Task Summary: Configuring Host Checker on page 33
CHAPTER3

Anti-Malware Checks

- Using the Predefined Enhanced Endpoint Security Option on page 11

Using the Predefined Enhanced Endpoint Security Option

This topic describes when and how to use the Host Checker Enhanced Endpoint Security (EES) feature. It includes the following information:

- Enhanced Endpoint Security Option Overview on page 11
- Enhanced Endpoint Security User Experience on page 12
- Enabling the Enhanced Endpoint Security Option on page 13

Enhanced Endpoint Security Option Overview

Host Checker includes integrated antispyware functionality that can detect and remediate Windows endpoints using OAC or Pulse. Enhanced Endpoint Security (EES) ensures that malware, spyware, viruses, or worms are not present on endpoints that attempt to connect to the Policy Secure, and that you can restrict or quarantine these endpoints according to your Host Checker policy configuration.

EES can scan processes that are loaded in memory on endpoints, and can provide real-time file system write and execution shield to automatically remediate machines that are not in compliance. As part of the remediation status, EES reports any threats that are detected but not remediated. In some cases the user might be directed to reboot the machine to achieve compliance.

EES uses a signature database that is automatically downloaded to endpoints from Web Root Spy Sweeper servers on the Internet. (The signature database is not hosted on the Policy Secure.)

Endpoints must have access to the Internet for EES to run successfully, because live signature updates must be able to download. Additionally, if you configure default remediation roles ensure that endpoints that are directed to remediation roles can access *.webroot.com.

You can configure the age of the database on the Policy Secure to determine the acceptable age of the signature database. The age of the database is the threshold used to determine whether a user can access resources by passing a Host Checker policy. For example, if signatures are 5 days old, and you configure the age as 5 days, the endpoint is allowed to access resources. If you configure the age as 4 days, the endpoint fails the Host Checker policy. If an endpoint passes the initial EES Host Checker policy, signature updates are performed regularly, so endpoints should generally have the most current updates.
If Internet connectivity is not available to an endpoint before it connects to the Policy Secure, and you have chosen to implement the option to check for signature age, the policy does not pass if the signatures are too old. For example, if a user has not accessed the endpoint for several days and the signatures are not up to date, the endpoint cannot access the Policy Secure. In this case, you can create a default remediation role that allows limited access to the Internet for signature updates at *.webroot.com.

Any endpoint that is configured for an EES scan at Layer 2 always fails the check. To permit a network connection, you should configure the realm so endpoint users are reassigned to a remediation VLAN. This allows endpoint users to connect and download the required signature updates, or if connecting for the first time, the EES installer package.

EES antispyware functionality is available on Windows platforms (including Vista) with OAC and Pulse or with the agentless Host Checker component.

You configure EES on the Endpoint Security > Host Checker main page to ensure that multiple policies are not created, and that the same policy is used across all realms and roles for which you have enabled it. When you create a realm or a role, you can enable EES restrictions in addition to any other Host Checker policies.

---

**NOTE:** If you configure an EES policy for endpoints, a separate EES installer (about 5 MB) is downloaded to endpoints on their first attempt to access resources protected by a Host Checker EES policy. User endpoints are scanned for offending software, and signatures are automatically installed.

---

**Enhanced Endpoint Security User Experience**

For endpoints that do not have OAC or Pulse installed, or for agentless endpoints, the EES plugin is initialized before the EES policy can be evaluated. An informational page is displayed on the user's endpoint to communicate the assessment status.

A significant amount of data is downloaded (approximately 5 MB for the installer and approximately 12 MB for the signatures), followed by the memory scan.

After installation, signatures are updated and the memory scan is performed to verify that no spyware is loaded in memory. If it is determined that the endpoint does not have active spyware in memory, the policy passes.

The initial installation and scan on endpoints takes some time, so be to warn users to wait for the operation to complete.

Any threat detected is automatically remediated by Host Checker and is not reported. If threats cannot be remediated, the endpoint reports back to the server. Roles and user sessions can be adjusted based on endpoint compliance. A number of user strings automatically notify the user of the compliance status.
NOTE: Do not use machine authentication and GINA with the UAC agent and EES. If you configure an EES scan to run at machine authentication or GINA time, in some instances Windows will not display the login dialogue and the endpoint will be unusable until you disable the EES scan on the Policy Secure.

Enabling the Enhanced Endpoint Security Option

To enable and use EES antispyware:

1. In the admin console, click Authentication > Endpoint Security > Host Checker.
2. Under Options, select the Advanced Endpoint Protection: Malware Protection tab.
3. Select the Enable Advanced Endpoint Protection: Malware Protection check box.
4. To set the age of the signature definitions database, select the Signature definitions should not be older than check box. Enter the frequency in days (3 - 30). This function does not change the frequency of updates. This number determines the maximum permissible age of signatures.
5. Click Save Changes.

When you create or configure realm or role Host Checker restrictions, you can select Enhanced Endpoint Security: Malware Protection to apply to that role or realm.

Related Documentation:
- Host Checker and Trusted Network Computing on page 3
- Creating Global Host Checker Policies on page 65
- Task Summary: Configuring Host Checker on page 33
- Configuring Host Checker Restrictions on page 35
CHAPTER 4

Wildcard or Environment Variable

- Using a Wildcard or Environment Variable in a Host Checker Rule on page 15

Using a Wildcard or Environment Variable in a Host Checker Rule

Table 3 on page 15 lists the wildcards you can use to specify a file name in a Custom File rule or a process name in a Custom Process rule.

Table 3: Wildcard Characters for Specifying a File Name or Process Name

<table>
<thead>
<tr>
<th>Wildcard Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any character</td>
<td>*.txt</td>
</tr>
<tr>
<td>?</td>
<td>Matches exactly one character</td>
<td>app?.exe</td>
</tr>
</tbody>
</table>

In a Custom File rule for Windows, you can use the following environment variables to specify the directory path to a file:

Table 4: Environment Variables for Specifying a Directory Path on Windows

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Example Windows Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;%APPDATA%&gt;</td>
<td>C:\Documents and Settings\jdoe\Application Data</td>
</tr>
<tr>
<td>&lt;%windir%&gt;</td>
<td>C:\WINDOWS</td>
</tr>
<tr>
<td>&lt;%ProgramFiles%&gt;</td>
<td>C:\Program Files</td>
</tr>
<tr>
<td>&lt;%CommonProgramFiles%&gt;</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>&lt;%USERPROFILE%&gt;</td>
<td>C:\Documents and Settings\jdoe</td>
</tr>
<tr>
<td>&lt;%HOMEDRIVE%&gt;</td>
<td>C:</td>
</tr>
<tr>
<td>&lt;%Temp%&gt;</td>
<td>C:\Documents and Settings&lt;username&gt;\Local Settings\Temp</td>
</tr>
</tbody>
</table>
Table 4 on page 15 lists Custom File rules for Macintosh, Linux and Solaris.

Table 5: Environment Variables for Specifying a Directory Path on Macintosh, Linux and Solaris

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Example Macintosh Value</th>
<th>Example Linux and Solaris Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;%Java.home%&gt;</td>
<td>/System/Library/Frameworks/JavaVM Framework/Versions/1.4.2/Home</td>
<td>/local/local/Java/j2sdk1.4.1_02/jre</td>
</tr>
<tr>
<td>&lt;%Java.io.tmpdir%&gt;</td>
<td>/tmp</td>
<td>/tmp</td>
</tr>
<tr>
<td>&lt;%user.dir%&gt;</td>
<td>/Users/admin</td>
<td>/home-shared/cknouse</td>
</tr>
<tr>
<td>&lt;%user.home%&gt;</td>
<td>/Users/admin</td>
<td>/home/cknouse</td>
</tr>
</tbody>
</table>

NOTE: Although environment variables are formatted in the same way as Toolkit Template directives, they are not interchangeable. Be sure not to confuse them.

Related Documentation

Specifying Customized Requirements Using Custom Rules on page 77
CHAPTER 5

Patch Management

- Patch Management Info Monitoring and Patch Deployment on page 17

Patch Management Info Monitoring and Patch Deployment

Configuration and Migration Options for Deprecated Custom: Patch Assessment Rules

With Release 8.1/5.1, the OPSWAT patch solution provides support for patch information monitoring and deployment. Host Checker downloads the OPSWAT SDK and uses it to detect the installed patch management software and the patch status (the list of missing patches as reported by the patch management software). To enable the patch management software to evaluate the patch status of the client machine, the administrator must configure a patch management policy to use for evaluating the patch status of endpoints.

Custom patch assessment rules are not supported beginning in Release 8.1/5.1. The existing patch management rules will be converted to dummy rules during the migration. You can delete the existing rules or convert them to predefined: patch management rules.

To delete the custom patch assessment rules:

2. Select the check box to back up the configuration and the XML file that contains Host Checker, realms, and role details.
   
   Figure 1 on page 18 shows the configuration page for Host Checker.
   
   Result

   Displays a confirmation page with the list of deprecated Custom:Patch Assessment rules and the policies in which they are configured. It also lists the Rule Expression for the respective policies which will be changed and the list of policies that becomes empty because of deletion of above rules. You need to click on Confirm if you want to continue deletion of deprecated rules, otherwise click on Cancel.

To convert the existing Shavlik rules to Opswat rules:

2. Select the check box to back up the configuration and the XML file that contains Host Checker, realms, and role details.  

Figure 1 on page 18 shows the configuration page for Host Checker.

Figure 1: Delete or Convert the Deprecated Patch Assessment Rules

3. Select the patch management software that you will use to convert custom patch assessment rules to predefined patch management rules and then click on convert.

NOTE: Convert button appears only after selecting the Patch management Software. If you select convert you can see the confirmation page which lists the deprecated Custom:Patch Assessment rules and the policies in which they are configured. It also lists the Rule Expression for the respective policies which will be changed. Click Confirm to continue replacement of deprecated Custom:Patch Assessment rules with Predefined: Patch Management rules, otherwise click cancel.

Using a System Management Server

You can use a System Management Server (SMS) to provide a method for automatic updates to non-compliant software. From Release 8.1/5.1, only SMS/SCCM patch remediation is supported. You can enable SMS/SCCM patch remediation in the Predefined patch management policy page. The client machine must have the SCCM client installed and must be communicating to the SCCM server.

Related Documentation
- Configuring a Predefined Host Checker Patch Management Rule on page 46
CHAPTER 6

Third Parties

- Using Third-Party Integrity Measurement Verifiers on page 19

Using Third-Party Integrity Measurement Verifiers

The TNC standard enables the enforcement of security requirements for endpoints connecting to networks. The client-side components of the TNC are the IMCs and the TNCC. The TNCC compiles the IMC measurements and sends them to the server. At the server, there is a corresponding set of components: the TNC server (TNCS) and the IMVs. The TNCS manages the messages between the IMVs and the IMCs and sends the recommendations, based on the IMVs, to the policy engine. This type of rule is available for Host Checker policies on all platforms.

Policy Secure and Host Checker comply with the standards produced by the TNC. For more information about the TNC, IMVs and IMCs, see www.trustedcomputinggroup.org.

You can configure Host Checker to monitor third-party TNC-compliant IMCs installed on client computers. To do so, you must:

1. Run the Third-party Integrity Measurement Verifier (IMV) Server installer on the system designated as the remote IMV server. Install the third-party IMVs and create the server certificates.

2. Specify the remote IMV server so that Policy Secure can communicate with it.

3. Implement the Host Checker policy.

Related Documentation

- Configuring a Remote IMV Server on page 53
- Implementing a Third-Party IMV Policy on page 73
CHAPTER 7

Statement of Health

- Using Statement of Health Integration Host Checker Policies on page 21

Using Statement of Health Integration Host Checker Policies

You can use Host Checker policies on Policy Secure with the open standard Statement of Health (SOH) protocol by leveraging the existing protocols built into Policy Secure. To use this functionality, you must obtain SOH licensing from Pulse Secure, LLC.

SOH support is implemented through local Host Checker criteria that you configure on Policy Secure, alternatively or you can deploy an external Network Policy Server (NPS) to use third-party system health agents (SHAs) and system health validators (SHVs), as shown in Figure 2 on page 22.

The SOH 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. Policy Secure supports SOH interoperability for Windows Vista, Windows XP Service Pack 3, Windows 7, OAC, and Pulse. Windows Security Center (WSC) functionality is built into the Host Checker component that implements this feature for local host checking.

You can configure OAC SOH Host Checker policies if you are using Layer 2 and 802.1X or Layer 3 with the Infranet Enforcer. The Windows supplicant can connect only with 802.1X. There is no heartbeat between Policy Secure and the Windows client, and no other Host Checker policies are supported with the Windows client. If you are using OAC, you must use the default EAP-JUAC protocol. If you configure a different protocol set for OAC and do not include EAP-JUAC, the SOH cannot be transmitted. SOH Host Checker policies are not supported for agentless access.

You can use the SOH health state validation to determine which roles or realms can be accessed by endpoints. If an endpoint fails the SOH check, or if the SOH cannot be negotiated successfully, the Host Checker policy fails.

You can use local Host Checker SOH enforcement with either OAC, Pulse, or the Windows supplicant. With local enforcement, you can specify remediation actions if the endpoint does not pass the Host Checker policy. Local enforcement supports the WSC SHA, which includes support for checking the following:
- Antivirus is enabled.
- Antivirus is up to date.
- Antispyware is enabled.
- Antispyware is up to date.
- Firewall is enabled.
- Automatic updating is enabled.

To implement additional third-party SHAs, you must use an NPS.

Multiple local evaluations or multiple NPS evaluations are supported, but clients are limited to one state of health response (SOHR). The client receives the SOHR from the first failed policy. If the endpoint fails multiple policies, the agent receives SOHRs from the failed policies in the order in which they are performed. If the endpoint passes multiple policies, the agent receives the SOHR from the first passed policy.

**Figure 2: SOH Integration with a Network Policy Server**

NPS and Policy Secure communicate using a RADIUS-based protocol. The endpoint requests authentication from Policy Secure using the EAP-PEAPv0 protocol. Policy Secure communicates SOH information between the NPS and the endpoint as request/response messages. The server connection information that allows the NPS to communicate with Policy Secure is configured on the Host Checker SOH interface.

When you use an external NPS, as in all other Host Checker policies, you can restrict users whose endpoints fail to meet the requirements of the Health Registration Authority (HRA) on the NPS.

You can use the NPS as both the AAA server and the health policy server. Windows Server 2008 is the only server supported as an NPS. See the applicable Microsoft documentation for details about setting up the NPS.

If you use an external NPS for evaluation of the SOH, you cannot use local enforcement. Additionally, avoid putting any other Host Checker rules into a policy that is designed for SOH enforcement with the Windows client.

An SOH license is required to use this feature.
Related Documentation

Configuring a Statement of Health Host Checker Policy on page 59
PART 2

Installation

- Host Checker on page 27
CHAPTER 8

Host Checker

- Specifying Host Checker Installation Options on page 27
- Installing Host Checker Automatically or Manually on page 28

Specifying Host Checker Installation Options

- Automatic installation:
  - OAC on Windows—If you enable OAC installation, the first time the user accesses Policy Secure using a Web browser, the system automatically downloads agentless Host Checker to evaluate Host Checker restrictions for role-mapping. After the initial check is successfully completed, the system downloads OAC with its built-in Host Checker component to the user’s computer. If you evaluate or enforce a Host Checker policy at the realm level, OAC automatically runs its built-in Host Checker on the endpoint to verify security compliance.
  - Pulse on Windows—Pulse installation and functionality is similar to that of OAC. You must select Minimal components or All components as the component set.
  - OAC on Macintosh—On the Macintosh, users must manually install OAC. The Host Checker component is a part of the installation.
  - Agentless and Java agent—For agentless or Java agent deployments, the user signs in directly using a Web browser instead of OAC. If you evaluate or enforce a Host Checker policy at the realm level, the system automatically installs and runs Host Checker on the endpoint to verify security compliance.

If you evaluate or enforce a Host Checker policy for Windows OAC, the Java agent, or agentless deployments, the system evaluates the realm-level option when the user connects to Policy Secure or accesses the sign-in page and then determines if the current version of OAC or Host Checker is installed on the user’s machine. If OAC or Host Checker is not installed, the system attempts to install it using either an ActiveX or a Java delivery method.

- When a Windows user first signs in, the system attempts to install an ActiveX control on the user’s system. If the system successfully installs the ActiveX control, the control manages the installation of Host Checker in agentless access deployments. If the system cannot install the ActiveX control because ActiveX is turned off on the user’s system, it attempts to install Host Checker using Java.
For Linux and Solaris hosts, the system always uses the Java delivery method. The Java delivery method requires only user privileges, but Java must be enabled on the user’s system. For the Firefox browser on Linux, the Java runtime and plug-in must be installed.

If the system cannot use the Java delivery method because Java is disabled on the user’s system, the Host Checker policy fails and might cause restrictions on realms or roles where the policy is evaluated. If no other realms or roles are available to the user, the system displays a no-access error message.

The user or administrator manually installs Pulse, OAC or Host Checker—Download the OAC installer, the Pulse installer, or the Host Checker installer from and use it to manually install OAC or Host Checker on the user’s system.

For agentless access deployments only, you can configure Policy Secure to automatically install Host Checker on client computers.

To automatically install Host Checker on client computers:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.

2. Under Options, select Auto-upgrade Host Checker if you want the system to automatically download the Host Checker application to a client computer when the version of Host Checker on the system is newer than the version installed on the client. If the Auto-upgrade Host Checker option is selected or not selected, the following events occur:

   - If Host Checker is not installed on the client computer, Host Checker is installed automatically regardless of whether the Auto-upgrade Host Checker option is selected or not selected.

   - If the Auto-upgrade Host Checker option is selected and a previous version of Host Checker is installed, Host Checker is upgraded on the client automatically.

   - If the Auto-upgrade Host Checker option is not selected and a previous version of Host Checker is installed, Host Checker is not upgraded the client automatically.

   If you select the Auto-upgrade Host Checker option, note the following:

   - On Windows, the user must have administrator privileges in order for the system to automatically install the Host Checker application on the client. For more information, see the Client-side Changes Guide on the Pulse Secure Customer Support Center.

   - If the user uninstalls Host Checker and then signs in to a system that has not enabled the Auto-upgrade Host Checker option, the user no longer has access to Host Checker.

3. Click Save Changes.
The Maintenance > System > Installers page of the admin console provides OAC and Host Checker client applications. You can download the applications or service as a Windows executable file, which enables you to:

- Distribute the file to client machines using software distribution tools. This option enables you to install an application or service on client machines whose users do not have Administrator privileges, which are required to install the application or service.

- Post the executable in a secure repository so that users with the proper administrator right may download and install the appropriate version.

- Download and execute a script that automatically retrieves the proper version of the installer from an FTP server.

Related Documentation: Specifying Host Checker Installation Options on page 27
PART 3

Configuration

• Host Checker on page 33
• Predefined Rules on page 41
• Third Parties on page 53
• Statement of Health on page 59
Task Summary: Configuring Host Checker

To configure a Host Checker policy:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
   b. Enter a name in the Policy Name field. Then click Continue. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
   c. Create one or more rules to associate with the policy.

2. Configure additional system-level options:
   - To display remediation information to users if users fail to meet the requirements of a Host Checker policy, select Authentication > Endpoint Security > Host Checker.
   - To change default Host Checker settings, select Authentication > Endpoint Security > Host Checker.

3. Determine the level at which you want to enforce Host Checker policies:
   - To enforce Host Checker policies when the user initially signs in, implement the policy at the realm level select Users > User Realms > Select Realm > Authentication Policy > Host Checker.
4. Specify how users can access the Host Checker client-side agent that enforces the policies you define:

- **Windows**—If you enable OAC or Pulse installation, the system automatically downloads the client with built-in Host Checker when the user first accesses the system by means of a web browser. If you evaluate or enforce a Host Checker policy at the realm level, the client automatically runs the built-in Host Checker components on the endpoint to determine security compliance. Host Checker functionality is the same on Pulse and OAC.

- **Macintosh with OAC**—Users can navigate to the system and manually download and install the agent with the Host Checker component. After the user installs the agent, Host Checker policies that you configured for the user’s assigned roles or realms can be implemented.

- **Platforms with Java agent or agentless deployments**—To enable automatic installation of the Host Checker component on agentless computers, you must evaluate or enforce a Host Checker policy. To do so select Administrators > Admin Realms > Select Realm > Authentication Policy > Host Checker page or the Users > User Realms > Select Realm > Authentication Policy > Host Checker.

5. Determine whether you want to create client-side logs. If you enable client-side logging, the system creates log files on your users’ systems and writes to the file whenever OAC, Pulse, or Host Checker runs.

   If more than one valid session exists from the same system, and Host Checker is used in those sessions, all valid sessions are terminated if a user signs out from any of the sessions. To prevent this, turn off Host Checker for those sessions that do not need Host Checker.

   Related Documentation

   - Host Checker and Trusted Network Computing on page 3
   - Using Host Checker for Machine Account Logins on page 9
   - Using the Predefined Enhanced Endpoint Security Option on page 11
   - Creating Global Host Checker Policies on page 65
Configuring Host Checker Restrictions

To specify Host Checker restrictions:

1. Select Authentication > Endpoint Security > Host Checker and specify global options for Host Checker to apply to any user for whom Host Checker is required in an authentication policy or a role-mapping rule.

2. To implement Host Checker at the realm level:
   a. Select
      - Administrators > Admin Realms > Select Realm > General > Restrictions > Host Checker.
      - Users > User Realms > Select Realm > General > Restrictions > Host Checker.
   b. Select 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.
      - 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 for the user to meet the access requirement. Requires the system to download Host Checker to client machines that do not support Pulse or OAC. If you choose this option for a realm’s authentication policy, then the system 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.
   c. 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 by meeting the requirements of any one of the selected Host Checker policies.

3. To implement Host Checker at the role level:
   a. Select
      - Administrators > Admin Roles > Select Role > General > Restrictions > Host Checker.
      - Users > User Roles > Select Role > General > Restrictions > Host Checker.
   b. Select 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.


4. To create role-mapping rules based on a user’s Host Checker status:
   a. Select Users > User Realms > Select Realm > Role Mapping.
   b. 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.
   c. Click Expressions.
   d. 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.
   e. In the...then assign these roles section, select the roles that the system should map users to when they meet the requirements specified in the custom expression. Click Add.
   f. Select the Stop processing rules when this rule matches for the system to stop evaluating role-mapping rules if the user successfully meets the requirements defined in this rule.

These options allow you to control which version of an application or service runs on client machines.

**Related Documentation**

- Specifying General Host Checker Options on page 68
- Using the Predefined Enhanced Endpoint Security Option on page 11
Configuring General Host Checker Remediation

To specify remediation actions for a Host Checker policy:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create or enable Host Checker policies.
3. Specify the remediation actions for Host Checker to perform if a computer does not meet the requirements of the current policy:
   - Enable Custom Instructions—Enter the instructions to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and to add links to resources such as policy servers or web sites: <i>, <b>, <br>, <font>, and <a href>. For example:
     
     You do not have the latest signature files.

     <a href="www.company.com">Click here to download the latest signature files.</a>

   - Kill Processes—On each line, enter the name of one or more processes to kill if the computer does not meet the policy requirements. You can include an optional MD5 checksum for the process. (You cannot use wildcards in the process name.) For example:
     
     keylogger.exe
     
     MD5: 6A7DFAF12C3183B56C44E89B12DBEF56

   - Delete Files—Enter the names of files to delete if the user’s computer does not meet the policy requirements. (You cannot use wildcards in the file name.) Enter one filename per line. For example:
     
     c:\temp\bad-file.txt

     /temp/bad-file.txt

   - Send reason strings—Select this option to display a message to users (called a reason string) that is returned by Host Checker or IMV and that explains why the client machine does not meet the Host Checker policy requirements. This option applies to predefined rules, to custom rules, and to third-party IMVs that use extensions in the Pulse Secure TNC SDK. For example, an antivirus IMV might display the following reason string:
     
     The AntiVirus Product Version is too low. The age of the Virus Definitions is not acceptable.

     NOTE: By sending reason strings, you are disclosing to users what the IMV is checking on the client machine.

     4. Click Save Changes.

Related Documentation

Understanding Host Checker Policy Remediation on page 6
You can configure Host Checker to monitor and verify that the virus signatures, 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. Host Checker uses the current virus signatures and patch assessment versions from the vendor(s) you specify as predefined rules in a Host Checker policy.

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

You can also configure a proxy server as a staging site between the Pulse Policy Secure and the Pulse Secure site. To use a proxy server, you enter the servers network address, port and authentication credentials, if applicable.

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

To configure the Pulse Policy Secure to automatically import the current virus signature version monitoring and patch management version monitoring list(s) from the Pulse Secure staging site:

2. Click Virus signature version monitoring.
3. Select Auto-update virus signatures list.
4. For Download path, leave the existing URL(s) of the staging site(s) where the current list(s) are stored. The default URLs are the paths to the Pulse Secure staging site:
   http://www.pulsesecure.net/support  
   (Use the staging site to automatically update virus signature lists.)
5. For Download interval, specify how often you want the Pulse Policy Secure to automatically import the current list(s).
6. For Username and Password, enter your Pulse Secure Support credentials (which may have been originally issued by Juniper Networks).
7. Click Save Changes.

To manually import the current virus signature version monitoring and patch management version monitoring list(s):

2. Click Virus signature version monitoring.
3. Download the list(s) from the Pulse Secure staging site to a network server or local drive on your computer by entering the following URL in a browser window:
   https://download.juniper.net/software/av/uac/epupdate_list.xml
4. Under Manually import virus signatures list, click Browse, select the list, and then click OK.

5. Click Save Changes.

NOTE: If you use your own staging site for storing the current list(s), you must upload the trusted root certificate of the CA that signed the staging’s server certificate to the Pulse Policy Secure.

To use a proxy server as the auto-update server:


2. Click Virus signature version monitoring.

3. Select Auto-update virus signatures list.

4. For Download path, leave the existing URL(s) of the staging site(s) where the current list(s) are stored. The default URLs are the paths to the Pulse Secure staging site:

   https://download.juniper.net/software/av/uac/epupdate_hist.xml

   (Use the staging site to automatically update virus signature lists.)

5. For Download interval, specify how often you want the Pulse Policy Secure to automatically import the current list(s).

6. For Username and Password, enter your Juniper Networks Support credentials.

7. Select the check box for Use Proxy Server.

8. Enter the IP Address of your proxy server.

9. Enter the Port that the Juniper Networks Support site will use to communicate with your proxy server.

10. If your proxy server is password protected, type the Username and Password of the proxy server.

11. Click Save Changes.

Related Documentation

- Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh) on page 41
- Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh) on page 43
- Implementing Host Checker Policies on page 66
CHAPTER 10

Predefined Rules

- Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh) on page 41
- Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh) on page 43
- Configuring a Predefined AntiSpyware Rule (Windows and Macintosh) on page 45
- Configuring a Predefined Host Checker Patch Management Rule on page 46
- Configuring a Predefined Host Checker Rule for Hard Disk Encryption (Windows and Macintosh) on page 48

Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh)

You can configure antivirus remediation actions with Host Checker. You can specify a requirement for the age in days of the last successful virus scan, and you can specify that virus signatures installed on client machines not be older than a specified number of updates or days.

You can also monitor policies to ensure that logged-in endpoints maintain compliance status, and remediate the endpoint to another role or realm depending on the current status.

If a client attempts to log in and the client machine does not meet the requirements you specify, Host Checker can attempt to correct the deficiencies to allow the client to successfully log in. With Host Checker antivirus remediation, you can prompt the endpoint to download the latest virus signature files, turn on antivirus protection, and initiate an antivirus scan.

Not all of the remediation options are supported on products by all antivirus software vendors. There is an option to display all available vendors and products that are supported.

Alternately, you can select the Require specific products/vendors option button. Then select either the Require any supported product from a specific vendor or Require specific products check boxes. Then add an available type to Selected Types. The remediation options appear, and you can determine which remediation options are available for specific products or vendors.
NOTE:

- Remediation is not supported for Macintosh.
- Not all products support basic functions. For example if Host Checker can detect that an Anti-Virus product is installed, but it cannot check for real time protection, then the host check is not effective. In these cases, the product is not listed.

To configure a predefined antivirus rule:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create a policy or click on existing policy in the Policies section of the page.
3. Select the tab for Windows or Mac, depending on the platform for which this rule is intended.
5. Enter the name of this antivirus rule.
6. To determine if your software vendor’s product is supported for the System Scan check, click these Antivirus products. A new window opens with a list of the products that support the feature.
7. 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 box.

   If you select this check box, a new option is displayed. If the remediation action to start an antivirus scan successfully begun, you can override the previous check.
8. Select or clear the Consider this rule as passed if ‘Full System Scan’ was started successfully as remediation check box.
9. Select or clear the Check for Virus Definition files check box. If you select this check box, then choose either Virus Definition files should not be older than n Updates (the default is 10, and the maximum is 20) or Virus Definition files should not be older than n Days. The range for this value is 1 - 30.
10. Select one of the following options:

   - 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 allows you to select individual products to define compliance.

NOTE: A limited number of antivirus products are available for Macintosh with Release 4.2. When new ESAP packages are released, support for new products may be added. See the applicable release notes when new ESAP packages are installed.
Chapter 10: Predefined Rules

After you select your vendors and products, remediation options 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 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.

11. If your product is supported, select the check box for the remediation action that you want to apply.

12. Under Optional, select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints. If this check box is selected, the compliance status of an endpoint that has successfully logged in changes, Policy Secure initiates a new handshake to reevaluate realm or role assignments.

13. Click Save Changes to save the antivirus rule and enforce antivirus remediation.

14. (Optional) Add more rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

**Related Documentation**

- Checking for Third-Party Applications Using Predefined Rules on page 71
- Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh) on page 43
- Configuring a Predefined AntiSpyware Rule (Windows and Macintosh) on page 45

**Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh)**

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 before it connects 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. For a list of all available products select the Require any supported product or Require specific products/vendors option button.
To configure a Host Checker predefined firewall rule:

1. In the admin console, choose Authentication > Endpoint Security > Host Checker.
2. Create a policy or click an existing policy in the Policies section of the page.
3. Select the tab for Windows or Mac, depending on the platform for which this rule is intended.
5. Enter a name for the firewall rule.
6. Select either the Require any supported product or Require specific products/vendors option buttons to select firewall vendors and products.
   - Require any supported product lets you 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 product-specific remediation options.
   - When you add an available product to Selected Products, the remediation option is displayed, 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 and product, the remediation options appear on the page.

   **NOTE:** A limited number of firewall products are available for Macintosh with Release 4.2. When new ESAP packages are released, support for new products may be added. See the applicable release notes when new ESAP packages are installed.

7. If your firewall is supported, select the Turn on Firewall check box.
8. 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, Policy Secure initiates a new handshake to reevaluate realm or role assignments.
9. Click Save Changes to save the firewall rule and enforce firewall remediation.
10. (Optional) Add more rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

   - **Related Documentation**
   - Checking for Third-Party Applications Using Predefined Rules on page 71
   - Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh) on page 41
   - Configuring a Predefined AntiSpyware Rule (Windows and Macintosh) on page 45
You can configure Host Checker to check for installed antisyware on endpoints. After you enforce the Host Checker rule, if an endpoint attempts to log in without the required spyware, the Host Checker rule fails.

This configuration is not supported for all spyware products. To display all available products, select Require any supported product or Require specific products/vendors option button.

To configure a Host Checker Predefined AntiSpyware rule:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create a new or click an existing policy in the Policies section of the page.
3. Select the tab for Windows or Mac, depending on the platform for which this rule is intended.
5. Enter a name for the firewall rule.
6. 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.
   - Select either the Require any supported product from a specific vendor or Require specific products option button.
   - Add antisyware from Available Products to Selected Products.

---

**NOTE:** SecureMac.com and Trend Micro are the only products available for the Macintosh with Release 4.2. When new ESAP packages are released, support for new products may be added. See the applicable release notes when new ESAP packages are installed.

---

7. 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, Policy Secure initiates a new handshake to re-evaluate realm or role assignments.
8. Click Save Changes.
9. (Optional) Add more rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.
Checking for Third-Party Applications Using Predefined Rules on page 71

- Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh) on page 41
- Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh) on page 43

Configuring a Predefined Host Checker Patch Management Rule

To configure a predefined patch management rule:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Click the Windows tab.

Figure 3 on page 46 shows the rule settings page for host checker.

Figure 3: Rule Settings for Host Checker Policy


Figure 4 on page 47 shows the configuration page to you use to add a patch management rule to the Host Checker policy.
Figure 4: Patch Management

Configuration > Host Checker Policy >
Add Predefined Rule: Patch Management

- Rule Type: Patch Management
- Rule Name: [Enter name]

Criteria

Select Product Name: BigFix Enterprise Client (8.x) ▼

Remediation

- Note: Only SMS/SCM patch deployment method is used.
- Enable Automatic Patch Deployment

Save Changes?

[Save Changes] [Cancel]

* indicates required field

6. In the Rule Name box, enter a name for the integrity measurement rule.

NOTE: If a policy includes a selection that does not apply (for example, if the target software application is not installed on the endpoint), the check for that selection is not performed.

7. Under Criteria, select the product name.

Figure 5 on page 48 shows the different product names that you can select.
8. To automatically enable patch deployment, select Enable Automatic Patch Deployment.

   NOTE: Only the SMS/SCCM patch deployment method is used.

9. Click Save Changes.

Related Documentation
   Patch Management Info Monitoring and Patch Deployment on page 12

Configuring a Predefined Host Checker Rule for Hard Disk Encryption (Windows and Macintosh)

Hard disk encryption software is used to encrypt the hard disk on endpoints for security purposes. You can verify the status of the hard disk encryption on the client machine as part of security posture assessment.
You can configure the hard disk encryption through host checker policy. If the hard disk encryption status on client machine meets the policy requirements the user is granted access otherwise the access is provided/denied based on the policy. Note that the existing OESIS SDK from Opswat is used for collecting hard disk encryption details from client machine.

To configure a predefined hard disk encryption rule:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Select the tab for Windows or Mac, depending on the platform for which this rule is intended.

   Figure 6 on page 49 shows the rule settings page for Host Checker.

   Figure 6: Rule Settings for Host Checker Policy

5. Under Rule Settings, select Predefined: HardDisk Encryption and then click Add.

   Figure 7 on page 50 shows the configuration page you use to add a hard disk encryption rule to the Host Checker.
Figure 7: HardDisk Encryption

Table 6: HardDisk Encryption Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Identifies the rule.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require any supported product</td>
<td>Select this option if you require any supported product for Pulse Secure access management framework.</td>
</tr>
</tbody>
</table>
Table 6: HardDisk Encryption Settings *(continued)*

<table>
<thead>
<tr>
<th>Settings</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require any specific product/vendors</td>
<td>Select this option if you require support from any specific product or from vendors.</td>
</tr>
<tr>
<td></td>
<td>• Require any supported product from a specific vendor– Select the vendor from the available vendor list.</td>
</tr>
<tr>
<td></td>
<td>• Require specific products–Select the product from the available products list.</td>
</tr>
</tbody>
</table>

Drive Configuration Details

| All Drives | (Default) Select this option to check if all the drives on the client machine are encrypted. |
| Specific Drives | Select this option to check if only specific drives on the client machine are encrypted. |
|             | • Drive Letters– Enter the drive name. For example, C, D, E. |
|             | • Consider policy as passed if the drives are not detected– Select this option to consider policy as passed if the drives are not detected. |

7. Click Save Changes.
CHAPTER 11

Third Parties

• Configuring a Remote IMV Server on page 53

Configuring a Remote IMV Server

NOTE:

• In an active/passive cluster, the active/passive nodes' individual IP addresses must be added to the RIMV as Policy Secure IP addresses.
• The successful addition of remote IMV server is not logged in the event log.
• When Host Checker fails, custom instructions are not displayed. There is no user access log on Policy Secure about Host Checker failure.

During this step, you install third-party IMVs. Third-party IMVs are installed on the remote IMV server, not on Policy Secure. You also obtain a server certificate for the remote IMV server. You import the trusted root CA certificate of the CA that generated the server certificate onto Policy Secure. Policy Secure 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.

To install, configure, and implement the server software:

1. Select Maintenance > System > Installers and download the Third-party Integrity Measurement Verifier (IMV) Server installer.
2. Run the installer on the system designated as the remote IMV server.
3. Install the third-party IMVs on the remote IMV server and the corresponding IMCs on the client systems.
4. Generate a server certificate from a certificate authority for the remote IMV server. The server’s certificate Subject CN value must contain the actual host name or IP address of the remote IMV server.

   The server certificate and the private key must be combined into a single PKCS#12 file and must be encrypted with a password.

   If you do not have a CA, you can use the following steps to create one, and then create a server certificate for the remote IMV server.
**NOTE:** Be sure to install the full version of OpenSSL. The "light" version of OpenSSL will not work.

To set up OpenSSL:

a. Download and install OpenSSL from this site:

   http://www.slproweb.com/products/Win32OpenSSL.html

   **NOTE:** Depending on your operating system, the default installation directory may be different. You should ensure that OpenSSL is installed in `c:\openssl`.

b. At the Windows command prompt, type the following commands:

   ```
   cd \openssl
   md certs
   cd certs
   md demoCA
   md demoCA/newcerts
   md demoCA/private
   edit demoCA/index.txt
   ```

c. Press ALT-F and then S to save the file.

d. Press ALT-F and then X to exit the editor.

e. At the Windows command prompt, type the following command:

   ```
   edit demoCA/serial
   ```

f. In the document window type: 01

g. Press ALT-F and then S to save the file.

h. Press ALT-F and then X to exit the editor.

i. At the Windows command prompt, type the following commands:

   ```
   set path=c:\openssl;bin;%path%
   set OPENSSL_CONF=c:\openssl\bin\openssl.cfg
   ```

j. In Wordpad (or an equivalent text editor that correctly handles Unix line breaks), edit the openssl config file (`c:\openssl\bin\openssl.cfg`), change the CA policy match for country and state from "match" to "optional", and save your changes. The resulting config stanza should appear as follows:

   ```
   # For the CA policy
   [policy_match]
   countryName = optional
   stateOrProvinceName = optional
   organizationName = match
   organizationalUnitName = optional
   commonName = supplied
   ```
emailAddress = optional

To create a CA key:

a. Type the following command at the Windows command prompt in the c:\openssl\certs directory:
   openssl genrsa -out ca.key 1024
   The following output appears:
   Loading 'screen' into random state - done
   Generating RSA private key, 1024 bit long modulus
   ........+++++
   ++++
   e is 65537 (0x10001)

b. Copy the CA key into the private directory of your CA:
   cp ca.key demoCA/private/cakey.pem

To create a CA certificate:

a. Type the following command at the Windows command prompt in the c:\openssl\certs directory:
   openssl req -new -x509 -days 365 -key ca.key -out demoCA/cacert.pem

b. Enter the appropriate Distinguished Name (DN) information for the CA certificate. You can leave some fields blank by hitting enter.

   For example:
   Country Name: US
   State or Province Name: CA
   Locality Name: Sunnyvale
   Organization Name: XYZ
   Org. Unit Name: IT
   Common Name: ca.xyz.com
   e-mail Address: user@xyz.com

c. Type the following command to generate an RSA private key for the remote IMV server:
   openssl genrsa -out rimvs_key.pem 1024

d. Type the following command to generate a CSR for the remote IMV server:
   openssl req -new -key rimvs_key.pem -out rimvs_csr.pem

e. Enter the required information. For example:

   Country Name:US
   State or Province Name:MA
   Locality Name:Boston
   Organization:XYZ
   Organizational Unit:IT
   Common Name: [IP Address]:10.0.1.10 e-mail Address: user@xyz.com
   A challenge password:
   An optional company name:
**NOTE:** The Common Name field must contain the IP address of the machine running the remote IMV server. This machine must have a static IP address. The organization name in the CSR must match the CA certificate's organization name. If the organization names do not match, you cannot sign the CSR.

f. Type the following command to generate a certificate for the remote IMV server:
   ```
   openssl ca -in rimvs_csr.pem -out rimvs_cert.pem
   ```

g. Type y twice when prompted to generate the certificate. This certificate is valid for 365 days by default. If you want a different certificate lifetime, change the `default_days` parameter in the openssl.cfg file, or use the `–days` parameter to the `openssl ca` command to specify a different lifetime.

h. Type the following command to place the remote IMV server key and certificate in a PKCS#12 file (substitute the challenge password you entered previously for `<password>` in this command):
   ```
   openssl pkcs12 -export -in rimvs_cert.pem -inkey rimvs_key.pem -passout pass:<password> -out rimvs_p12.pem
   ```

i. On the remote IMV server, select Programs > Pulse Secure > Remote IMV Server > Remote IMV Server Configurator from the Start menu.

5. Under Client Info, click Add.

6. Configure the port to service SOAP requests from Policy Secure.

7. Enter the client's IP address, the number of addresses to use, and the shared secret used by both Policy Secure and the remote IMV server.

8. (Optional) Change logging settings (log is generated in the install directory).

9. Browse and find the PKCS#12 file you generated in the file system.

10. Specify the password associated with the certificate.

11. Select the System > Configuration > Certificates > Trusted Server CAs tab to import the trusted root CA certificate of the CA that issued the certificate for the remote IMV server.

   If you used OpenSSL to generate the remote IMV server's server certificate is:
   ```
   demoCA\cacert.pem.
   ```

   If you did not use OpenSSL to generate this certificate, ensure that the file you import has the CA certificate (not the root certificate).
12. Click Import Trusted Server CA and browse for the server certificate used on the remote IMV server.

13. Add the new remote IMV server:

To specify the remote IMV server so that Policy Secure can communicate with it:

a. In the admin console, select Authentication > Endpoint Security > Host Checker.


c. In the New Server page:

i. Create a label for the server using the Name and (optional) Description fields.

ii. In the Hostname field, enter either the IP address or hostname as defined in the server certificate.

iii. In the Port field, enter the unique port number Policy Secure uses to communicate with the remote IMV server. Ensure that no other service is using this port number.

   The default port number is the same as the default HTTPS port number. If you are running a web server on the same system as the Remote IMV Server, enter a new port number in the Port field.

iv. In the Shared Secret field, enter the same shared secret used in the client information entry on the remote IMV server.

v. Click Save Changes.

d. Under Remote IMV, click New IMV to specify the third-party IMV.

e. In the New IMV page:

i. Create a label for the IMV using the Name and (optional) Description fields.

ii. In the IMV Name field, enter the name of the IMV. This name must match the “human-readable name” in the IMV’s well-known registry key on the remote IMV server. For more information about human readable names and the well-known registry key, see www.trustedcomputinggroup.org.

iii. From the Primary Server menu, select the remote IMV server where this IMV is installed.

iv. (Optional) From the Secondary Server menu, select the secondary remote IMV server where this IMV is installed. The secondary server acts as a failover in case the primary server becomes unavailable.
Policy Secure continues to try to re-establish connection to the primary remote IMV Server, and uses the primary Remote IMV Server on subsequent handshakes once it becomes available.

v. Click Save Changes.

f. Click Save Changes.

Related Documentation

- Using Third-Party Integrity Measurement Verifiers on page 19
- Implementing a Third-Party IMV Policy on page 73
CHAPTER 12

Statement of Health

- Configuring a Statement of Health Host Checker Policy on page 59

Configuring a Statement of Health Host Checker Policy

To configure a SOH policy in Host Checker:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create a new policy or click on an existing policy in the Policies section of the page.
3. Click the Windows tab.
5. Click Add under Rule Settings. The Statement of Health page is displayed.
6. Type a Rule Name for this rule.

To configure a local SOH Host Checker policy:

1. Under Criteria, enter a Label for a SOH parameter.
2. Select an SOH policy option from the Parameter menu then click Add for the following types:
   - Antivirus Enabled
   - Antivirus up to date
   - Antispyware enabled
   - Antispyware up to date
   - Firewall Enabled
   - Automatic Updating Enabled
3. Select additional options from the Parameterlist to add additional SOH parameters.
4. Select the check box for each item to activate that item for this Host Checker SOH policy.
NOTE: Each SOH rule receives one SOHR. If a single Host Checker rule has multiple policy configurations, all of these are remediated by one SOHR.

5. (Optional) For each rule, select the Enable automatic remediation check box. If you select this option for a rule, the user will receive a message from the SOH agent, and appropriate remediation is performed, if possible. If the box is not checked the user receives a message.

NOTE: For remediation to succeed, you must configure at least one remediation role for the user. If the user cannot negotiate a realm with at least one role, the user cannot be authenticated and the SOHR is ignored by the SOH agent.

6. Click Save Changes.

To configure a SOH Host Checker policy using a remote NPS:

1. If you have not already done so, configure Policy Secure for 802.1X enforcement with the Windows client.

NOTE: You must configure an authentication protocol set that includes the EAPSOH protocol for negotiation with the Windows supplicant.

2. Ensure that your NPS server is configured in accordance with the applicable server documentation.

3. Ensure that the non-Pulse Secure supplicants are configured to authenticate using the appropriate authentication protocols for SOH communication.

4. Under Settings, select the Use NPS Server check box. The Criteria section on the page disappears. You cannot combine a remote NPS rule with a local rule.

5. Enter the following remote server settings:
   - Server IP address
   - Shared Secret of the server
   - Maximum Retries

6. Click Save Changes.
NOTE: To use SOH Host Checking on a Windows host machine, you must configure the client to use EAP. Use the EAP enforcement ID 79623 for both the Vista and Windows XP SP3 supplicants.

For Windows Vista instructions, see the following Web site:

For Windows XP SP3 instructions, see the following Web site:

Related Documentation

Using Statement of Health Integration Host Checker Policies on page 21
PART 4

Administration

- Host Checker on page 65
- Third Parties and Plug-Ins on page 71
- Customized Requirements on page 77
CHAPTER 13

Host Checker

- Creating Global Host Checker Policies on page 65
- Implementing Host Checker Policies on page 66
- Specifying General Host Checker Options on page 68

Creating Global Host Checker Policies

To use Host Checker as a policy enforcement tool for managing endpoints, you create Host Checker policies, and then implement the policies at the realm or role level.

Policy Secure provides options that you can use to enable, create, and configure Host Checker policies:

- Pre-defined rules (check for third party applications on Windows machines)—Host Checker contains a wide array of predefined rules that monitor antivirus software, firewalls, malware, spyware, and specific operating systems from a variety of industry leaders. You can enable one or more of these rules within a Host Checker client-side policy to ensure that the integrated third-party applications that you specify are running on users’ computers.

- Custom rules (check for additional requirements)—In addition to predefined rules, you can create custom rules within a Host Checker policy to define requirements that user endpoints must meet. Using custom rules, you can:
  - Configure Host Checker to check for custom third-party DLLs that perform customized client-side checks.
  - Verify that certain ports are open or closed on the user’s computer.
  - Confirm that certain processes are or are not running on the user’s computer.
  - Verify that certain files are or are not present on the client machine.
  - Evaluate the age and content of required files through MD5 checksums.
  - Confirm that registry keys are set on the client machine (Windows only).
  - (Windows only) Check the NetBIOS name, MAC addresses, or certificate of the client machine.
  - (Windows only) Assess the client operating system and application service packs to ensure they are up to date.
  - (Windows only) Perform application and version checks to ensure that endpoints are running the correct software.
Within a single policy, you can create different Host Checker requirements for Windows, Macintosh, Linux and Solaris, checking for different files, processes, and products on each operating system. You can combine any number of host check types within a single policy and check for alternative sets of rules.

Task Summary: Configuring Host Checker on page 33

Implementing Host Checker Policies

After you create global policies, you can restrict network and resource access by requiring Host Checker in the following ways:

- Realm authentication policy—When administrators or users try to sign in, the system evaluates the specified realm’s authentication policy to determine when the preauthentication requirements include Host Checker. You can configure a realm authentication policy to download Host Checker, launch Host Checker and enforce Host Checker policies specified for the realm, or you can not require Host Checker. The user must sign in using a computer that adheres to the Host Checker requirements specified for the realm. If the computer does not meet the requirements, then the system denies user access unless you configure remediation actions to help the user bring his computer into compliance. You can configure realm-level restrictions from the admin console. If you have enabled Advanced Endpoint Defense, you can select this feature from any realm.

- Role—When the system determines the list of eligible roles to which it can map an administrator or user, it evaluates each role’s restrictions to determine whether the role requires the user’s computer to adhere to certain Host Checker policies. If it does and the computer does not follow the specified Host Checker policies, then the system does not map the user to that role unless you configure remediation actions to help the user bring the computer into compliance. You can configure role-mapping using settings in the Users > User Realms > SelectRealm > Role Mapping page. You can configure role-level restrictions from the Host Checker page. If you have enabled Advanced Endpoint Defense Malware Protection, you can implement this feature for any role.
Executing Host Checker Policies

When the user tries to access the network or resource, Host Checker evaluates policies in the following order:

1. Initial evaluation—When a user first tries to access the sign-in page, Host Checker performs an initial evaluation. Using the rules you specify in your policies, Host Checker verifies that the client meets endpoint requirements and returns the results to Policy Secure. Host Checker performs an initial evaluation regardless of whether you have implemented Host Checker policies at the realm, role, or resource policy level.

For agentless deployments, if the user navigates away from the sign-in page after Host Checker starts running but before signing in, Host Checker continues to run on the user’s machine until the process times out. If Policy Secure does not receive a result from Host Checker for any reason (including the user manually terminating Pulse, OAC or Host Checker), the system displays the remediation instructions (if they are enabled), or displays an error and directs the user back to the sign-in page.

If the Host Checker process returns a result, the system then evaluates the realm-level policies.

2. Realm-level policies—The system uses the results from Host Checker’s initial evaluation to determine which realms the user can access. Then the system displays or hides realms, allowing the user to sign only into those realms that you enable for the sign-in page, and if the Host Checker requirements for each realm are met. If the user cannot meet the Host Checker conditions required by available realms, the system does not display the sign-in page. Instead, it displays an error stating the user has no access unless you bring the endpoint into compliance.

Note that Host Checker performs realm-level checks when the user first signs in and throughout the user’s session.

3. Role-level policies—After the user signs in to a realm, the system evaluates role-level policies and maps the user to the role or roles if the Host Checker requirements for those roles are met. Then, the system pushes the role and policy information to the Infranet Enforcer and to Pulse or OAC.

If Host Checker returns a different status during a periodic evaluation, the system dynamically remaps the user to roles based on the new results. If the user loses rights to all available roles during one of the periodic evaluations, the system disconnects the user session unless you bring the endpoint into compliance.

4. Infranet Enforcer Resource Access Policies—After the system pushes the role and policy information to the Infranet Enforcer and to Pulse or OAC, the user can try to access a protected resource that is controlled by an Infranet Enforcer resource access policy or Host Enforcer policy. The Infranet Enforcer and Pulse or OAC determine whether to allow or deny the user access to the protected resource based on the user’s assigned role.

If Host Checker returns a different status during a periodic evaluation, the new status can change the assigned roles. The system then pushes the new role and policy information to the Infranet Enforcer and Pulse or OAC, which might prevent the user from accessing the protected resource.
With either a success or failure, Pulse, OAC, or Host Checker remain on the client. Windows users can manually uninstall OAC by choosing OAC in the Add or Remove Programs control panel.

If you enable client-side logging through the, the directory where Pulse or OAC is installed contains a log file, which the system appends each time the client or Host Checker runs.

You can specify that the system evaluate your Host Checker policies only when the user first tries to access the realm or role that references the Host Checker policy. Or you can specify that the system periodically re-evaluate the policies throughout the user’s session. If you periodically evaluate Host Checker policies, the system dynamically maps users to roles and instructs the Infranet Enforcer and Pulse or OAC to allow users access to new resources based on the most recent evaluation.

Related Documentation

- Configuring Host Checker Restrictions on page 35
- Specifying General Host Checker Options on page 68

Specifying General Host Checker Options

You can specify global options for Host Checker that apply to any user for whom Host Checker is required in either an authentication policy or a role-mapping rule.

To specify general Host Checker options:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Under Options:
   - In the Perform check every X minutes field, 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, then the Infranet Enforcer or OAC denies the associated user requests.

For example, you might require that a user runs a specific third-party antivirus application to map to Role A, which enables the user to access protected resources. If the user’s client machine is running the required antivirus application when the user signs in, then the user maps to Role A and is granted access to the protected resources specified for Role A in an Infranet Enforcer resource access policy. However, if the antivirus application stops running during the user session, the next time Host Checker runs, the user fails to meet the security requirements for Role A and, therefore, loses all access privileges for Role A.

When a user logs in to a Realm, Host Checker performs an initial policy check, regardless of whether the policy is enforced at the realm, role, or resource level. The initial policy check establishes a start time. Host Checker evaluates policies at the frequency set by the Perform check every X minutes option, starting the clock at the initial policy check. Although the frequency setting is set globally for all Host Checker policy checking, it is not synchronized for all user clients connected to Policy Secure.
Chapter 13: Host Checker

Each client performs its own initial policy check and starts its own countdown. If you configure the authentication policy within a realm where Host Checker enforces policies (versus installing), the enforcement occurs only during the preauthentication phase. After an end-user signs in and for the duration of the user's session, any subsequent Host Checker policy checks have no impact on realm access, meaning that there is no concept of removing an end-user session from a realm once a user successfully authenticates into that realm.

If you configure a role restriction where Host Checker enforces policies, the enforcement occurs just after authentication during role-mapping. Role restrictions are enforced periodically during the end-user session at an interval specified using the Host Checker frequency setting. If the user successfully passes the Host Checker evaluation during role-mapping but later fails X minutes after login, that specific user loses rights to that role. If the user loses rights to all available roles due to Host Checker policy evaluation, the user session is disconnected.

NOTE: If you enter a value of zero, Host Checker runs on the client machine only when the user first signs in.

- (Applies to agentless access deployments only) For the Client-side process, login inactivity timeout option, specify an interval to control timing out in the following situations:
  - If the user navigates away from the sign-in page after Host Checker starts running but before signing in, 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.

3. Click Save Changes.

4. Implement the policy at the realm or role levels. To verify that the package itself is installed and running on the client computer (as opposed to a specific policy in the package passing or failing) you can use the name you specified when you uploaded the policy package (for example, myPestPatrol). To enforce a particular policy in the package, use the syntax `<PackageName>, <PolicyName>`. For example, to enforce the FileCheck policy in the myPestPatrol package, use myPestPatrol.FileCheck.

Related Documentation

Configuring Host Checker Restrictions on page 35
CHAPTER 14

Third Parties and Plug-Ins

- Checking for Third-Party Applications Using Predefined Rules on page 71
- Implementing a Third-Party IMV Policy on page 73
- Upgrading the Endpoint Security Assessment Plug-In on page 73

Checking for Third-Party Applications Using Predefined Rules

Host Checker comes equipped with a vast array of predefined rules that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of vendors. You can enable one or more of these rules within a Host Checker client-side policy to ensure that integrated third-party applications are running on users’ computers in accordance with your specifications. For firewall and antivirus rules, you can specify remediation actions to automatically bring the endpoint into compliance.

To view the currently supported applications, select Authentication > Endpoint Security > Host Checker and create a new policy. You can choose predefined rule types from the Select Rule Type list to see a list of the supported applications within that category. The lists of applications can be extensive and are updated at each support release, so check the list periodically.

The following predefined rule types are available:

- Predefined: AntiVirus—Select this option to create a rule that checks for the antivirus software that you specify, and to specify remediation options.
- Predefined: Firewall—Select this option to create a rule that checks for the firewall software that you specify, and to specify remediation options.
- Predefined: Malware—Select this option to create a rule that checks for the malware protection software that you specify.
- Predefined: AntiSpyware—Select this option to create a rule that checks for the antispyware protection software that you specify.
- 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.)
NOTE: If the underlying TNCC service is killed or stopped, the endpoint can remain on the network, possibly out of compliance, until the next refresh of the Host Checker policy.

This section details Predefined Malware and Predefined OS check. Predefined Antivirus, Firewall and Malware checks are defined in sections that follow.

To create a Host Checker rule using Predefined Malware or Predefined OS check rules:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create a new policy, or select an existing policy in the Policies section of the page.
3. Under Rule Settings, choose one of the following options and click Add:
   - Predefined Malware
   - Predefined OS Checks
   The predefined rule page opens.
4. In the Rule Name field, enter an identifier for the rule.
5. Under Criteria, select the specific malware or operating systems check for and click Add. (When checking for an operating system, you can also specify a service pack version.)

NOTE: When you select more than one type of software within a predefined rule, Host Checker considers the rule satisfied if any of the selected software applications are present on the user's machine.

6. 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, Policy Secure initiates a new handshake to re-evaluate realm or role assignments.
7. Click Save Changes.
8. (Optional) Add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Task Summary: Configuring Host Checker on page 33

- Configuring a Predefined Antivirus Rule with Remediation Options (Windows and Macintosh) on page 41
- Configuring a Predefined Firewall Rule with Remediation Options (Windows and Macintosh) on page 43
- Configuring a Predefined AntiSpyware Rule (Windows and Macintosh) on page 45
Implementing a Third-Party IMV Policy

To use Host Checker as a policy enforcement tool for managing endpoints, you must create global Host Checker policies at the system level and then implement the policies at the realm and role levels.

NOTE: The Custom: Remote IMV option does not appear until you add the Remote IMV New Server and New IMV on the main Host Checker page.

To implement the third-party IMV policy:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
3. Enter a name in the Policy Name field and click Continue. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
5. In the Add Custom Rule: Remote IMV page:
   a. In the Rule Name field, enter an identifier for the rule.
   b. Under Criteria, select the third-party IMV to associate with this rule.
   c. Click Save Changes.
6. Specify how Host Checker must evaluate multiple rules within the policy.
7. (Recommended) Specify remediation options for users whose computers do not meet the requirements specified in the policy.
8. Click Save Changes.
9. Implement the policy at the realm or role level.

Using Third-Party Integrity Measurement Verifiers on page 19
- Configuring a Remote IMV Server on page 53

Upgrading the Endpoint Security Assessment Plug-In

The Endpoint Security Assessment Plug-in (ESAP) on the system verifies third-party applications on endpoints for compliance with the pre-defined rules you configure in a Host Checker policy. This plug-in is included in the system software package.

New plug-in releases are available independently and more frequently than new releases of the system software package. If necessary, you can upgrade the plug-in independently of a system upgrade.
You can upload up to four versions of the plug-in, but the system uses only one version at a time (called the active version). If necessary, you can rollback to a previously active version of the plug-in.

If the endpoints in your deployment connect to multiple servers simultaneously, all of those connected servers must use the same version of the ESAP plug-in.

To upgrade the ESAP plug-in:

1. Download the Endpoint Security Assessment Plug-in from the Juniper Networks Customer Support Center to your computer:
   a. Open the following page:
      http://www.pulsesecure.net/support
   b. To access the Customer Support Center, enter a username and password for a Pulse Secure Support Center account.
   c. Click the ESAP Download Page link.
   d. Navigate to the ESAP release you want.
   e. Download the plug-in zip file to your computer.

2. Select Authentication > Endpoint Security > Host Checker.

3. On the Host Checker page, under Manage Endpoint Security Assessment Plug-In Versions:
   a. If you previously uploaded four versions of the component software, you must delete one of the versions before you can upload another one. Select the version you want to delete and click Delete.
   b. If you want Policy Secure to actively begin using the new component software immediately after you upload it, select the Set as active after upload option.
   c. Click Browse, select the plug-in file to upload and click OK.
   d. Click Upload. While the system uploads and decrypts the plugin .zip file, the message “Loading...” is displayed in the plug-in list under Manage Endpoint Security Assessment Plug-In Versions. If the system is a member of a cluster, it displays the message “Loading...” while the plug-in is transferred to the other cluster nodes. After the plug-in is installed, the date and time of the plug-in installation is displayed in the plug-in list.
   e. If you did not select the Set as active after upload option, activate the plug-in to use by selecting the version in the plug-in, list and click Activate.
NOTE:

- If you attempt to activate a version of the plug-in that does not support all of the predefined rules already configured in all Host Checker policies, the system does not allow activation of that plug-in version. For example, if a Host Checker policy is configured to use a predefined rule to check for a version of antivirus software, and you attempt to activate a plug-in version that does not support that version of the antivirus software, the system does not allow you to activate that plug-in version. To view the list of supported products for a particular plug-in version, click the plug-in version number under Manage Endpoint Security Assessment Plug-In Versions.

- You can rollback to an older plug-in version after you upgrade to a later version by selecting the older version as the active version. But, if you modified any Host Checker policies after you upgrade to the later version, the rollback might not succeed. Rollback is guaranteed to succeed only if the policies did not change.

- If you upgrade the system software to a newer version, or if you import a user configuration file, the currently active plug-in version does not change. If you want to use a different plug-in version after you upgrade or importing a user configuration file, you must manually activate that plug-in version.

- If the system already has four versions of the plug-in installed when you upgrade the system software to a newer version, the system automatically deletes the oldest plug-in version and installs, but does not activate, the plug-in included with the new system software.
Customized Requirements

- Specifying Customized Requirements Using Custom Rules on page 77

Specifying Customized Requirements Using Custom Rules

In addition to the predefined policies and rules that come with Policy Secure, you can create custom rules within a Host Checker policy to define requirements that your users’ computers must meet. Custom rules, allow you to:

- Configure remote integrity measurement verifiers (IMVs) to perform customized client-side checks.
- Configure Host Checker to check for custom DLLs that perform customized client-side checks.
- Verify that certain ports are open or closed on the user’s computer.
- Confirm whether certain processes are or are not running on the user’s computer.
- Confirm whether certain files are or are not present on the client machine.
- Evaluate the age and content of required files through MD5 checksums.
- Confirm that registry keys are set on the client machine, and specify remediation actions.
- Confirm the NetBios name of the client machine.
- Confirm the MAC addresses of the client machine.
- Check the validity of the machine certificate that is installed on the user's computer.

NOTE: You can only check for registry keys, third-party DLLs, NetBios names, MAC addresses, and machine certificates on Windows computers.

To create a client-side Host Checker policy:

1. In the admin console, select Authentication > Endpoint Security > Host Checker.
2. Create a new policy or click an existing policy in the Policies section of the page.
3. Click the tab that corresponds to the operating system for which you want to specify Host Checker options—Windows, Macintosh, Linux, or Solaris. In the same policy, you can specify different Host Checker requirements on each operating system.
For example, you can create one policy that checks for different files or processes on each operating system.

NOTE: You must explicitly create policies for each operating system you want to allow. For example, if you create a Windows Host Checker policy. But you do not create one for Macintosh or Linux, users who sign in from a Macintosh or Linux machine do not comply with the Host Checker policy and therefore will not be able to access the realm, role, or resource on which you enforce Host Checker.

4. Under Rule Settings, select the options in the following sections and click Add. The Add Custom Rule page for the rule type is displayed.

- Custom: Remote IMV—Configures integrity measurement software that a client must run to verify a particular aspect of the client’s integrity, such as the client’s operating system, patch level, or virus protection.
- 3rd Party NHC Check (Windows only)— Specifies 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 rule is met. In the 3rd Party NHC Check configuration page:
  a. Enter a name and vendor for the 3rd Party NHC Check rule.
  b. Enter the location of the DLL on client machines (path and file name).
  c. Click Save Changes.

  The 3rd Party NHC Check feature is provided primarily for backwards compatibility. We recommend that you use IMCs and IMVs instead.

- Ports—Controls 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 network. In the Ports configuration page:
  a. Enter a name for the port rule.
  b. Enter a comma-list (without spaces) of ports or port ranges, such as 1234,11000-11999,1235.
  c. Select Required to require that these ports are open on the client machine, or select Deny to require that they are closed.
  d. Under Optional, select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints. If a compliance status changes on an endpoint that has successfully logged in occurs, Policy Secure initiates a new handshake to re-evaluate realm or role assignments.
  e. Click Save Changes.

- Process—Controls the software that a client can 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 Policy Secure. In the Processes configuration page:
Chapter 15: Customized Requirements

a. Enter a name for the process rule.

b. Enter the name of a process (executable file), such as good-app.exe.

NOTE: For Linux, Macintosh and Solaris systems, the process that is being detected must be started using an absolute path.

---

You can use a wildcard character to specify the process name.

For example: good*.exe

c. Select Required to require that this process is running, or select Deny to require that this process is not running.

d. (Optional) Specify the MD5 checksum value of each executable file to which you want the policy to apply. For example, an executable can 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>.

e. Click Save Changes.

• File—Ensures that certain files are present or not present on the client machine before the user can access the network. You can also use file checks to evaluate the age and content (through MD5 checksums) of required files and to allow or deny access accordingly. In the Files configuration page:

  a. Enter a name for the file rule.

  b. 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 <\%> characters. For example:

    <%windir%>\bad-file.txt

c. Select Required to require that this file is present on the client machine, or select Deny to require that this file is not present.

d. (Optional) Specify the minimum version of the file. 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 later, of notepad.exe.
e. (Optional) Specify the maximum age (File modified less than n days) (in days) for a file. If the file is older than the specified number of days, then the client does not meet the attribute check requirement.

NOTE: You can use the maximum age option to verify the age of virus signatures. Make sure you specify the path to a file in the File Name field whose timestamp indicates when virus signatures were last updated, such as a virus signature database or log file that updates each time the database updates. For example, if you use TrendMicro, you can specify:

C:\Program Files\Trend Micro\OfficeScan Client\TmUpdate.ini.

f. (Optional) Specify the MD5 checksum value of each file to which you want the policy to apply. On Macintosh, Linux, and Solaris, you can determine the MD5 checksum by using this command: openssl md5<filePath>

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

h. Click Save Changes.

- Registry Setting (Windows only)—Controls the corporate PC images, system configurations, and software settings that a client needs to have to access the network. This rule type ensures that certain registry keys are set on the client machine before the user can access the network. You may also use registry checks to evaluate the age of required files and to allow or deny access accordingly. In the Registry Settings configuration page:

  a. Enter a name for the registry setting rule.

  b. Select a root key from the list.

  c. Enter the path to the application folder for the registry subkey.

  d. (Optional) Enter the name of the key’s value that you want to require. This name is displayed in the Name column of the Registry Editor.

  e. (Optional) Select the key value’s type (String, Binary, or DWORD) from the list. This type is displayed in the Type column of the Registry Editor.

  f. (Optional) Specify the required registry key value. This information is displayed 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 system uses lexical sorting to determine whether the client contains the specified version or higher. For example:
3.3.3 is newer than 3.3
4.1 is newer than 3.3
4.0a is newer than 4.0b
4.2 is newer than 3.3.1

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

g. 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, Policy 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.

h. Select the Set Registry value specified in criteria check box.

i. Click Save Changes.

• NetBIOS (Windows only, does not include Windows Mobile)—Verifies the NetBIOS name of the client machine before the user can access the network. In the NetBIOS configuration page:
  a. Enter a name for the NetBIOS rule.
  b. 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.
  c. 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.
  d. Click Save Changes.

• MAC Address (Windows only)—Verifies the MAC addresses of the client machine before the user can access the network. In the MAC Address configuration page:
  a. Enter a name for the MAC address rule.
  b. Enter a comma-delimited list (without spaces) of MAC addresses in the form XX:XX:XX:XX:XX:XX where the X is a hexadecimal number. For example: 00:0e:1b:04:40:29
You can use a wildcard character to represent a 2-character section of the address. For example, you can use a wildcard to represent the "04", "40", and "29" sections of the previous example address:

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

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

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

c. Select Required to require that a MAC address of the client machine matches any of the addresses you specify, or select Deny to require that all of your 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 requirement is met if any of the addresses you specify match any MAC address on the client machine.

d. Click Save Changes.

---

NOTE: Since the MAC address is changeable on some network cards, this check does not guarantee that a client machine meets the requirements of your Host Checker policy.

---

• Machine Certificate (Windows only)—Verifies that the client machine is permitted access by validating the machine certificate stored on the client machine. In the Machine Certificate configuration page:

a. Enter a name for the machine certificate rule.

b. From the Select Issuer Certificate list, select the certificate 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.

c. In the Optional fields (Certificate field and Expected value), specify any additional criteria for Host Checker to use to verify the machine certificate.

d. Click Save Changes.

---

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 Policy Secure for validation.

• Do not apply remediation options for endpoints that are authenticated using machine certificates.

---

5. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.
Related Documentation

- Task Summary: Configuring Host Checker on page 33
- Checking for Third-Party Applications Using Predefined Rules on page 71
- Using a Wildcard or Environment Variable in a Host Checker Rule on page 15
PART 5

Troubleshooting

- Host Checker on page 87
CHAPTER 16

Host Checker

- Using Host Checker Logs on page 87

Using Host Checker Logs

You can enable client-side logging for the Host Checker and OAC. When you enable this option, the IC Series device writes a client-side log to endpoints. The IC Series device appends to the log file during user session. This feature is useful when you work with the support team to debug problems with the respective feature.

Because these settings are global, the IC Series device writes a log file to all clients that use the feature for which you enable client-side logging. Also, the IC Series device does not remove client-side logs. Users must manually delete log files from the clients. For information about where the Policy Secure gateway installs log files, see the Client-Side Changes Guide at the Pulse Secure Global Support Center site at http://www.pulsesecure.net/support

To specify global client-side logging settings:

1. In the admin console, select System > Log/Monitoring > Client Log > Settings.
2. Select the features for which the IC Series device writes client-side logs.
3. Click Save Changes to save these settings globally.

Related Documentation

Task Summary: Configuring Host Checker on page 33