Host Checker Configuration Guide

Published August 2020

Document Version 1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Host Checker Configuration Guide

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

END USER LICENSE AGREEMENT

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

Host Checker

Overview

Host checker is a client-side agent that performs endpoint health and security checks for hosts that attempt to connect to a Connect Secure device. It supports two types of rules within a policy; predefined and custom. The pre-defined inspection capabilities consist of health and security checks including antivirus versions, antispyware, OS versions, hard disk encryption status and patch checks. The pre-defined rules are provided by OPSWAT and it uses the ESAP plug-in for pre-defined checks.

Custom rules allow admin to define checks to collect system health using Integrity message collector (IMC) and evaluate using Integrity message verifier (IMV) of TNC framework. The custom rules are created by the admin to include inspection checks such as absence or presence of specific file, certificate checks, TCP ports, processes, registry key settings, NetBIOS name, MAC addresses or certificate of the client machine and third-party inspection methods (custom DLLs).

You can invoke Host Checker at the role level, or the realm level to specify access requirements for endpoints attempting to authenticate.

All Host Checker rules are implemented through IMCs and IMVs based on the TNC open architecture. IMCs are software modules that Host Checker runs on the client machine. You can also 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.

- IMCs are responsible for collecting information, such as antivirus, antispyware, patch management, firewall, and other configuration and security information for a client machine.
- IMVs are software modules running on the device that are responsible for verifying a particular aspect of an endpoint's integrity.
- The system and Host Checker manage the flow of information between the corresponding pairs of IMVs and IMCs. Each IMV on the device works with the corresponding IMC on the client machine to verify that the client meets the Host Checker rules.

Trusted Network Connect

Host Checker is compliant with the Trusted Network Connect (TNC) model developed by Trusted Computing Group (TCG). TCG created an architecture and set of standards for verifying endpoint integrity and policy compliance during or after a network access request. For more information about TNC, see www.trustedcomputinggroup.or

Policies

Pulse Policy Secure(PPS) Host checker component supports many different type of product policy evaluation on endpoint along with continues monitoring of system health. The below table lists the description of various policies and features, which can be defined as part of device compliance check.

Table 1 Supported Policies

Policy	Description
Predefined	
Antivirus Policy	Policy to detect whether the Antivirus is installed and up-to-date with latest virus signatures. It also includes other options to check the last scan time, virus signature download, and remediation options.
Firewall Policy	Policy to detect the firewall installed on endpoint and the remediation option to turn on the firewall if it's turned off.
Anti-Spyware Policy	Policy to detect the installed spyware on endpoints.
Hard disk Encryption	Policy to detect and check the encryption status of the specified or all drives using installed encryption software.
Patch Management	Policy to check whether the required operating system patches are installed properly.
OS Checks	Policy to check the version of the windows operating systems and minimum service packs.
Common Vulnerability and Exposure (CVE)	Policy to check any vulnerable attacks such as ransomware attack.
System Integrity Protection (SIP)	Policy to check the status (enabled/disabled) of System Integrity Protection (SIP) on the Mac OS endpoints.
Custom	
3rd Party NHC Check	Policy to specify the location of custom DLL files.
Ports policy	Policy to check if a particular port is either opened or closed to allow or reject the user authentication.
Process policy	Policy to control the software or processes that runs on the client machine.
File policy	Policy to check if a particular file with specific version or checksum, or last modified file is present on endpoint to allow or reject the user authentication.
Registry Settings policy	Policy to check the registry and its value to allow or reject the user authentication, with a remediation option to set the registry value if not configured.
NetBIOS policy	Policy to check the NetBIOS name from list of NetBIOS names provided to control user access.
MAC Address policy	Policy to check if the endpoint MAC address is in the provided regex or white listing of mac addresses to control user access.
Machine Certificate policy	Policy to check for the required machine certificate on the endpoint to control user access. This policy evaluates both public and private keys of the installed machine certificate on endpoint for users using Pulse Client. For agentless users, only public key is evaluated.

Policy	Description
Advanced Host Checking	Policy to dynamically check the compliance status of the endpoints. It includes combining 2 policy types for obtaining the expected values of the check type. The expected values are fetched from registry location on the client machine for evaluating the policies. The advanced support for checking the expected values against another policy is supported on Ports, Process, File, Registry, NETBIOS, MAC Address, and Machine certificate.
Statement of Health	Policy to perform the health state validation to determine which roles or realms can be accessed by endpoints. It checks the system health indicators such as antivirus is enabled and up to date, antispyware is enabled and up to date, firewall is enabled and so on.
Command	Policy to check the versions of the installed applications on the Mac OS endpoints.
Host Checker General Settings	PPS provides following admin configuration options while performing host checking.
General Options	
Continuous Policy Evaluation	Option to configure periodic and continuous policy evaluation so that the endpoint is compliant with the Host Checker policy.
Virus Signature Version Monitoring	Option to monitor and verify the virus signatures, operating systems, and patches installed are up to date.
Pre-Authentication Host Checking	Pre-Authentication host checking are policies that are enforced at the realm level before authentication.
Post-Authentication Host Checking	Post-Authentication host checking are policies that are enforced when role assignment happens after authentication.

Supported Platform Matrix

A Host Checker policy contains one or more rules. Each rule can apply to different host checks and for different device types (Windows, Mac, Linux, Solaris, iOS, Android). The below table lists the Host Checker policies that are supported on Windows, Mac, Linux, and Solaris.

Table 2 Supported Policies for Agent/Agentless Login

Policy	Windows		Macintosh		Linux		Solaris		Mobile		
	Client	Client less	Client	Client less	Client	Client less	Client	Client less	Windows Phone & ChromeOS	iOS	Android
Antivirus	Yes	Yes*	Yes	Yes*	No	No	No	No	No	No	No
Firewall	Yes	Yes*	Yes	Yes*	No	No	No	No	No	No	No
AntiSpyware	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
Hard Disk Encryption	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
Patch Assessment	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
OS Checks	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Rooting Detection	No	No	No	No	No	No	No	No	No	No	Yes
Jail Breaking Detection	No	No	No	No	No	No	No	No	No	Yes	No
Common Vulnerability and Exposure (CVE) Check	Yes	Yes	No	No	No	No	No	No	No	No	No
3rd Party NHC Checks	Yes	Yes	No	No	No	No	No	No	No	No	No
Ports	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Process	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Files	Yes	Yes**	Yes	Yes**	Yes	Yes**	Yes	Yes**	No	No	No
Registry Setting	Yes	Yes***	No	No	No	No	No	No	No	No	No
NetBIOS	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
MAC Address	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
Machine Certificates	Yes	Yes****	Yes	Yes	No	No	No	No	No	No	No
Statement of Health	Yes	Yes	No	No	No	No	No	No	No	No	No
System Integrity Protection (SIP)	No	No	Yes	Yes	No	No	No	No	No	No	No
Command	No	No	Yes	Yes	No	No	No	No	No	No	No
Advanced Host Checking	Yes	Yes	No	No	No	No	No	No	No	No	No

Note:

- * In some occasions, Antivirus/Firewall products restricts the remediation actions to admin/services (For example but not limited to, turning on firewall). In such scenarios, certain remediation actions won't work with browser/clientless logins. Note that, this is defined by the corresponding security products.

- **Admin should enable system level access for accessing certain files and file locations for browser login.
- ***To access device-certificates from system store, the plugin needs admin rights. With browser/ clientless login private key verification is not supported in Agentless login.
- ****Registry verification requires admin privileges for accessing certain registry files. There are limitations with accessing some of the registry hierarchy for evaluating registry checks for browser login.
- Agentless mode with Profiler is supported only with Windows platforms. The supported policies are Antivirus, Firewall, Antispyware, OS checks, Ports, Process, NetBIOS, and MAC Address. For more information, see Profiler documentation.

Host Checker Remediation Capabilities

	Windows	Mac OS	Linux
Custom Instructions	Yes	Yes	Yes
Custom Actions	Yes	-	-
Kill Process	Yes	Yes	Yes
Delete Files	Yes	Yes	Yes
Reason String	Yes	Yes	Yes

Configuring Host Checker Policy

Note: Ensure that user endpoints have signed ActiveX components or signed Java applets enabled or PSAL downloaded within their browsers to permit Host Checker to download, install, and launch.

Due to the end of ActiveX and Java support on many browsers, an alternate solution is provided for launching of client applications such as Host Checker or Pulse Client called Pulse Secure Application Launcher (PSAL).

For a new user, launching the Host Checker for the first time, it involves following steps:

1. Download and install Pulse Application Launcher for the first time from PCS.
2. Launch Host Checker Using Pulse Secure Application Launcher.

To configure a Host Checker policy, perform these tasks:

1. Create and enable Host Checker policies through the **Authentication > Endpoint Security > Host Checker** page of the admin console.
2. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
3. Under Policies, click **New**.
4. Enter a name in the Policy Name field and then click **Continue**. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)

5. Create one or more rules to associate with the policy.
6. Configure additional system-level options on the **Authentication > Endpoint Security > Host Checker** page of the admin console as necessary:
   - If you want to display remediation information to users if they fail to meet the requirements of a Host Checker policy, configure remediation options through the Authentication > Endpoint Security > Host Checker page of the admin console.
   - For Windows clients, determine whether you need to use a pre-authentication access tunnel between the clients and policy server(s) or resources. If necessary, create a manifest.hcif file with the tunnel definition and upload it through the Authentication > Endpoint Security > Host Checker page of the admin console.
   - To change default Host Checker settings, configure settings through the **Authentication > Endpoint Security > Host Checker** page of the admin console.
7. Determine the level you that you want to enforce Host Checker policies:
   - To enforce Host Checker policies when the user initially accesses the device, implement the policy at the realm level by selecting the policy at the **Users > User Realms > *Select Realm* > Authentication Policy > Host Checker** page of the admin console.
   - To allow or deny users access to specific roles based on compliance with Host Checker policies, implement the policies at the role level by using the Users > User Roles > *Select Role* > General > Restrictions > Host Checker page of the admin console.
   - To map users to roles based on their compliance with Host Checker policies, use custom expressions in the Users > User Realms > *Select Realm* > Role Mapping page of the admin console.
   - To allow or deny users access to individual resources based on their compliance with Host Checker policies, use conditions in the Users > Resource Policies > *Select Resource* > Select Policy > Detailed Rules > Select|Create Rule page of the admin console.
8. Specify how users can access the Host Checker client-side agent that enforces the policies you define:
   - To enable automatic installation of the Host Checker client-side agent on all platforms, use the Administrators > Admin Realms > *Select Realm* > Authentication Policy > Host Checker page or the Users > User Realms > *Select Realm* > Authentication Policy > Host Checker page of the admin console.
   - To download the Host Checker installer and manually install it on your Windows users' systems, use the Maintenance > System > Installers page of the admin console.
9. Determine whether you want to create client-side logs. If you enable client-side logging through the System > Log/Monitoring > Client Logs page of the admin console, the system creates log files on your users' systems and writes to the file whenever Host Checker runs.

   If more than one valid session exists from the same system, and Host Checker is used in those sessions, all of the 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.

Creating Global Host Checker Policies

To use Host Checker as a policy enforcement tool for managing endpoints, you create Host Checker policies through the Authentication > Endpoint Security > Host Checker page of the admin console, and then implement the policies at the realm, role, and resource policy levels.

The system provides many options that you can use to enable, create, and configure Host Checker policies:

- Predefined policies (prevent in-network attacks or downloads malware detection software)-The system comes equipped with a predefined client-side Host Checker policy that you simply need to enable. The Connection Control policy prevents attacks on Windows client computers from other infected computers on the same network.
- Predefined rules (check for third party applications)-Host Checker contains a wide array of predefined rules that check for 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 your 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.
  - Check 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).
  - 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 (Windows only).
- Custom integrated applications (implement through server API)-For Windows clients, you can upload a third-party J.E.D.I. DLL to the system.
- Within a single policy, you can create different Host Checker requirements for Windows, Macintosh and Linux, checking for different files, processes, and products on each operating system. You can also can combine any number of host check types within a single policy and check for alternative sets of rules.

Enabling Connection Control Host Checker Policies

The predefined connection control Host Checker policy prevents attacks on Windows client computers from other infected computers on the same physical network.

Note: The Host Checker connection control policy is not supported on Windows Vista or Windows 7.

The Host Checker connection control policy blocks all incoming TCP, UDP and ICMP connections. This policy allows all outgoing TCP and VPN Tunneling traffic, as well as all connections to DNS servers, WINS servers, DHCP servers, proxy servers, and the system.

Note: Users must have administrator privileges in order for Host Checker to enforce the connection control policy on the client computer.

To enable the predefined Host Checker connection control policy:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker.**
2. Under Options, select the **Create Host Checker Connection Control Policy** check box.
3. Click **Save Changes.** The system enables the Host Checker connection control policy.

Note: Note that you cannot modify this policy-only enable or disable it. Also note that since you cannot modify this policy, the system does not display it in the Policies section of the Authentication > Endpoint Security > Host Checker page with other configurable policies.

4. Implement the Host Checker connection control policy at the realm, role, or resource policy levels.

   You must evaluate or enforce the connection control policy at the realm level to make the policy effective on client computers.

Creating and Configuring New Client-side Host Checker Policies

You can create a variety of policies through the Host Checker client that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can also create checks for custom third-party DLLs, ports, processes, files, registry keys and the NetBIOS name, MAC addresses, or certificate of the client machine.

Note: We recommend you check for multiple MAC addresses in a single policy instead of creating a policy for each MAC address. If you create policies for each MAC address, unexpected results may occur if there are more than 100 policies due to browser cookie size limitations.

When creating the policies, you must define the policy name, and either enable predefined rules, or create custom rules that run the specified checks. Optionally, you can specify how Host Checker should evaluate multiple rules within a single policy.

To create a standard client-side policy:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker.**
2. Under Policies, click **New**.
3. Enter a name in the **Policy Name** field and then click **Continue**. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
4. Create one or more rules to associate with the policy.
5. Specify how Host Checker should evaluate multiple rules within the policy.

6. (Recommended) Specify remediation options for users whose computers do not meet the requirements specified in the policy. (If you do not create remediation instructions and the policy fails, your users will not know why they cannot access their resources.)
7. Implement the policy at the realm, role, or resource policy levels.

Checking for Third-Party Applications Using Predefined Rules

Host Checker comes pre-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 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 your 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, go to **Authentication > Endpoint Security > Host Checker** and create a new policy. You can choose predefined rule types from the **Select Rule Type** drop down list box to see a list of the supported applications within that category. The lists of applications can be quite extensive and are updated at each support release, so it is useful to 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: AntiSpyware**-Select this option to create a rule that checks for the anti-spyware protection software that you specify.
- **Predefined: Hard Disk encryption**-- Select this option to create a rule that checks for the encryption software that you specify and check for the specified drives being encrypted or not using this encryption software.
- **Predefined: Patch Management-**-- Select this option to create a rule that checks for the patch Management 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.)
- **Predefined: CVE Checks**-Select this option to create a rule that helps in identifying the endpoints which are vulnerable using the OPSWAT library.
- **Predefined: System Integrity Protection**-Select this option to create a rule that helps in restricting various actions that root user can perform on the client machine.

Note: If the underlying TNCC service is killed or stopped, the endpoint can remain on the network, potentially out of compliance, until the next Host Checker policy refresh.

This section details Predefined Malware and Predefined OS check. Predefined Antivirus, Firewall and Malware checks, Hard Disk Encryption and Patch management 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 click on 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.

1. In the Rule Name field, enter an identifier for the rule.
2. Under Criteria, select the specific malware or operating systems that you want to check for and click Add. (When checking for an operating system, you may 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.

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

Note: Use this option only for dynamic rules, such as checking whether Real Time Protection is enabled on the antivirus software. Use the host checker update frequency to monitor other rules periodically.

Note: **Monitor this rule for change in result** for port check is applicable only for Windows and not for Linux or MAC machines.

4. Click **Save Changes**.g
5. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Configuring a Predefined Antivirus Rule with Remediation Options

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 should not be older than a specified number of updates.

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.

All of the remediation options are not supported for all antivirus software vendors' products. All available vendors and products that are supported are displayed when you select the **Require any supported product option** button.

Alternately, you can select the **Require specific products/vendors option** button and 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

To configure a Predefined Antivirus rule:

1. In the admin console, select A**uthentication > Endpoint Security > Host Checker**.
2. Create a new policy or click on an existing policy in the Policies section of the page.
3. Under Rule Settings, choose P**redefined: Antivirus** and click **Add**.
4. Enter the **Rule Name** for this antivirus rule.
5. To determine if your software vendor's product is supported for the System Scan check, click **these Antivirus products.** A new window will open with a list of all of the products that support the feature.
6. Select or clear the check box next to **Successful System Scan must have been performed in the last _ days,** and enter the number of days in the field.

   If you select this check box, a new option appears. If the remediation action to start an antivirus scan has been successfully begun, you can override the previous check.
7. Select or clear the check box next to **Consider this rule as passed if 'Full System Scan' was started successfully as remediation.**
8. Select or clear the check box next to **Virus definition files should not be older than _ updates**. Enter a number between 1 and 20. If you enter 1, the client must have the latest update. You must import the virus signature list for the supported vendor.
9. Select your antivirus vendor(s) and product(s) by using either the R**equire any supported product or Require specific products/vendors option** buttons.

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

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

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

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

   For each of the following remediation actions:

   - **Download latest virus definition files**-obtains the latest available file for the specified vendor from the vendor's web site
   - **Turn on Real Time Protection**-launches the virus scanning mechanism for the specified vendor
   - **Start Antivirus Scan**-performs a real-time virus scan for the specified vendor

   The check box is active (clickable) if the action is supported for your product.

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

10. If your product is supported, select the check box for any or all of the remediation actions that you want to apply.
11. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the system initiates a new handshake to re-evaluate realm or role assignments.

Note: Use this option only for dynamic rules, such as checking whether Real Time Protection is enabled on the antivirus software. Use the host checker update frequency to monitor other rules periodically.

Note: **Monitor this rule for change in result** for port check is applicable only for Windows and not for Linux or MAC machines.

12. Click **Save Changes** to save the antivirus rule and enforce antivirus remediation.
13. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Configuring a Predefined Firewall Rule with Remediation Options

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

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

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

To configure a Host Checker Predefined Firewall rule:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker.**
2. Create a new policy or click an existing policy in the Policies section of the page.
3. Under Rule Settings, choose **Predefined: Firewall** and click **Add**.
4. Enter a Rule Name for the firewall rule.
5. Select your firewall vendor(s) and product(s) by using either the **Require any supported product or Require specific products/vendors** option buttons.

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

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

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

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

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

6. If your firewall is supported, select the check box to Turn on Firewall.
7. Under Optional, select **Monitor this rule for change in resul**t to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the system initiates a new handshake to re-evaluate realm or role assignments.

Note: **Monitor this rule for change in result** for port check is applicable only for Windows and not for Linux or MAC machines.

8. Click **Save Changes** to save the firewall rule and enforce firewall remediation.
9. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Configuring a Predefined AntiSpyware Rule

You can configure Host Checker to check for installed antispyware on endpoints.

After you enforce the Host Checker rule, if an endpoint attempts to log in without the required spyware, the Host Checker rule will fail.

The option is not supported for all spyware products. All available products are displayed by using the Require any supported product or Require specific products/vendors option buttons.

To configure a Host Checker Predefined Spyware 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. Under Rule Settings, choose **Predefined: AntiSpyware** and click **Add**.
4. Enter a **Rule Name** for the firewall rule.
5. Select one of the following options:
   - Select the **Require any supported product** option button to check for any product (rather than requiring you to select every product separately).
   - Select the **Require specific products/vendors** option button to specify the spyware that you want to check for.
     - Choose either **Require any supported product from a specific vendor or Require specific products to specify spyware**.
     - Add antispyware from **Available Products** to **Selected Products**.
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, the system initiates a new handshake to re-evaluate realm or role assignments.

Note: **Monitor this rule for change in result** for port check is applicable only for Windows and not for Linux or MAC machines.

7. Click **Save Changes**.
8. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Configuring a Predefined Hard Disk Encryption Rule

You can configure Host Checker to check for installed Hard Disk Encryption on endpoints and specify the drives which needs to be encrypted using these software

After you enforce the Host Checker rule, if an endpoint attempts to log in without the required encryption software and the drives not encrypted, the Host Checker rule will fail.

The option is not supported for all Hard Disk Encryption products. All available products are displayed by using the Require any supported product or Require specific products/vendors option buttons.

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. Under Rule Settings, select **Predefined: HardDisk Encryption**.
4. Enter a **Rule Name** for the Hard Disk Encryption rule.
5. Select one of the following options:
   - Select the **Require any supported product option** button to check for any product (rather than requiring you to select every product separately).
   - Select the **Require specific products/vendors option** button to specify the spyware that you want to check for.
     - Choose either **Require any supported product from a specific vendor** or **Require specific products to specify spyware**.
     - Add Hard Disk Encryption Software from **Available Products** to **Selected Products**.
6. Under Drive Configuration, select the required option
   - **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.

- **Consider policy as passed if the drive Encryption is in progress** – Select this option to allow the Host Checker policy to pass if the encryption process is in progress and the drive is not fully encrypted. The drive encryption process takes time to complete depending up on the drive size and contents. For multiple drives, the HC policy passes only if the encryption process is in progress in all the drives.

7. Click **Save Changes.**

Configuring Predefined Patch Management Rules

You can configure Host Checker to check for installed Patch management Software on endpoints

After you enforce the Host Checker rule, if an endpoint attempts to log in without the required Patch Management Software, the Host Checker rule will fail.

The option is not supported for all Patch Management Software. All available products are under the Criteria Section.

Customers need to have their own patch management solution. Administrator is given option to configure the patch management software that needs to be verified on the endpoint.

On the client machine, Patch management software detects patch status based on the configured rules on corresponding patch management server. Detection of patches status on the client machine depends on the support provided by the 3rd party patch management solution that customer is using Hence different patch management software on the same client can report the status differently. To avoid conflicts, administrator is allowed to configure only one patch management software product on policy configuration page.

It provides options to configure various Severity and Category options that administrator is interested in. These additional details are used during policy evaluation such that only the missing patches that belongs to configured "**Severity**" and "**Category**" are considered. Any other patches that does not belong to configured "**Severity**" and "**Category**" are not considered during policy evaluation.

Default "**Severity**" options selected in policy are **Critical, Important**.

Default "**Category**" options selected in policy are S**ecurity Update, Critical Update, Regular Update, Driver Update.**

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/Mac** tab.

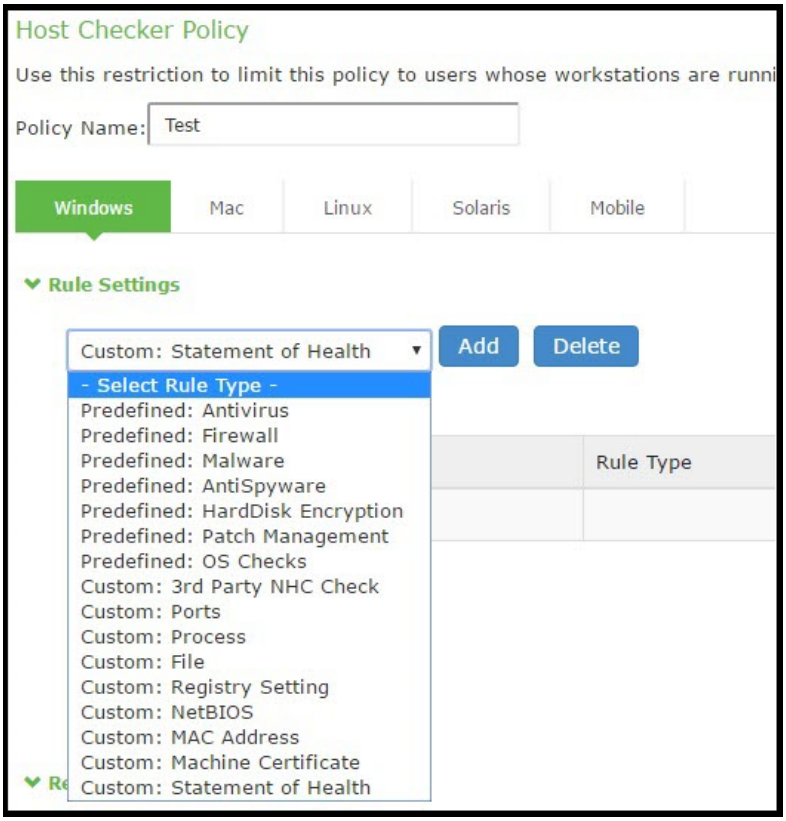
Note:

- The remediation support for patch management rule is not supported for Mac platform. If any missing patch is found, the endpoint will not be triggered to automatically install the missing patches. Currently, this is possible in Windows platform using SCCM client.
- Patch management on Mac OS is qualified only with one product that is Software Update on Mac 10.11, 10.12 and 10.13. You can use V4 SDK for Patch management on Mac platform.

4. Under Rule Settings, select **Predefined: Patch Management**.

Figure 1 shows the rule settings page for host checker.

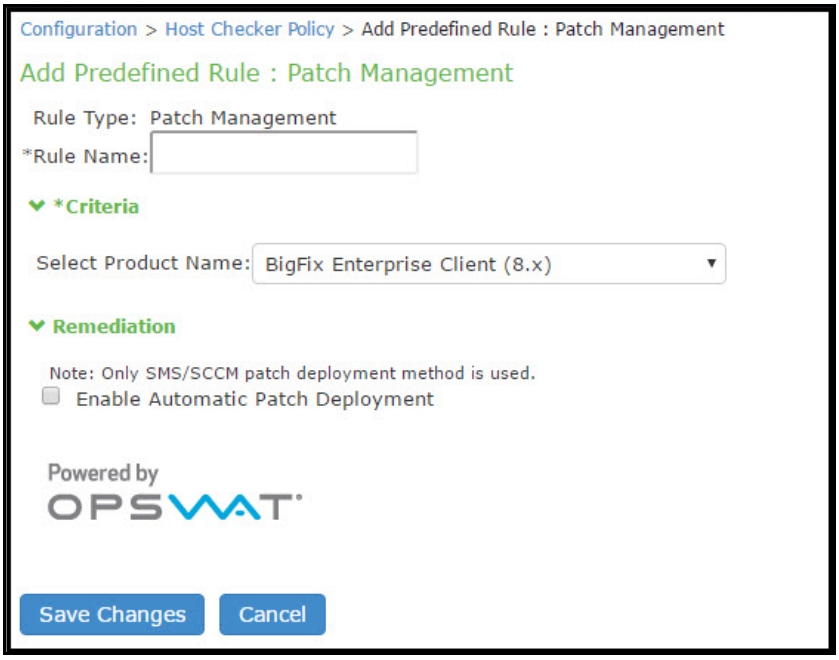
Figure 1 Rule Settings for Host Checker Policy



5. Under Rule Settings, click **Add**. The Add Predefined Rule:Patch Management page is displayed.

Figure 2 shows the configuration page to you use to add a patch management rule to the Host Checker policy.

Figure 2 Patch Management



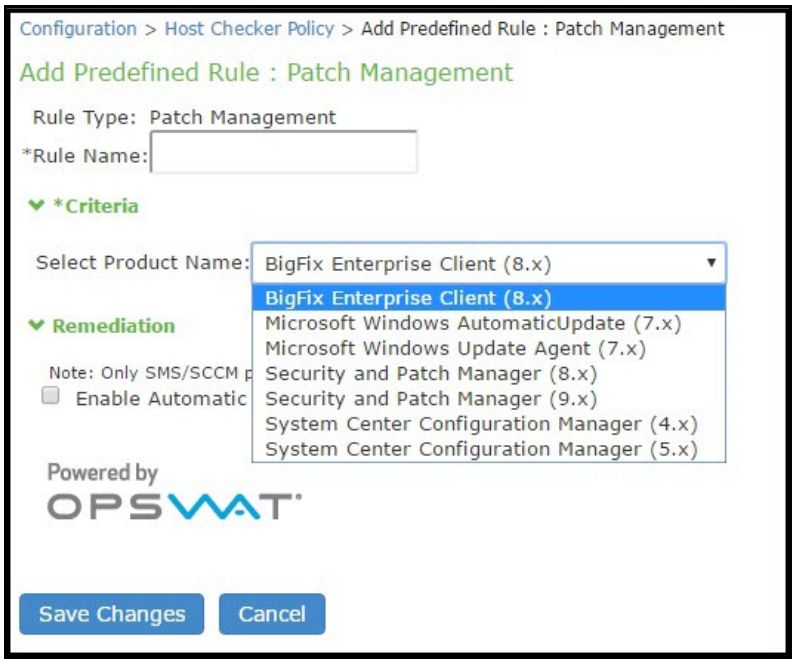
6. In the Rule Name box, enter a name for the integrity measurement rule.

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 3 shows the different product names that you can select.

Figure 3 Patch Management - Select Product Names



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.**

Configuring Predefined Common Vulnerability and Exposure (CVE) Check Rules

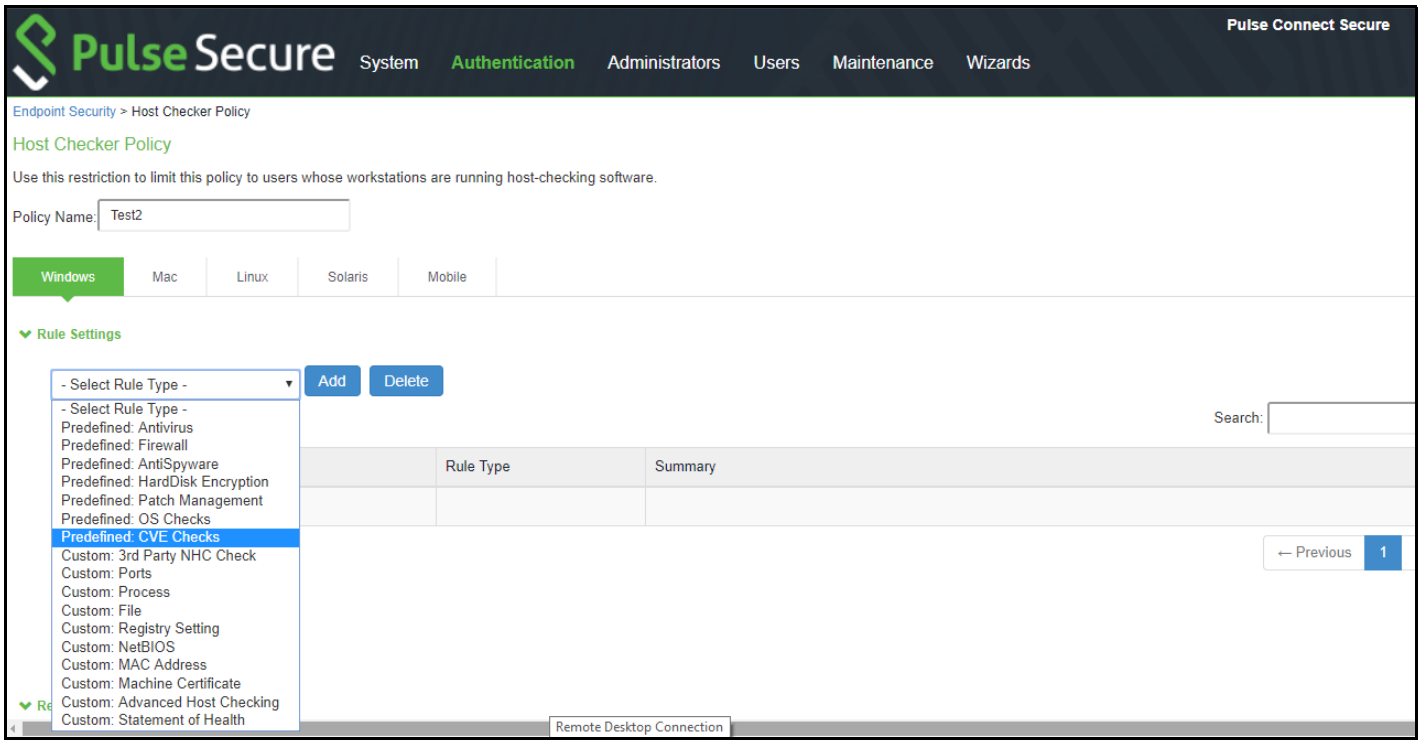
Host Checker is used for analyzing the health of the endpoint before providing access to the network. As endpoints are vulnerable to many types of new attacks such as Ransomware attack. It becomes extremely important to identify such endpoints, which are vulnerable to any attacks. The CVE lists some of these attacks along with the required software patches to prevent from such attacks. PCS provides the CVE check rule, which helps in identifying the endpoints which are vulnerable using the OPSWAT library. If the endpoint is vulnerable appropriate action is taken based on the rule configuration. For example, the user can be denied from accessing the network.

Note:

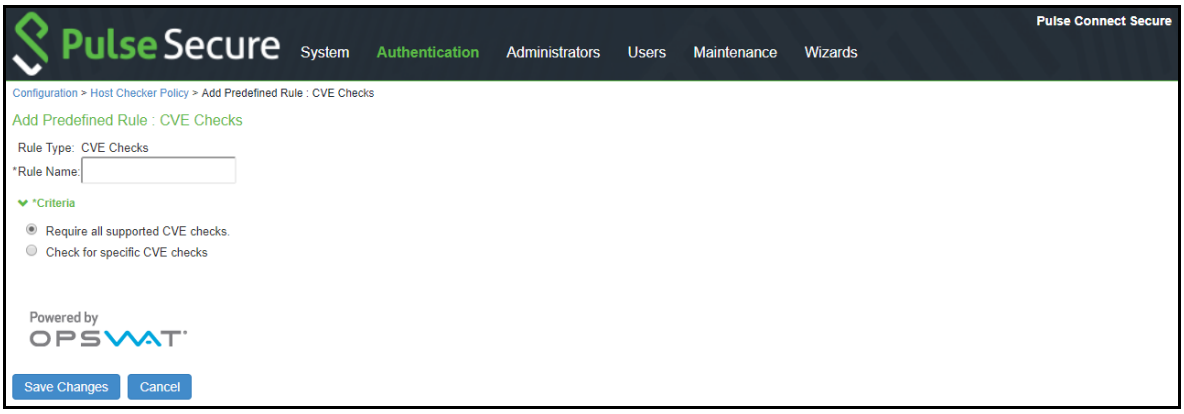
- CVE check rule is supported with active OPSWAT SDK version V4.
- OPSWAT version 3 does not support CVE rules. These rules will always be evaluated as failed and may cause the host checker policy to fail. We recommend to either delete CVE rules or use OPSWAT V4 SDK for CVE rules support.

To configure a predefined CVE check rule:

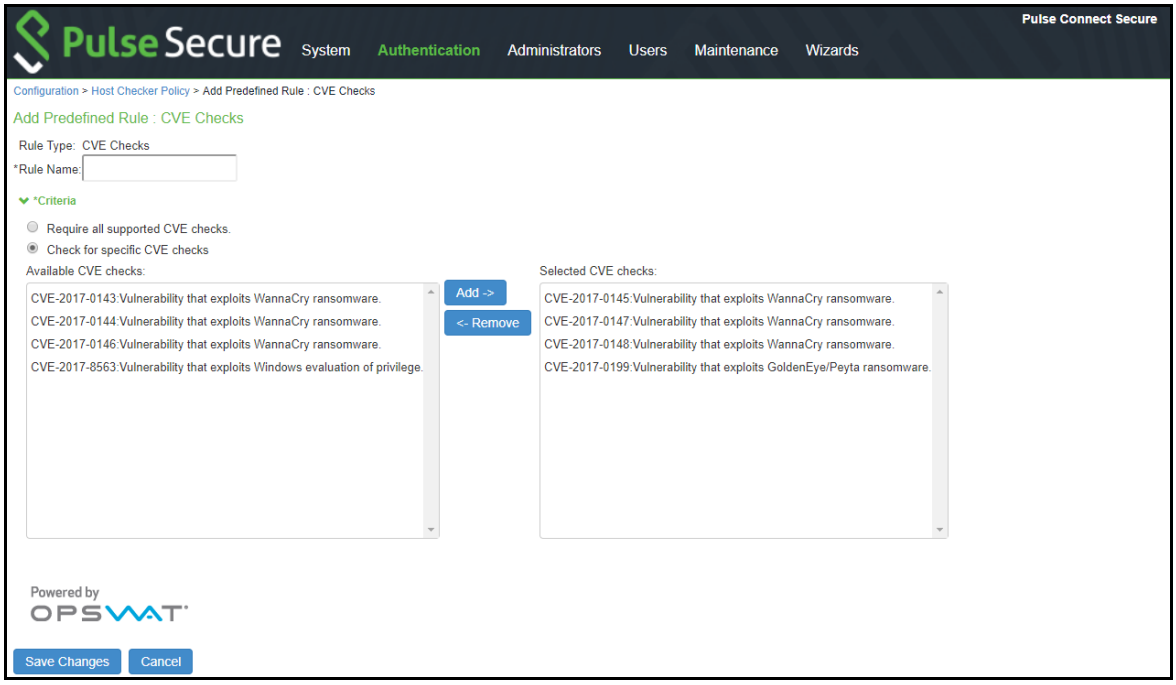
1. Select **Authentication > Endpoint Security > Host Checker.**
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Click the **Windows** tab.
4. Under Rule Settings, select **Predefined: CVE Checks** and click **Add**.



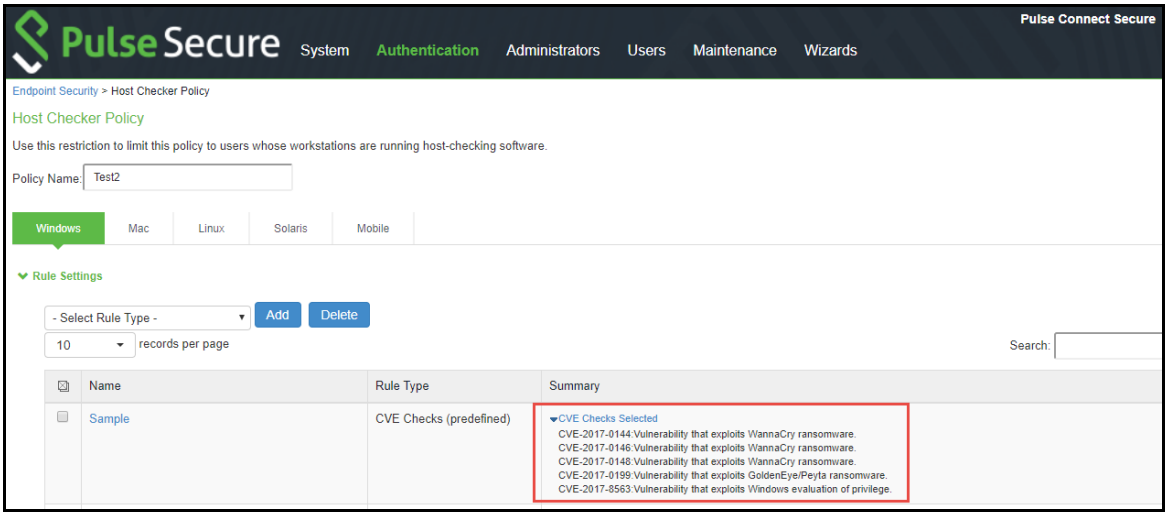
5. Enter a Rule Name for the CVE Check rule. For example, you can configure a check for WannyCry vulnerability.



6. From the Criteria, select if you require all the CVE checks from OPSWAT or choose the specific CVE checks from the available CVE checks list.



7. Click **Save Changes**.



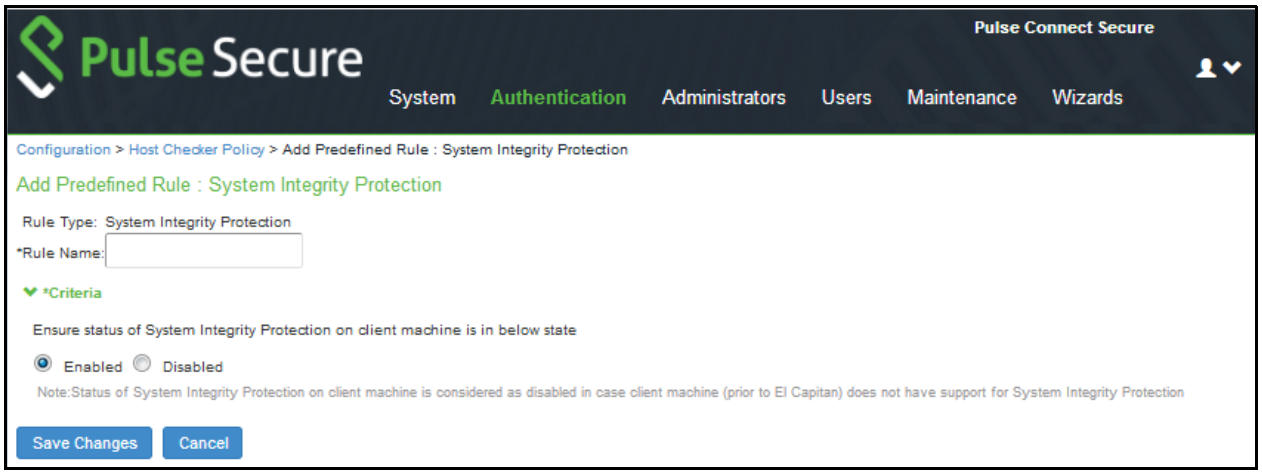
Configuring Predefined System Integrity Protection Rule

System Integrity Protection (SIP) is a security feature introduced in Mac OS X El Capitan. It provides security by restricting various actions that root user can perform on the client machine. System Integrity Protection is enabled by default but can be disabled.

PCS supports System Integrity Protection policy to check the status of System Integrity Protection (SIP) on the Mac OS endpoints. Using this, the administrators can provide different access level to the end points based on the status of "System Integrity Protection" on the client machines.

To configure a Host Checker Predefined SIP rule:

1. 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 **Mac** tab.
4. Under Rule Settings, select **Predefined: System Integrity Protection Rule** and click **Add**.



5. Enter the rule name.
6. Under Criteria, select **Enabled** to ensure that the System Integrity Protection on the client machine is enabled.
7. Click **Save Changes**.

Configuring Virus Signature Version Monitoring

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 from the vendor(s) you specify for predefined rules in a Host Checker policy.

You can automatically import the current Virus signature version monitoring lists 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 system 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 system automatically import the current virus signature version monitoring list(s) from the Pulse Secure staging site:

1. Choose **Authentication > Endpoint Security > Host Checker.**
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.pulsesecure.net/software/av/uac/epupdate_hist.xml) (for auto-update virus signatures list)
5. For Download interval, specify how often you want the system to automatically import the current list(s).
6. For Username and Password, enter your Pulse Secure Support credentials.
7. Click **Save Changes.**

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

1. Choose **Authentication > Endpoint Security > Host Checker.**
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 Pulse Secure URLs in a browser window. https://download.pulsesecure.net/software/av/uac/epupdate_hist.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 system.

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

1. Choose **Authentication > Endpoint Security > Host Checker**.
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.pulsesecure.net/software/av/uac/epupdate_hist.xml) (for auto-update virus signatures list)
5. For Download interval, specify how often you want the system to automatically import the current list(s).
6. For Username and Password, enter your Pulse Secure 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 Pulse Secure 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**.

Host Checker Statement of Health for Pulse Connect Secure

You can use the open standard Statement of Health (SoH) rule in a Host Checker policy for the Pulse for Windows client and for the Windows in-box Pulse client. SoH components evaluate an endpoint's state of health and make policy decisions for network access based on the result of the health check. To use SoH with the Windows in-box Pulse client, you must also enable the SoH functionality on the endpoint.

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 check the following system health indicators:

- Antivirus is enabled.
- Antivirus is up to date.
- Antispyware is enabled.
- Antispyware is up to date.
- Firewall is enabled.
- Automatic updating is enabled

Configuring a Statement of Health Host Checker Policy for Pulse Connect Secure

You can use the open standard Statement of Health rule in a Host Checker policy for both the Pulse for Windows client and the Windows in-box Pulse client.

To configure a Statement of Health rule in a Host Checker policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker.**
2. In the Policies section, click **New** to create a new policy, or click an existing policy.
3. For a new policy, specify a name for the policy and then click **Continue**.
4. Click the **Windows** tab. Statement of Health is available for Windows endpoints only.
5. Under Rule Settings, select **Custom: Statement of Health**, and then click **Add**.
6. Type a Rule Name for this rule.

To configure the SoH rule, you must select one or more of the Statement of Health parameters.

1. Under Criteria, enter a **Label** for the selected SoH parameter, or accept the default.
2. Select an SoH policy option from the Parameter menu, and 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 Parameter list to add additional SoH parameters.
4. (Optional) For each rule, select the **Enable automatic remediation** check box. If you select this option for a rule, the user receives a remediation message from the SoH agent, and appropriate remediation is performed, if possible. If the box is not selected, the user receives a remediation message, but no remediation action is performed.

Note: Automatic remediation works for the Pulse for Windows client only. The Windows in-box Pulse client does not support automatic remediation.

5. Click **Save Changes.**

Specifying Customized Requirements Using Custom Rules

In addition to the predefined policies and rules that come with the system, you can create custom rules within a Host Checker policy to define requirements that your users' computers must meet. Using custom rules, you can:

- 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 that certain processes are or are not running on the user's computer.
- Check 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.
- 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, Mac, 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 don't create one for Mac or Linux, users who sign into the device from a Mac or Linux machine will 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, choose the options in the following sections and click Add. The Add Custom Rule page for the rule type appears.

   - **Custom: Remote IMV** - Use this rule type to configure 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** - Use this rule type to specify the location of a custom DLL (Windows only). Host Checker calls the DLL to perform customized client-side checks. If the DLL returns a success value to Host Checker, then the system considers the rule met. In the 3rd Party NHC Check configuration page:

5. Enter a name and vendor for the 3rd Party NHC Check rule
6. Enter the location of the DLL on client machines (path and file name).
7. Click **Save Changes.**

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

   - **Ports** - Use this rule type to control the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access the device. In the Ports configuration page:

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

     Note: **Monitor this rule for change in result** for port check is applicable only for Windows and not for Linux or MAC machines.

     5. Click **Save Changes**.

   - **Process** - Use this rule type to control the software that a client may run during a session. This rule type ensures that certain processes are running or not running on the client machine before the user can access resources protected by the system. In the Processes configuration page:

1. Enter a name for the process rule.
2. 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

3. Select **Required** to require that this process is running or **Deny** to require that this process is not running.
4. Specify the MD5 checksum value of each executable file to which you want the policy to apply (optional). For example, an executable may have different MD5 checksum values on a desktop, laptop, or different operating systems. On a system with OpenSSL installed-many Macintosh, Linux and Solaris systems have OpenSSL installed by default-you can determine the MD5 checksum by using this command: openssl md5 <processFilePath>
5. Click **Save Changes**.

- **File** - Use this rule type to ensure that certain files are present or not present on the client machine before the user can access the device. You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly. In the Files configuration page:

  1. Enter a name for the file rule.
  2. Enter the name of a file (any file type), such as: c:\temp\bad-file.txt or /temp/bad-file.txt.

  You can use a wildcard character to specify the file name. For example:

  *.txt

  You can also use an environment variable to specify the directory path to the file. (You cannot use a wildcard character in the directory path.) Enclose the variable between the <% and %> characters. For example:

  <%windir%>\bad-file.txt

  3. Select **Required** to require that this file is present on the client machine or Deny to require that this file is not present.
  4. Specify the minimum version of the file (optional). For example, if you require notepad.exe to be present on the client, you can enter 5.0 in the field. Host Checker accepts version 5.0 and later, of notepad.exe.
  5. Specify the maximum age (File modified less than n days) (in days) for a file (optional). If the file is older than the specified number of days, then the client does not meet the attribute check requirement.

Note: You can use the maximum age option to check 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 may specify:

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

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

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

Note: **Monitor this rule for change in result** for port check is applicable only for Windows and not for Linux or MAC machines.

8. Click **Save Changes**.

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

  1. Enter a name for the registry setting rule.
  2. Select a root key from the drop-down list.
  3. Enter the path to the application folder for the registry subkey.
  4. Enter the name of the key's value that you want to require (optional). This name appears in the Name column of the Registry Editor.
  5. Select the key value's type (String, Binary, or DWORD) from the dropdown list (optional). This type appears in the Type column of the Registry Editor.
  6. Specify the required registry key value (optional). This information appears in the Data column of the Registry Editor.

  If the key value represents an application version, select Minimum version to allow the specified version or newer versions of the application. For example, you can use this option to specify version information for an antivirus application to make sure that the client antivirus software is current. The system uses lexical sorting to determine if the client contains the specified version and later. For example:

  3.3.3 is newer than 3.3

  4.0 is newer than 3.3

  4.0a is newer than 4.0b

  4.1 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.

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

Note: **Monitor this rule for change in result** for port check is applicable only for Windows and not for Linux or MAC machines.

You can configure registry setting remediation actions with Host Checker. 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 discrepancies to allow the client to log in.

8. Select the check box for **Set Registry value specified in criteria**.
9. Click **Save Changes**.

- **NetBIOS (Windows only, does not include Windows Phone)** - Use this rule type to check the NetBIOS name of the client machine before the user can access the device. In the NetBIOS configuration page:

  1. Enter a name for the NetBIOS rule.
  2. 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.
  3. 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.
  4. Click **Save Changes**.

- **MAC Address (Windows only)** - Use this rule type to check the MAC addresses of the client machine before the user can access the device. In the MAC Address configuration page:

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

  00:0e:1b:04:40:29

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

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

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

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

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

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

- **Machine Certificate (Windows only)** - Use this rule type to check that the client machine is permitted access by validating the machine certificate stored on the client machine. In the Machine Certificate configuration page:
  1. Enter a name for the machine certificate rule.
  2. From the Select Issuer Certificate list, select the certificate that you want to retrieve from the user's machine and validate. Or, select Any Certificate to skip the issuer check and only validate the machine certificate based on the optional criteria that you specify below.
  3. From the Optional fields (Certificate field and Expected value), specify any additional criteria that Host Checker should use when verifying the machine certificate.
  4. Click **Save Change**s.

Note: If more than one certificate is installed on the client machine that matches the specified criteria, The Host Checker client passes the first certificate it finds to the system for validation.

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

Using a Wildcard or Environment Variable in a Host Checker Rule

You can use the following wildcards 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

Wildcard Character	Description	Example
*	Matches any character	*.txt
?	Matches exactly one character	app-?.exe

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

Environment variable	Example Windows Value
<%APPDATA%>	C:\Documents and Settings\jdoe\Application Data
<%windir%>	C:\WINDOWS
<%ProgramFiles%>	C:\Program Files
<%CommonProgramFiles%>	C:\Program Files\Common Files
<%USERPROFILE%>	C:\Documents and Settings\jdoe
<%HOMEDRIVE%>	C:
<%Temp%>	C:\Documents and Settings \<username>\Local Settings\Temp

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

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

Environment variable	Example Linux and Solaris Values
<%java.home%>	/local/local/java/j2sdk1.4.1_02/jre
<%java.io.tmpdir%>	/tmp
<%user.dir%>	/home-shared/cknouse
<%user.home%>	/home/cknouse

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

Table 6 Environment Variables for Specifying a Directory Path on Macintosh

Environment variable	Example Macintosh Value
<%HOME%>	/Users/admin where admin is the logged in username
<%USER%>	Maps to the login name of the MAC machine

Note: Although environment variables are formatted in the same way as Toolkit Template directives, they are not interchangeable and you should not confuse them.

Configuring Patch Management Policies

You can configure, Hostchecker policies that checks for patch management software installed on the client machines. Customers need to have their own patch management solution. Administrator is given option to configure the patch management software that needs to be verified on the endpoint.

On the client machine, Patch management software detects patch status based on the configured rules on corresponding patch management server. Detection of patches status on the client machine depends on the support provided by the 3rd party patch management solution that customer is using Hence different patch management software on the same client can report the status differently. To avoid conflicts, administrator is allowed to configure only one patch management software product on policy configuration page.

Patch remediation support is provided only using Microsoft's SMS/SCCM clients.

Note: In non-English installations, the English version of local patches is displayed.

Note: The patch management policy cannot be used in L2 case with some products when they require internet connectivity to get the latest patch status.

Using Microsoft System Management Server or Microsoft System Center Configuration Manager (SMS/SCCM)

For Windows clients, you can use Microsoft System Management Server or Microsoft System Center Configuration Manager (SMS/SCCM) to provide a method for automatic updates to non-compliant software.

Using the SMS/SCCM remediation feature, you can force the client to initiate the software update immediately after the Patch Management check.

To have SMS/SCCM update the client when notified, set the advertisement time on the SMS/SCCM to As soon as possible.

- The Patch Management policy specifies the required software.
- When an endpoint attempts to authenticate, Host Checker evaluates the client and sends the results obtained from the patch management software back to the system.
- The system evaluates the results and sends reason strings and remediation information to the client .and initiates remediation action if enabled.
- If the endpoint has SMS/SCCM client, the SMS/SCCM client queries the SMS/SCCM server for software advertisements.
- The server identifies what patches should be advertised to the client. This information is configured on the server, Host Checker does not interact with the server.
- The SMS/SCCM client receives the advertisement and applies the required patch(es).

You assign clients to a particular group or collection on the server, then SMS/SCCM can advertise patches for that collection. You can configure roles that correspond to collections, and SMS/SCCM can send the appropriate patches for a particular role.

You must have the SMS/SCCM client installed and configured correctly on endpoints, and the SMS/SCCM server must be reachable. In a Layer 2 network, Host Checker is performed before the endpoint is connected to the network. Host Checker can obtain the IP address of the SMS/SCCM server configured for the client. If the endpoint is out of compliance and remediation is necessary, Host Checker pings the server IP address every 15 seconds until the server can be notified to update the client.

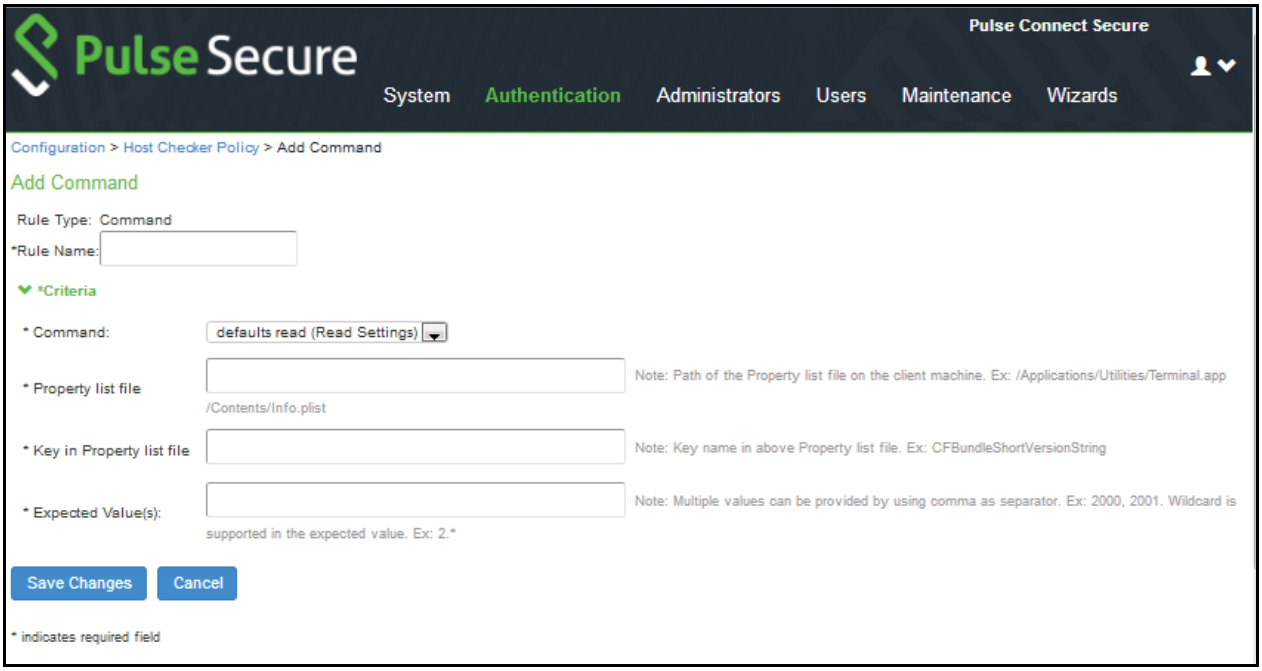
It is important as an administrator to inform users of the expected behavior if this feature is enabled, as there is no notification to the user until SMS sends back the advertisement.

Configuring Custom Command Rule

Command rule enables administrators to check for the versions of the installed applications on the Mac OS endpoints.

To configure a Host Checker: Custom Command rule:

1. 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 **Mac** tab.
4. Under Rule Settings, select **Custom: Command** and click **Add**.



5. Enter the rule name.
6. Under Criteria, complete the following configuration:
   - Select the command type as default read (Read Settings)
   - Specify the path of the property list file of the required application on the client machine.
   - Enter the key name used in the property list file for obtaining the version of the application.

- Enter the expected version that needs to be present on the client machine

7. Click **Save Changes**.

Note: Ensure that the required ESAP package (which has support for Command Rule) is installed and activated on the server.

Configuring Custom Advanced Host Checking Rule

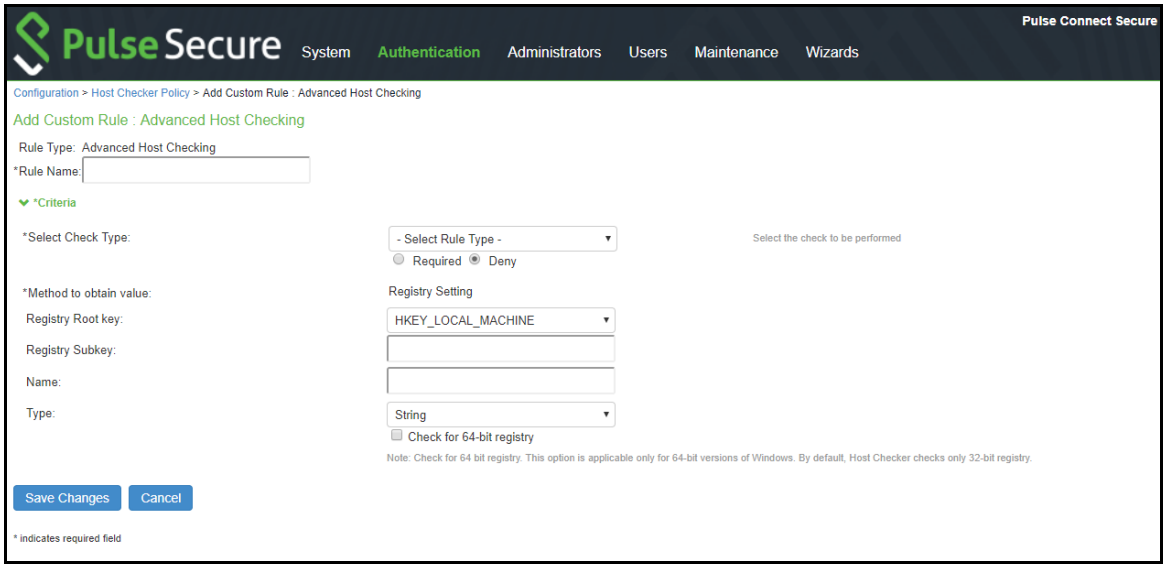
Note: Use this rule type to combine multiple policies for performing advanced host checking. The supported policy types are ports, process, file, registry setting, NETBIOS, MAC address and machine certificate. It allows Administrator to dynamically configure the expected values from registry locations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

Note: This feature is supported only on Windows platform.

To configure an advanced host checking rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Under Rule Settings, select **Custom: Advanced Host Checking** and then click **Add**.
4. Enter a name for the rule.
5. Select the check to be performed from the Rule Type list.

Figure 4 Advanced HC Rule



6. Under Criteria, **Select Rule Type** list.

a. Select **Ports** to check whether a specific port number is opened or closed on the endpoint.

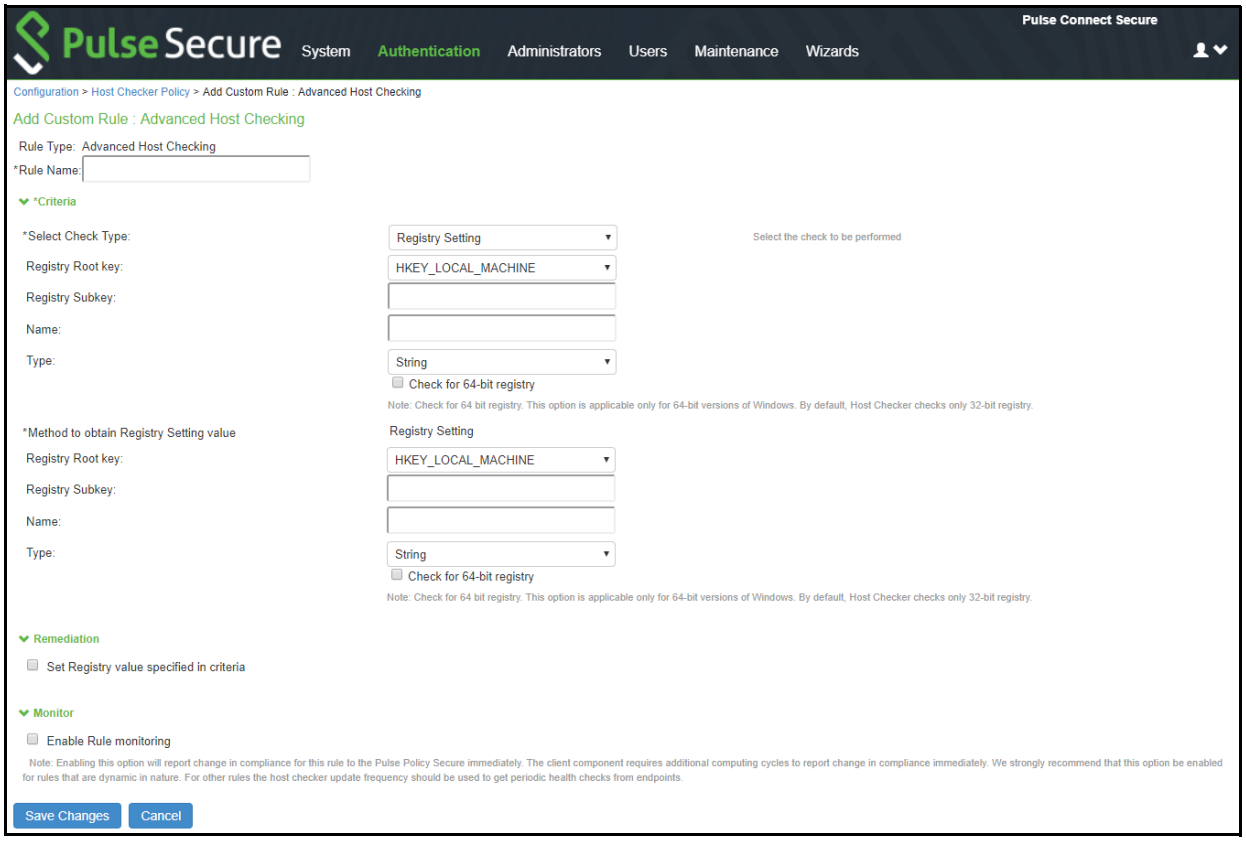
   1. Enable R**equired/Deny** to check if the specified port is open/closed.
   2. Select the registry root key- HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, or HKEY_CLASSES_ROOT.
   3. Enter the registry subkey.
   4. Enter the name of the registry.
   5. Select the type of the registry- String, Binary, or DWORD.
   6. Select **Check for 64-bit registry** to check the 64-bit registry on Windows. The default is 32-bit registry

Note: You can similarly add the check type for Process/File/NETBIOS/MAC Address. The port number/process name/file path/NETBIOS name/MAC address is obtained from the Registry setting. Advanced Host Check- Ports

b. Select Registry Setting to verify the specific registry values on the endpoint. You can define only the registry location in the policy and define another registry location, which provides the expected registry value.

1. Select the registry root key- HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, or HKEY_CLASSES_ROOT.
2. Enter the registry subkey.
3. Enter the name.
4. Select the type of the registry- String, Binary, or DWORD.
5. Configure another registry setting to fetch the expected registry value. Select the registry subkey, name, and type.

Figure 5 Advanced Host Check- Registry Setting



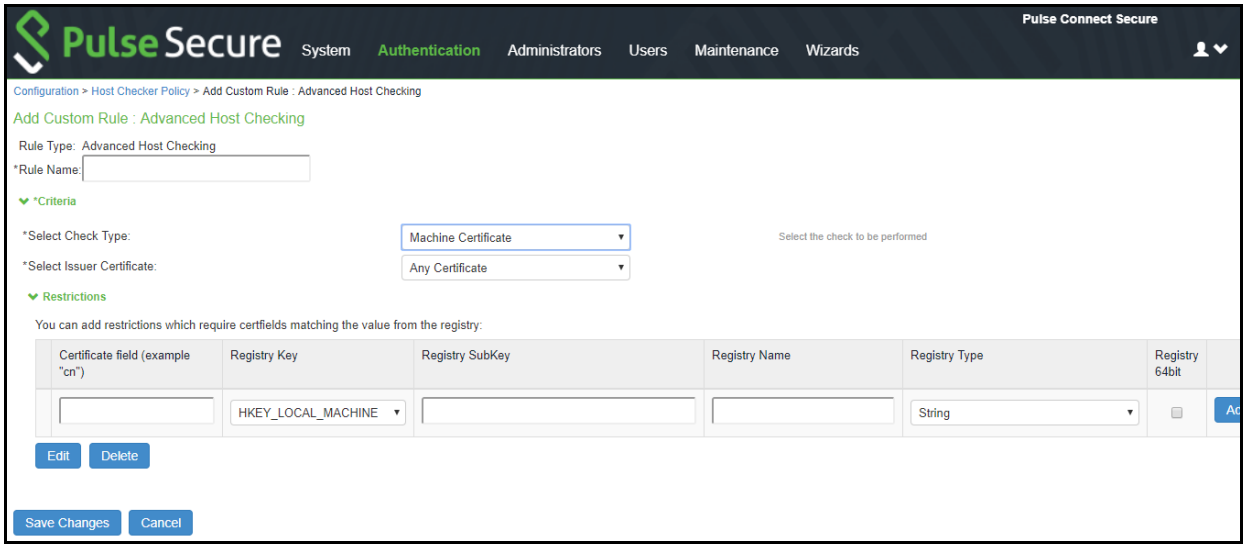
c. Select **Machine Certificate** to verify the required certificate is installed on the client machine certificate store.

1. Select the issuer certificate from the list.
2. Specify any additional criteria that Host Checker must use while verifying the certificate.

- Enter the certificate field name. For example, cn.
- Select the registry key.
- Enter the registry subkey.
- Enter the registry name.
- Select the registry type.

- Click **Add**.

Figure 6 Advanced Host Check- Machine Certificate



7. Click **Save Changes**.

Using Third-party Integrity Measurement Verifiers

The Trusted Network Connect (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 TNC-client (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.

Connect 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 the system can communicate with it.
3. Implement the Host Checker policy.

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 the system 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 the system about Host Checker failure.

During this step, you install third-party IMVs. Third-party IMVs are installed on the remote IMV server, not on the device.

During this step, 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 the device. The system then authenticates with the remote IMV server through the certificate. If you do not have a certificate authority, install and use OpenSSL to generate a CA certificate.

To install, configure, and implement the server software:

1. In the system admin console, choose **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 hostname 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 encrypted with a password.

   If you do not have a certificate authority, you can use the following steps to create a CA and then create a server certificate for the remote IMV server.

Note:

- Install the full version of OpenSSL. The "light" version of OpenSSL will not work.

Follow the steps below to set up OpenSSL:

1. Download and install OpenSSL from this site: http://www.slproweb.com/products/Win32OpenSSL.html
2. At the Windows command prompt, type the following commands:

   cd \openssl

   md certs

   cd certs

   md demoCA

   md demoCA\newcerts

   edit demoCA\index.txt
3. Press the **ALT-F** keys and then the **S** key to save the file.
4. Press the **ALT-F** keys and then the **X** key to exit the editor.
5. At the Windows command prompt, type the following commands:

edit demoCA\serial

6. Type the following in the document window: **01**
7. Press the **ALT-F** keys and then the **S** key to save the file.
8. Press the **ALT-F** keys and then the **X** key to exit the editor.
9. At the Windows command prompt, type the following commands:

   set path=c:\openssl\bin;%path%

Follow the steps below to create a CA key:

1. To create a CA key, type the following command at the Windows command prompt in the c:\openssl\certs directory:

   openssl genrsa -out ca.key 1024

   The following output should appear:

   Loading 'screen' into random state - done

   Generating RSA private key, 1024 bit long modulus

   .....++++++

   .++++++

   e is 65537 (0x10001

Follow the steps below to create a CA Certificate:

1. 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

2. Enter the appropriate Distinguished Name (DN) information for the CA certificate. You can leave some fields blank by entering a period.

   For example:

   Country Name: US

   State or Province Name: CA

   Locality Name: Sunnyvale

   Organization Name: XYZ

   Org. Unit Name: IT

   Common Name: ic.xyz.com

   Email Address: user@xyz.com

3. To set up the CA, type the following command at the Windows command prompt in the directory c:\openssl\certs:

   copy ca.key demoCA

notepad demoCA.cnf

4. When prompted to create a new file, press the yes button.
5. Type the following lines in the document, pressing the Enter key at the end of each line.

   [ca]
   default_ca = demoCA
   [demoCA]
   dir = ./demoCA
   database = $dir/index.txt
   new_certs_dir = $dir/newcerts
   certificate = $dir/cacert.pem
   serial = $dir/serial
   private_key = $dir/ca.key
   default_days = 365
   default_md = md5
   policy = policy_any
   email_in_dn = no
   name_opt = ca_default
   name_opt = ca_default
   copy_extensions = none
   [policy_any]
   countryName = supplied
   stateOrProvinceName = optional
   organizationName = optional
   organizationalUnitName = optional
   commonName = supplied
   emailAddress = optional
6. Save the file and close notepad.
7. Type the following command to generate an RSA private key for the remote IMV server:

   openssl genrsa -out rimvs_key.pem 1024
8. Type the following command to generate a CSR for the remote IMV server:

   openssl req -new -key rimvs_key.pem -out rimvs_csr.pem
9. Type the following lines:

   Country Name:

State or Province Name:

Locality Name:

Organization Name:

Organizational Unit Name:

Common Name: [IPAddress]

Email Address:

A challenge password:

An optional company name:

You may enter any value you like for most fields, but the Common Name field must contain the IP address of the machine running the remote IMV server. This machine should have a static IP address.

10. Type the following command to generate a certificate for the remote IMV server:

    openssl ca -config demoCA.cnf -in rimvs_csr.pem -out rimvs_cert.pem

11. 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 demoCA.cnf file, or use the - days parameter to the openssl ca command to specify a different lifetime.

12. Type the following command to place the remote IMV server key and certificate in a PKCS#12 file (substitute your password):

    openssl pkcs12 -export -in rimvs_cert.pem -inkey rimvs_key.pem -passout pass:<password>-out rimvs_p12.pem

13. On the remote IMV server, choose **Programs > Pulse Secure > Remote IMV Server > Remote IMV Server Configurator** from the Start menu.

14. Under Client Info, click **Add**.

15. Configure the port to service SOAP requests.

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

17. Change logging settings if you choose (log is generated in the install directory).

18. Browse and find the PKCS#12 file you generated in the filesystem.

19. Specify the password associated with the certificate.

20. In the Connect Secure admin console, use 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).

21. Click **Import Trusted Server CA** and browse for the server certificate used on the remote IMV server.

22. Add the new remote IMV server:

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

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

    b. Under Remote IMV, click **New Server.**

    c. In the New Server page:

        1. Create a label for the server using the **Name** and (optional) Description fields.
        2. In the Hostname field, enter either the IP address or hostname as defined in the server certificate.
        3. In the Port field, enter the unique port number the system 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.
        4. In the **Shared Secret** field, enter the same shared secret used in the client information entry on the remote IMV server.
        5. Click **Save Changes**.

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

    e. In the New IMV page:

        1. Create a label for the IMV using the **Name** and (optional) **Description** fields.
        2. 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.
        3. From the Primary Server pop-up menu, select the remote IMV server where this IMV is installed.
        4. (Optional) From the Secondary Server pop-up 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.
           The system 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.
        5. Click **Save Changes**.

    f. Click **Save Changes**.

Implementing the 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 through the Authentication > Endpoint Security > Host Checker page of the admin console, 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.**
2. Under Policies, click **New**.
3. Enter a name in the **Policy Name** field and then click Continue. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
4. Under Rule Settings, choose Custom: **Remote IMV** and click **Add**.
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 be associated with this rule.
   c. Click **Save Changes**.
6. Specify how Host Checker should 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.

Implementing Host Checker Policies

After you create global policies through the Authentication > Endpoint Security > Host Checker page of the admin console, you can restrict the system and resource access by requiring Host Checker in a:

- **Realm authentication policy-**When administrators or users try to sign in to the device or launch a Virtual Workspace session, the system evaluates the specified realm's authentication policy to determine if the pre-authentication 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 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 user's computer does not meet the requirements, the system denies access to the user unless you configure remediation actions to help the user bring his computer into compliance. You can configure realm-level restrictions through the Administrators > Admin Realms > SelectRealm > Authentication Policy > Host Checker page or the Users > User Realms > SelectRealm > Authentication Policy > Host Checker page of the admin console.
  - **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 if the role requires that the user's computer adheres to certain Host Checker policies. If it does and the user's 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 his 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 through the Administrators > Admin Roles > SelectRole > General > Restrictions > Host Checker page of the admin console or the Users > User Roles> SelectRole > General > Restrictions > Host Checker page. If you have enabled Advanced Endpoint Defense Malware Protection, you can select to implement this feature for any role.

- **Resource policy**-When a user requests a resource, the system evaluates the resource policy's detailed rules to determine if the resource requires that the user's computer adheres to certain Host Checker policies. The system denies access to the resource if the user's computer does not follow the specified Host Checker policies unless you configure remediation actions to help the user bring his computer into compliance. To implement Host Checker restrictions at the resource policy level, use settings in the Users > Resource Policies > SelectResource > SelectPolicy > Detailed Rules page.

  You may specify that the system evaluate your Host Checker policies only when the user first tries to access the realm, role, or resource that references the Host Checker policy. Or, you may specify that the system periodically re-evaluate the policies throughout the user's session. If you choose to periodically evaluate Host Checker policies, the system dynamically maps users to roles and allows users access to new resources based on the most recent evaluation.

Executing Host Checker Policies

When the user tries to access the system, Host Checker evaluates its policies in the following order:

1. Initial evaluation-When a user first tries to access the system sign-in page, Host Checker performs an initial evaluation. Using the rules you specify in your policies, Host Checker verifies that the client meets your endpoint requirements and returns its results to the system. Host Checker performs an initial evaluation regardless of whether you have implemented Host Checker policies at the realm, role, or resource policy level.
   If the user navigates away from the system sign-in page after Host Checker starts running but before signing in, Host Checker continues to run on the user's machine until the Host Checker process times out.
   If the system does not receive a result from Host Checker for any reason (including because the user manually terminated Host Checker), it displays an error and directs the user back to the sign-in page. Otherwise, if the Host Checker process returns a result, the system goes on to evaluate 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 may access. Then, the system displays or hides realms from the, only allowing the user to sign 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 any of the available realms, the system does not display the sign-in page. Instead, it displays an error stating the user has no access unless you have configured remediation actions to help the user bring the endpoint into compliance.
   Note that Host Checker only performs realm-level checks when the user first signs in. If the state of the user's system changes during his session, the system does not remove him from the current realm or allow him access to a new realm based on his new system state.

3. Role-level policies-After the user signs into a realm, the system evaluates role-level policies and maps the user to the role or roles if he meets the Host Checker requirements for those role(s). Then, the system displays the homepage to the user and enables those options that the mapped role(s) allow.
   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's session unless you have configured remediation actions to help the user bring the endpoint into compliance.

4. Resource-level policies-After allowing the user to access the homepage, the user may try to access a resource that is controlled by a resource policy. When he does, the system determines whether or not to perform the action specified in the resource policy based on the last status returned by Host Checker.
   If Host Checker returns a different status during a periodic evaluation, the new status only impacts new resources that the user tries to access. For example, if the user successfully initiates a VPN Tunneling session and then fails his next resource-level host check, he may continue to access the open VPN Tunneling session. The system only denies him access if he tries to open a new VPN Tunneling session. The system checks the last status returned by Host Checker whenever the user tries to access a new Web resource or open a new Secure Application Manager, VPN Tunneling, or Secure Terminal Access session.
   With either a success or fail result, Host Checker remains on the client. Windows users may manually uninstall the agent by running uninstall.exe in the directory where Host Checker is installed. If you enable client-side logging through the System > Log/Monitoring > Client Logs page, this directory also contains a log file, which the system rewrites each time Host Checker runs.
   If you enable dynamic policy evaluation for Host Checker, the system evaluates resource policies implemented at the realm level whenever a user's Host Checker status changes. If you do not enable dynamic policy evaluation for Host Checker, it does not evaluate resource policies but it does evaluate the authentication policy, role mapping rules, and role restrictions whenever a user's Host Checker status changes.

Configuring Host Checker Restrictions

To specify Host Checker restrictions:

1. Navigate to: **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, a role mapping rule, or a resource policy.

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

   a. Navigate to:

   - Administrators > Admin Realms > *Select Realm* > General > Restrictions > Host Checker.
   - Users > User Realms > *Select Realm* > General > Restrictions > Host Checker.

   b. Choose one of the following options for either all available policies or for individual policies listed in the Available Policies column:

   - **Evaluate Policies-**Evaluates without enforcing the policy on the client and allows user-access. This option does not require Host Checker to be installed during the evaluation process; however, Host Checker is installed once the user signs in to the system.

- **Require and Enforce-**Requires and enforces the policy on the client in order for the user to log in to the specified realm. Requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement. This option requires the system to download Host Checker to the client machine. 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 if he meets the requirements of any one of the selected Host Checker policies. Note that Cache Cleaner policies are not part of the "requirement" decision process. Users can access the realm as long as they meet the other requirements regardless of whether they meet the Cache Cleaner policy.

3. If you want to implement Host Checker at the role level:

   a. Navigate to:

      - **Administrators > Admin Roles > Select Role > General > Restrictions > Host Checker**.
      - **Users > User Roles > Select Role > General > Restrictions > Host Checker.**

   b. Choose one of the following options:

      - **Allow all users** - Does not require Host Checker to be installed in order for the user to meet the access requirement.
      - **Allow only users whose workstations meet the requirements specified by these Host Checker policies** - Requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement.
      - **Select the Allow access to role if any ONE of the selected "Require and Enforce" policies** is passed check box if you do not want to require users to meet all of the requirements in all of the selected policies. Instead, the user can access the role if he meets the requirements of any one of the selected Host Checker policies.

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

   a. Navigate to: **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 to map users to when they meet the requirements specified in the custom expression and click **Add**.

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

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

a. Navigate to: U**sers > Resource Policies > Select Resource > Select Policy > Detailed Rules**.

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

c. Write a custom expression for the detailed rule to evaluate Host Checker's status using the hostCheckerPolicy variable.
These options allow you to control which version of an application or service runs on client machines.

Remediating Host Checker Policies

You can specify general remediation actions that you want 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 choose to include a message to users (called a reason string) that is returned by Host Checker or an integrity measurement verifier (IMV) and explains why the client machine does not meet the Host Checker policy requirements.

For example, the user may 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. Please follow the instructions below to fix these problems. When you are done click Try Again. If you choose to Continue without fixing these problems, you may not have access to all of your intranet servers.

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, 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. 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 IMV. On Windows, you can also call the HCIF_Module.Remediate () API function as part of a third-party J.E.D.I. DLL. Host Checker does not inform users when performing automatic actions. (You could, however, include information in your custom instructions about the automatic actions.)

General Host Checker Remediation User Experience

Users may see the remediation page in the following situations:

- Before the user signs in:

- If you enable custom instructions for a policy that fails, the system displays the remediation page to the user. The user has two choices:
  - Take the appropriate actions to make the endpoint conform to the policy and then click the Try Again button 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 the Continue button 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 for a policy that fails, Host Checker does not display the remediation page to the user. Instead, the system displays the sign-in page but does not allow the user to access any realms, roles, or resources that have a failed Host Checker policy.

- After the user signs in:
  - (Windows only) During a session, if a user's Windows computer becomes non-compliant with the requirements of a Host Checker policy, an icon appears in the system tray along with a pop-up message that informs the user of the non-compliance. The user can then click the pop-up message to display the remediation page.
  - (Macintosh or Linux) During a session, if a user's Macintosh or Linux computer becomes non-compliant with the requirements of a Host Checker policy, the system displays the remediation page to inform the user of the non-compliance.

Note: If the user hides the remediation page by setting a user preference, he may only continue using the secure gateway if you configure other realms and roles that do not enforce a Host Checker policy.

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 that you want Host Checker to perform if a user's computer does not meet the requirements of the current policy:
   - **Enable Custom Instructions**-Enter the instructions you want to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and add links to resources such as policy servers or web sites: <i>, <b>,
, <font>, and <a href>. For example:
     You do not have the latest signature files.
     Click here to download the latest signature files.

Note: For Windows clients, if you include in the instructions a link to a system-protected policy server, define a pre-authentication access tunnel.

- **Enable Custom Actions-**You can select one or more alternate policies that you want Host Checker to evaluate if the user's computer does not meet the current policy requirements. The alternate policy must be a third-party policy that uses a J.E.D.I. package. For example, you can use a J.E.D.I. package to launch an application if the user's computer does not meet the current policy requirements. Select the alternate policy in the HC Policies list and then click Add.

- **Remediate-**(Third party DLLs only) You can select this option to perform remediation actions specified by means of the Remediate () API function in a third-party J.E.D.I. DLL.

Note: The Remediate feature is primarily provided for backwards compatibility. We recommend that you use IMCs and IMVs instead.

- **Kill Processes**-On each line, enter the name of one or more processes you want to kill if the user's 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 you want to delete if the user's computer does not meet the policy requirements. (You cannot use wildcards in the file name.) Enter one file name 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 integrity measurement verifier (IMV) and explains why the client machine does not meet the Host Checker policy requirements. This option applies to predefined rules, 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**.

Store and Reuse Host Checker Policy Results

The Host Checker configuration page enables you to store and reuse the host checker evaluation results. The admin can configure the time interval in days for not performing the host check on the endpoint. When the user connects for the first time the Host Checker runs and the results are saved in PPS. However, for the subsequent logins from the same endpoint, the host checking is not performed and the saved host check result is reused till the expiration of the admin defined time interval.

The first connection from the endpoint never reuses the cached results. The subsequent logins from the same endpoint uses the cached host checker results.

This feature saves the Host Check results for clients connecting from Windows and Mac desktop operating systems. This feature helps in providing faster connection or access to the network.

The Host Checker saved/cached results will be cleared in the following scenarios:

- Change in HC policy configuration such as addition, deletion and modifications.
- Change in Active ESAP version.
- Change in HC configuration such as periodic interval, disabling the caching feature and role configuration under caching feature.

- Server reboot.

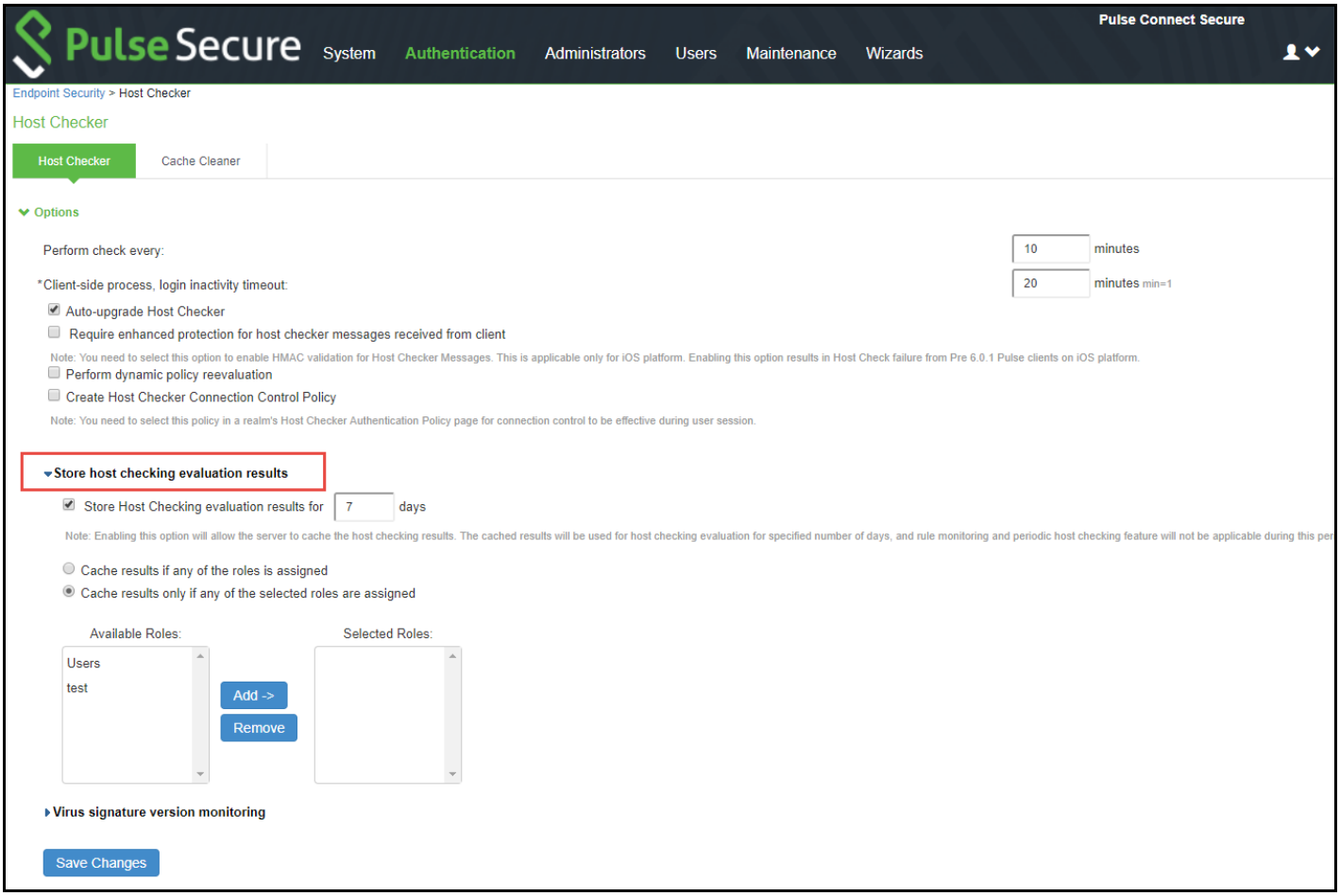
Limitations

- Periodic host checking, rule monitoring, and remediation are supported only for the first connection when the results are not cached.
- Change in Compliance status of the device is not detected if cached results are used for the connection.

To configure caching on Host Checker:

1. Select **Authentication > Endpoint Security > Host Checke**r.
2. Under Options, Store host checking evaluation results enable Store Host Checking evaluation results and enter the number of days for not performing the Host Check. The default number of days for storing HC results is 7 days. The supported range is between 1- 30 days.
3. The Admin can also choose to cache results based on the roles assigned:
   - **Any role is assigned** - If you select this option, the HC results are cached irrespective of the role assigned.
   - **Any of the selected roles is assigned** - If you select this option, the HC results are cached only when the selected role is assigned.

Note: It is recommended to not enable caching for remediation roles because the subsequent logins will be in the remediation role as cached results are used.



4. Click Save Changes.

Using Endpoint Security Assessment Plug-In

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

Pulse Secure frequently adds enhancements, bug fixes, and support for new third-party applications to the plug-in. 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 upgrading the system software package.

You can upload up to four versions of the plug-in to your system, but it uses only one version at a time (called the active version). If necessary, you can roll back to a previously active version of the plug-in.

Upgrading the Endpoint Security Assessment Plug-In

To upgrade the Endpoint Security Assessment Plug-in:

1. Download the Endpoint Security Assessment Plug-in from the Pulse Secure Global Support Center (PSGSC) Center to your computer:
   a. Open the following page: http://www.pulsesecure.net/support
   b. Click the **Software** tab.
   c. Navigate to the **ESAP release** you want and click the link to download the package file to your computer.
2. Select **Authentication > Endpoint Security > Host Checker**.
3. At the bottom of the Host Checker page under Manage Endpoint Security Assessment Plug-In Versions:
4. If you have 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**.
5. If you want the system to actively begin using the new component software immediately after you upload it, select the Set as active after upload option.
6. Click Browse, select the plug-in file you want to upload to the system, and click **OK**.
7. Click Upload. While the system uploads and decrypts the plugin .zip file, the message "Loading" appears in the plug-in list under Manage Endpoint Security Assessment Plug-In Versions. If the device 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 appears in the plug-in list.
8. If you did not select the Set as active after upload option, activate the plug-in you want to use by selecting the version in the plug-in list and clicking **Activate**.

Note:

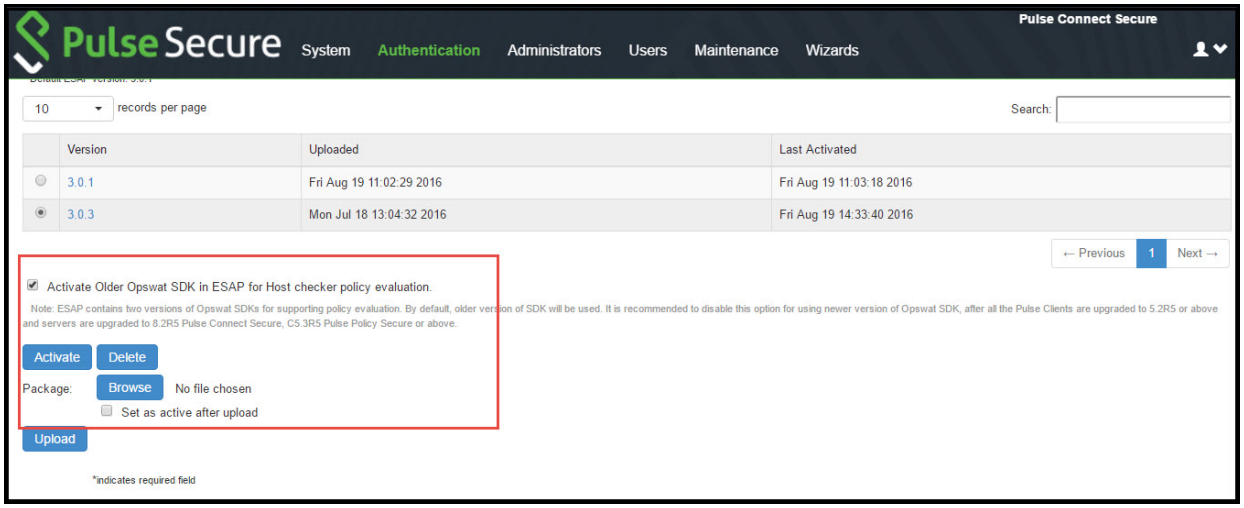
- If you attempt to activate a version of the plug-in that does not support all of the predefined rules already configured in all Host Checker policies, the system does not allow activation of that plug-in version. For example, if a Host Checker policy is configured to use a predefined rule to check for a version of antivirus software, and you attempt to activate a plug-in version that does not support that particular 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 plug-in version, click the plug-in's version number under Manage Endpoint Security Assessment Plug-In Versions.
- You can roll back to an older plug-in version after upgrading to a later version by selecting the older version as the active version. But, if you modified any Host Checker policies after upgrading to the later version, the rollback may 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 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 upgrading 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, it automatically deletes the oldest plug-in version and installs, but does not activate, the plug-in included with the new system software.

Activating the OPSWAT SDK Version

Beginning with Release 8.2R5, Pulse Policy Secure supports both v3 and v4 SDKs provided by OPSWAT. The default SDK version used is v3, but it can be reconfigured based on your requirement. The product/vendor names used by v3 and v4 SDK might differ. Due to the product/vendor names mismatch, there is a possibility that the rules become empty while creating Host Checker rule with v3 SDK activated and upon enabling v4 SDK. To avoid this, a migration page is added to help the administrators in migrating the policies from v3 to v4 SDK. To use v3 or v4 SDK:

1. Select **Authentication > Endpoint Security > Host Checke**r.
2. Select the **Activate Older SDK in ESAP for Host Checker policy evaluation** check box for v3 SDK.
3. Clear the **Activate Older SDK in ESAP for Host Checker policy evaluation** check box for v4 SDK.

Figure 7 Activating SDK

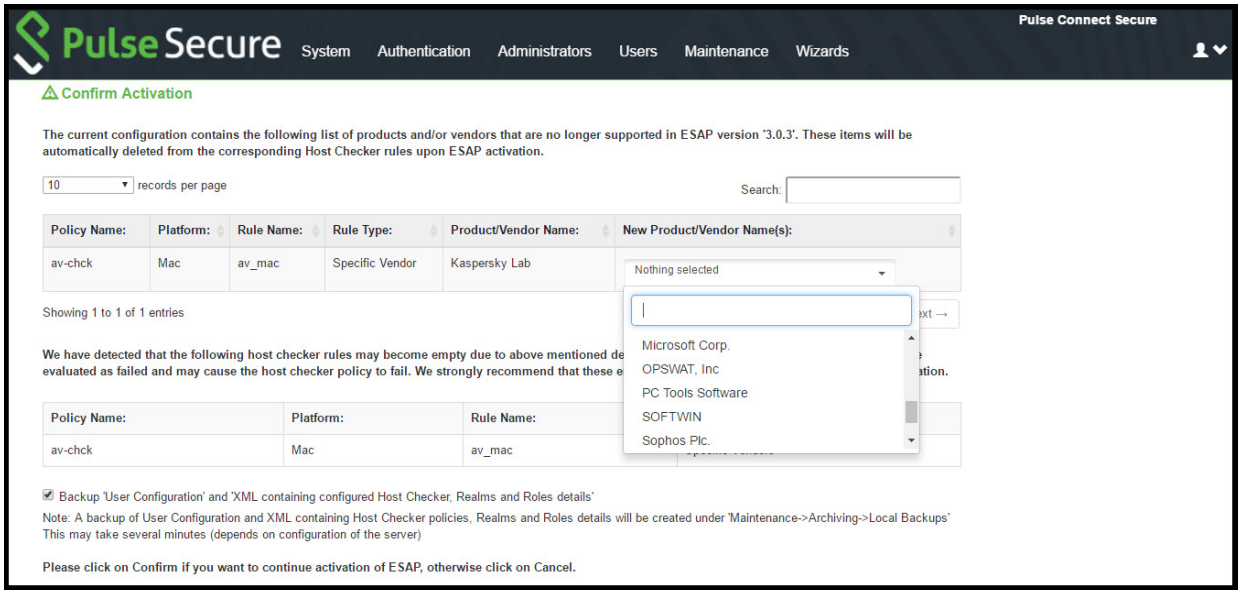


Note:

- It is recommended to disable this option for using newer version of OPSWAT SDK, after all the Pulse Clients are upgraded to 5.2R5 or above and servers are upgraded to PCS 8.2R5 or above.

4. Click **Activate**. A confirm Activation page appears which lists the products and/or vendors, which are no longer supported in that particular ESAP SDK version. From the drop-down list, admin can select one or many new products/vendors instead of the existing product/vendor.

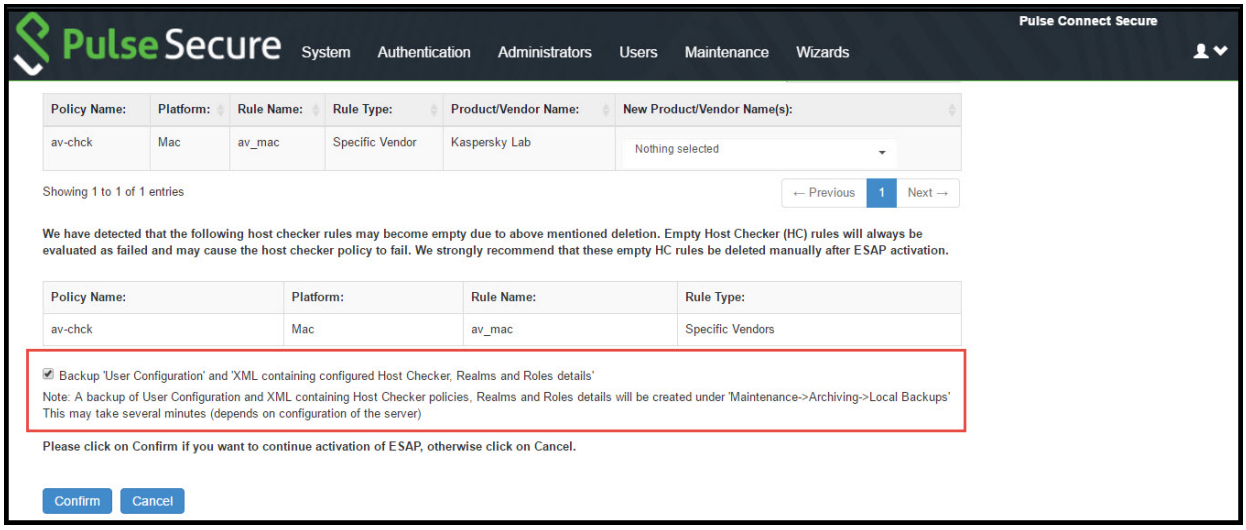
Figure 8 ESAP Activation



Note: Only the products/vendors, which gets changed are listed. If some rules have some products/vendors whose names are not changed, it will be automatically migrated and will not be listed.

5. Select **Backup 'User Configuration' and 'XML containing configured Host Checker, Realms and Roles** details to create a local backup of user configurations under Maintenance > Archiving > Local Backups.

Figure 9 Backup User Configuration



Note: Server maintains a maximum of 5 backups. To capture a new backup, older one will be automatically deleted.

Server Notification: Server already contains allowed maximum number of user configuration backups. Existing backup configuration 'xxxxx' will be deleted for storing the new backup.

6. Click **Confirm**.

OPSWAT SDK V3 to V4 Migration

Pulse Secure supports OPSWAT version 3 and version 4 for endpoint compliance evaluation. The migration option helps the administrators to migrate their servers and clients with OPSWAT v4 to take advantage of latest updates.

Software Support

Beginning 9.1R2 release, the following OS are supported:

- Windows 7 and later releases
- macOS 10.12 and later releases

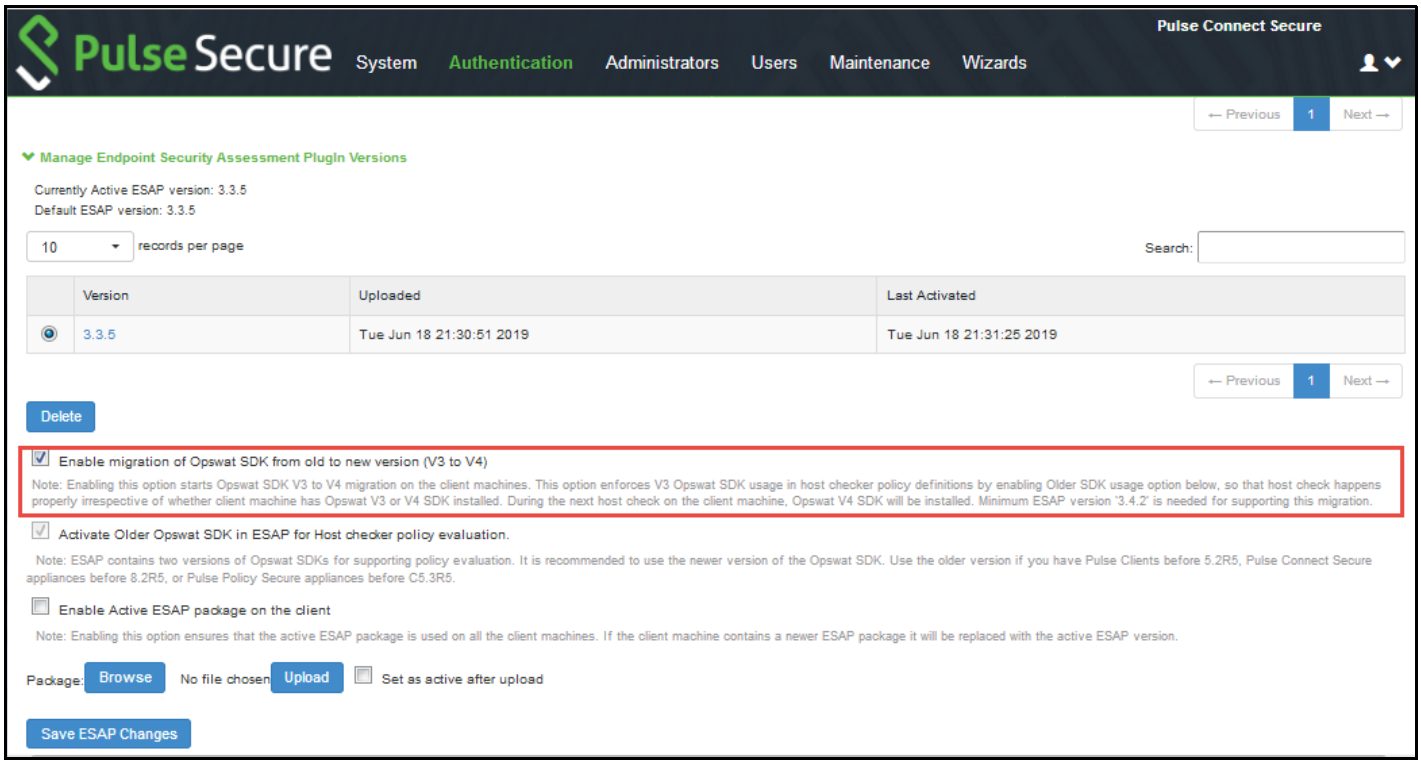
As a prerequisite, a minimum ESAP version 3.4.2 is required for supporting migration of OPSWAT SDK from v3 to v4 version. A warning message is displayed if the minimum version is not present.

To migrate from v3 to v4 version:

1. Navigate to "Manage Endpoint Security Assessment PlugIn Versions" section on the Authentication > Endpoint Security > Host Checker page.
2. Select the Enable migration of Opswat SDK from old to new version (V3 to V4) option.

On enabling this option, the clients start downloading the V4 SDK and migrate to newer SDK.

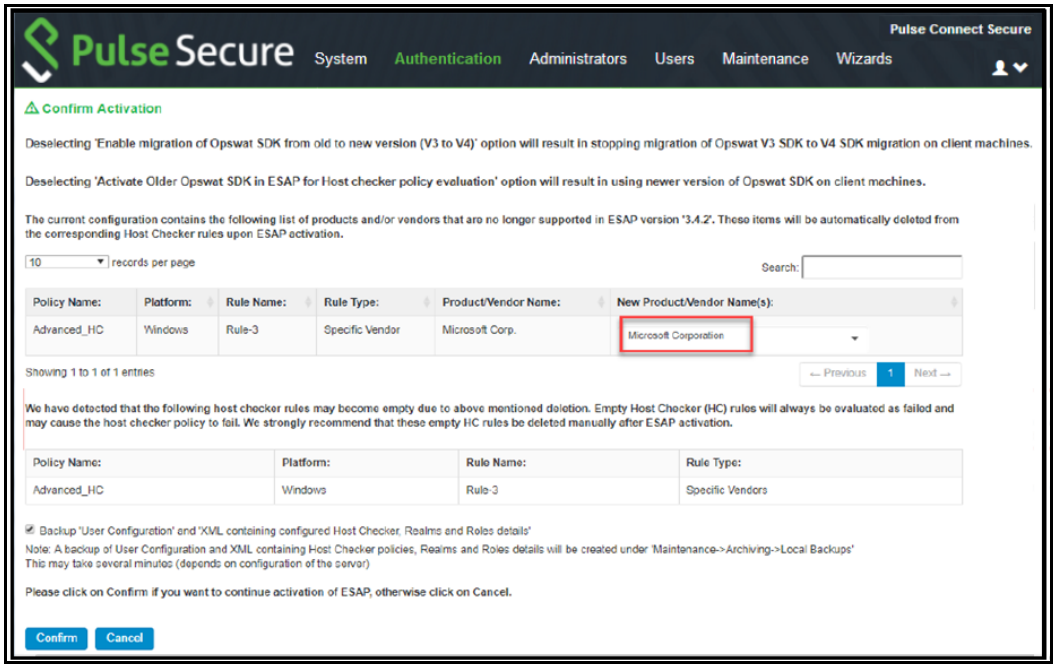
Figure 10 Migration of OPSWAT SDK V3 to V4



3. Clear the **Enable migration of Opswat SDK from old to new version (V3 to V4)** option once the migration is complete.
4. Verify the migration status. In the confirmation message box, click **Confirm**.

Post migration, an administrator can remap the configured products in the policies to map to the newer SDK using the Post Migration window. For example, in the below screenshot, the Product / Vendor Name for the policy has been changed from Microsoft Corp. to Microsoft Corporation for successful migration.

Figure 11 Post Migration Product Mapping



5. Enable **Backup User Configuration and XML containing Host Checker, Realms and Role details** for performing configuration backup. This option helps to revert to the previous version of PCS/PPS configuration, if required.
6. Click **Confirm**.

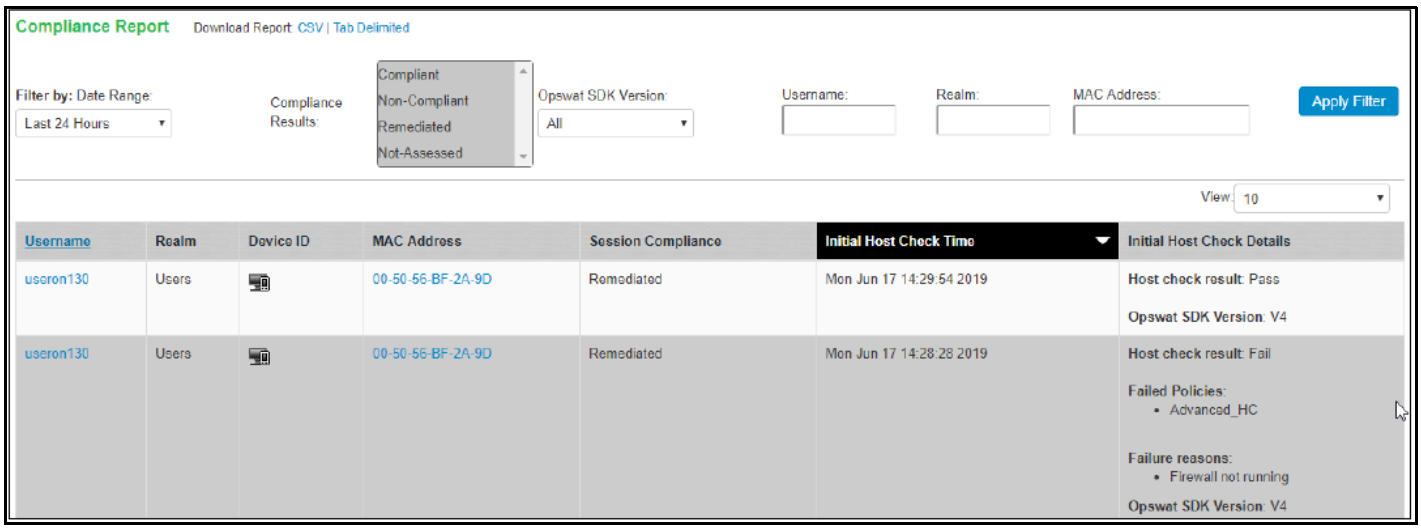
Compliance Report

The Compliance Report displays the compliance details of the users connected to the server. The report also includes the OPSWAT SDK version used for these connections. OPSWAT SDK version is used to filter the users using a specific OPSWAT SDK version.

The compliance report page displays the OPSWAT SDK version details only when the "Enable migration of OPSWAT SDK from old to new version (V3 to V4)" option is enabled.

To check the SDK version for each connection, view the report under System > Reports > Compliance Report.

Figure 12 Compliance Report

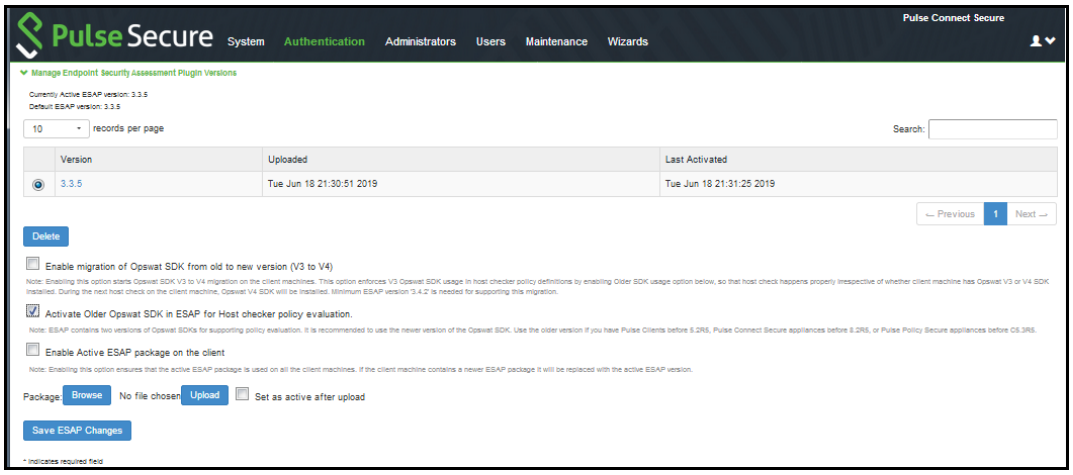


Roll Back Procedure

To roll back to previous version of OPSWAT SDK:

1. Navigate to "Manage Endpoint Security Assessment PlugIn Versions" section on **Authentication > Endpoint Security > Host Checker** page.
2. Clear the **Enable migration of Opswat SDK from old to new version (V3 to V4)** check box.
3. Enable Activate Older Opswat SDK in ESAP for Host Checker policy evaluation.
4. Click **Save ESAP** changes.

   Figure 13 Activate Older SDK



End User Flow

User logging in from browser or User logging in from Pulse Client for L3 connection:

- Client machine has OPSWAT V3 SDK installed.
- Host Check starts on the client machine as part of connection establishment.

- Server sends the required information to client for upgrading V3 to V4 SDK.
- Client downloads V4 SDK and collects the installed security products details using newly installed V4 SDK and sends the detected product details to server.
- Server evaluates configured OPSWAT based rules by consuming the details received from client machine.
- Host Checker continues to use the installed V4 SDK on client machine for subsequent host checks and connections.

User logging in from Pulse client for L2 connections:

- Client machine has OPSWAT V3 SDK installed.
- Host Check starts on the client machine as part of connection establishment.
- Server sends the required information to client for upgrading V3 to V4 SDK.
- During L2 connection, client fails to download V4 SDK.
- Host Checker collects the installed security products details using existing V3 SDK and sends the detected product details to server.
- Server evaluates configured OPSWAT based rules by consuming the details received from client machine.
- L2 connection is established followed by an L3 connection.
- Server detects L2 followed by L3 connection attempt and remembers that ESAP upgrade is needed on the client machine.
- Host Check is triggered again on client machine during L3 connection.
- Server sends the required information to client for upgrading V3 to V4 SDK.
- Client downloads V4 SDK (because L2 connection is complete already) and collects the installed security products details using newly installed V4 SDK and sends the detected product details to server.
- Server evaluates configured OPSWAT based rules by consuming the details received from client machine.
- Host Checker continues to use the installed V4 SDK on client machine for subsequent host checks and connections.

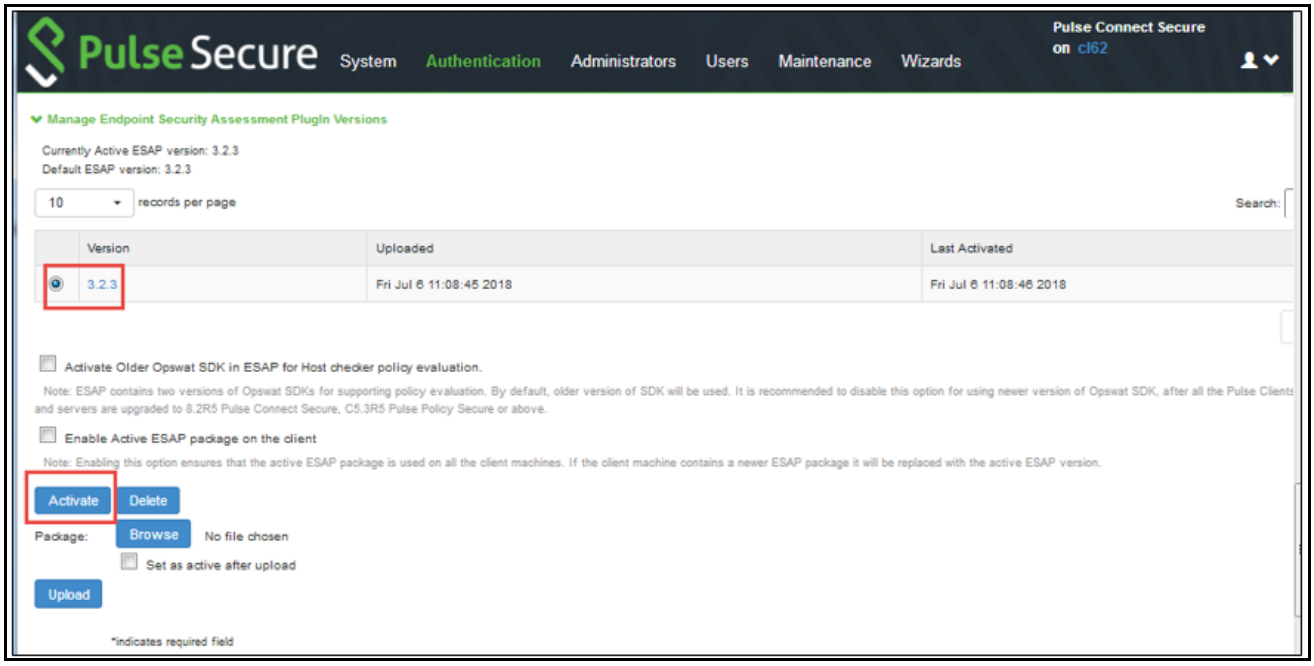
Changing the Active ESAP Package

Administrator can activate any of the already uploaded ESAP packages by selecting the corresponding radio button under "Manage Endpoint Security Assessment Plugin Versions" table and then clicking on "Activate" button.

To change the active ESAP packages:

1. Select **Authentication > Endpoint Security > Host Checker.**
2. Under Manage Endpoint Security Assessment Plugin Versions, select the required ESAP version.
3. Click **Activate**.

Figure 14 Changing Active ESAP package



Note: If the client machine has newer ESAP package and if it has to be replaced, then select "Enable the Active ESAP package". For detailed procedure, see Enabling the Active ESAP Package.

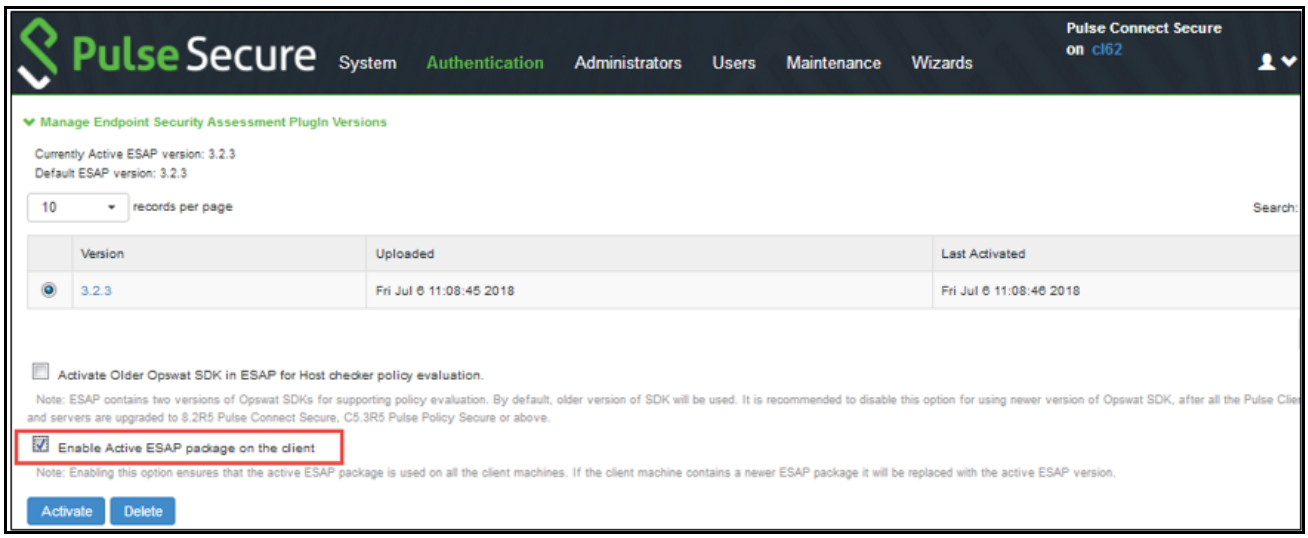
Enabling the Active ESAP Package

Administrator can enable "Enable Active ESAP package on the client" checkbox to ensure that client machine always uses the active ESAP package, even if the active ESAP package is older than the version installed on the client system. In case client machine has newer ESAP package installed, it will be replaced with the older Active ESAP version with this option enabled.

To enable the active ESAP package:

1. Select **Authentication > Endpoint Security > Host Checker.**
2. Under Manage Endpoint Security Assessment Plugin Versions, select the **Enable Active ESAP package** on the client check box.

Figure 15 Enabling Active ESAP package



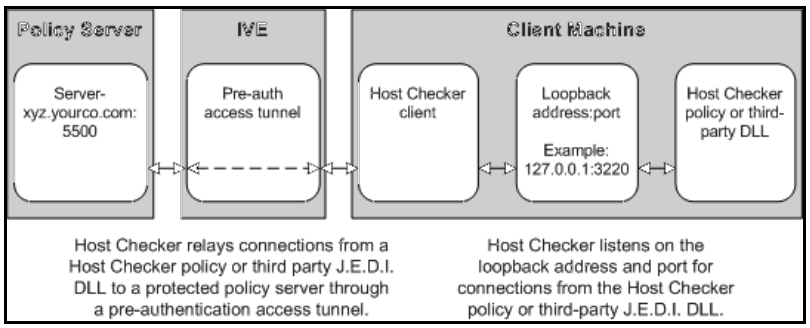
3. Click **Activate**.

Defining Host Checker Pre-Authentication Access Tunnels

If your policies require Host Checker rules or third-party J.E.D.I. DLLs to access a policy server (or other resource) to check compliance before users are authenticated, you can use one of the following methods to make the resource available to the Host Checker Windows clients:

- **Deploy the policy server in a DMZ where Host Checker rules or third-party J.E.D.I. DLLs** can access the server directly instead of going through Connect Secure-This deployment is the simplest solution because you do not have to define a Host Checker pre-authentication access tunnel through Connect Secure between clients and the policy server.
- **Deploy the policy server in a protected zone behind Connect Secure (Windows only)-**This deployment requires you to define a pre-authentication access tunnel. A pre-authentication access tunnel enables Host Checker rules or third-party J.E.D.I. DLLs to access the protected policy server or resource before the system authenticates users. To define a pre-authentication access tunnel, you associate a loopback address (or hostname) and port on the client with an IP address and port on the policy server. You add one or more tunnel definitions to a MANIFEST.HCIF file, which you then upload to Connect Secure. You can upload multiple MANIFEST.HCIF files to Connect Secure. For all third-party policies enabled on a realm, Host Checker creates tunnels for all of the tunnel definitions in all of the MANIFEST.HCIF files, assuming the definitions are unique.
  While running on a Windows client, Host Checker listens for a connection on each loopback address and port you specify in the tunnel definitions. The connections can originate from the integrated Host Checker rules and from client-side or server-side J.E.D.I. DLLs. Host Checker uses the pre-authentication access tunnel(s) to forward the connections through Connect Secure to the policy server(s) or other resource.

Figure 16 Host Checker Creates a Tunnel from a Client to a Policy Server Behind Connect Secure



Note: Host Checker pre-authentication access tunnels are supported on Windows only.

Specifying Host Checker Pre-Authentication Access Tunnel Definitions

For Windows clients, you can define a pre-authentication access tunnel that enables Host Checker methods or third-party J.E.D.I. DLLs to access a protected policy server (or other resource) before users are authenticated.

A definition for a Host Checker pre-authentication access tunnel configures access to one policy server or other resource. Each tunnel definition consists of a pair of IP addresses and ports: one loopback IP address and port on the client, and one IP address and port on the policy server.

You specify one or more tunnel definition(s) in a Host Checker policy package definition file. The package definition file, which must be named MANIFEST.HCIF, defines the name of an interface DLL, the Host Checker policies defined in the DLL, and the pre-authentication access tunnel definitions. Note that if you do not include policies in your package, Host Checker simply enforces that the package has run on the client. If you do declare policies through this file, they become available through the admin console where you can implement them at the realm, role, and resource policy levels.

Within the MANIFEST.HCIF file, you must include one definition per line, with a blank line between each definition, using the following format:

HCIF-Main: <DLLName>

HCIF-Policy: <PolicyName>

HCIF-IVE-Tunnel: <client-loopback>:port <policy-server>:port

where:

<DLLName> is the name of the interface DLL, such as myPestPatrol.dll. Even if you are not using an interface DLL, you must include a dummy DLL as a placeholder file that has this exact name.

<PolicyName> is the name of a policy defined in the DLL, such as myFileCheck. You can define multiple policies by using the HCIF-Policy statement for each policy. If you are not using an interface DLL, you can use any policy name as a placeholder.

The syntax of a Host Checker tunnel definition is:

HCIF-IVE-Tunnel: <client-loopback>:port <policy-server>:port

where:

<client-loopback> is a loopback address that begins with 127. and takes any of the following forms:

- An IP address and port that takes the form of 127.*.*.*:port. To avoid conflicts with JSAM, do not use 127.0.0.1 with port 80, but you can use 127.0.0.1 with other ports. For example: 127.0.0.1:3220

- A hostname that resolves to a loopback address that begins with 127. You can use a local hosts file on each client computer or a DNS server to resolve the loopback address.
- A hostname that does not resolve to a loopback address, or resolves to a non-loopback address. In these cases, Host Checker allocates a loopback address and updates the local hosts file on the client with the mapping. Note that the user must have administrator privileges in order for Host Checker to modify the local hosts file. If the user does not have administrator privileges, Host Checker cannot update the hosts file and cannot open the pre-authentication access tunnel. In that case, Host Checker logs an error.

<policy-server> is the IP address or hostname of the back-end policy server. Connect Secure resolves the hostname you specify.

For example, in the following tunnel definition, 127.0.0.1:3220 is the client loopback address and port, and mysygate.company.com:5500 is the policy server hostname and port:

HCIF-IVE-Tunnel: 127.0.0.1:3220 mysygate.company.com:5500

Or you can use a hostname for the client, as in this example:

HCIF-IVE-Tunnel: mysygate.company.com:3220 mysygate.company.com:5500

Keep the following in mind when specifying tunnel definitions:

- You must add a blank line between each line in the MANIFEST.HCIF file, and you can use a semi-colon at the beginning of a line to indicate a comment. For example:

  HCIF-Main: myPestPatrol.dll

  HCIF-Policy: myFileCheck

  HCIF-Policy: myPortCheck

  ; Tunnel definitions

  HCIF-IVE-Tunnel: 127.0.0.1:3220 mysygate.company.com:5500

  HCIF-IVE-Tunnel: 127.1.1.1:3220 mysygate2.company.com:5500

  HCIF-IVE-Tunnel: mysygate.company.com:3220 mysygate3.company.com:5500
- Host Checker pre-authentication access tunnels are supported on Windows only.
- If <client-loopback> is a non-loopback address, then Host Checker cannot open the pre-authentication access tunnel and logs an error instead.

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 an authentication policy, a role mapping rule, or a resource policy.

To specify general Host Checker options:

1. In the admin console, choose **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 or resource policy, then the system denies the associated user requests.

  For example, you may require that a user runs a specific third-party antivirus application in order to map to Role A, which enables network connections from an external location. 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 all access features enabled for Role A. If the antivirus application stops running during the user session, however, 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 an end-user logs into a Realm, Host Checker performs an initial policy check, regardless of whether or not the policy is enforced at the Realm, Role, and/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 end-user clients connected to the system. Each client performs its own initial policy check and starts its own X minute countdown. If you configure the authentication policy within a realm where Host Checker enforces policies (versus installing), the enforcement occurs only during the pre-authentication 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 an end-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 end-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 end-user loses rights to all available roles due to Host Checker policy evaluation, the end-user session is disconnected.

  If you configure a resource-based policy rule where Host Checker enforces policies, the enforcement occurs when the end-user attempts to access the resource/backend server. For web resources, the Host Checker evaluation occurs at each request. For SAM and STA resources, the Host Checker evaluation occurs when the system activates the connection to the backend application/server. For VPN Tunneling access, the Host Checker evaluation occurs when the system initiates VPN Tunneling. Existing connections of applications running by way of SAM, Telnet/SSH connection, and VPN Tunneling connections are not affected by further Host Checker evaluations. Only new Web requests, new applications across SAM, new instances of STA, and launching VPN Tunneling are affected. The Host Checker evaluation is based on the most recent policy check that occurred X minutes ago. Example, if you configure the frequency setting to Perform check every five minutes and the end-user attempts to access a protected resource or attempts to launch VPN Tunneling four minutes after the last check, then the policy evaluation is based on the state of the client machine four minutes ago, not at the moment the end-user attempted to access the resource.

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

- 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 to the device, 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.
- Select Perform dynamic policy reevaluation to automatically refresh the roles of individual users by enabling dynamic policy evaluation for Host Checker. Host Checker can trigger the system to evaluate resource policies whenever a user's Host Checker status changes. (If you do not select this option, the system does not evaluate resource policies but it does evaluate the authentication policy, role mapping rules, and role restrictions whenever a user's Host Checker status changes.)

3. Click **Save Changes.**

Specifying Host Checker Installation Options

If you implement any policy at the realm, role, or resource policy level that requires Host Checker, you must provide a mechanism by which the system or the user can install Host Checker on the client machine. Otherwise, when the system evaluates the Host Checker policy, the user's machine fails because the Host Checker client is not available to return a success status.

You can use three methods to install Host Checker on a user's system:

- Connect Secure automatically installs Host Checker-Enable automatic installation through the Users/ Administrators > User Realms/Administrator Realms > [Realm] > Authentication Policy > Host Checker page of the admin console. When you do, the system evaluates the realm-level option when the user accesses the sign-in page and then determines if the current version of Host Checker is installed on the user's machine. If Host Checker is not installed, the system attempts to install it using either an ActiveX or a Java delivery method or Pulse Secure Application Launcher (PSAL). When a Windows user signs in to a device, 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 the Host Checker program.

  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 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.

  Due to the end of ActiveX and Java support on many browsers, an alternate solution is provided for launching of client applications such as Host Checker or Pulse Secure Client. For Google Chrome and Edge Browsers on Windows and for Safari and Chrome browsers on MAC, we use PSAL for installing Host checker.

Note: Due to some anomalies with Microsoft JVM, Host Checker may not install, and an error box appears. If this occurs, click **Try Again**. The subsequent installation should succeed.

If the system cannot use the Java delivery method because Java is disabled on the user's system, it displays a no-access error message.

Note: On Microsoft operating systems, the setup client and Host Checker install automatically.

- The user or administrator manually installs Host Checker (Windows only)-Download the Host Checker installer from the Maintenance > System > Installers page of the admin console and use it to manually install Host Checker on the user's system.

Note: To install Host Checker, users must have appropriate privileges, as described in the Client-side Changes Guide on the Pulse Secure Global Support Center (PSGSC) Center. If the user does not have these privileges, use the Pulse Secure Installer Service available from the Maintenance > System > Installers page of the admin console to bypass this requirement.

Host Checker is supported for agent and agentless clients. The installation options are listed below:

- Browser-based Host Checking (Agentless) - This is used for browser-based logins and requires PSAL to be present on the endpoint. If PSAL is not available on the endpoint, it gets installed as part of the connection.
  It is recommended not to keep a very low value for login inactivity timeout (For example,1 or 2 minutes). This might result in connection timeouts on fresh endpoints where PSAL also need to be installed as part of compliance evaluation.
- Pulse Client (Agent)-You can use Pulse client, which contains the Host Checker component for compliance check. To manually install the Host Checker, Select Maintenance > System > Installers and download the Pulse installer.

Client ActiveX Installation Delay

During end-user sign-in, the setup client is delivered through either ActiveX or Java, depending on the client system's capability. By default, Internet Explorer blocks ActiveX content and displays an information bar that lets the user decide whether to install the new ActiveX control.

Note: For restricted users, the information bar displays help information only, it does not allow installation of new ActiveX controls.

The system displays to end-users an intermediate page with a 15-second delay to interact with the information bar content. End-users can choose to skip the installation (and the 15-second delay) by clicking the "click here" link. If end-users choose to skip the installation, they are not prompted again unless they clear their browser cookies.

Administrators can customize the message and locale displayed in this intermediate page by clicking the Custom Messages tab in the Default Options for User Roles page and filling out information under the User Login Messages section.

Using Host Checker with the GINA Automatic Sign-In Function

Using Host Checker in conjunction with the Windows Graphical Identification and Authorization (GINA) sign-in function for VPN Tunneling requires that you pay particular attention to the type, level, and number of items to verify on the client before granting or rejecting access to the system. Since the GINA sign-in function takes place before Windows has completely launched on the client, and therefore, before the user profile on Windows is created, we recommend you adopt the following practices when creating Host Checker policies, you plan to use for Windows clients featuring the GINA sign-in function:

- You can check system-level processes at both realms enforce and realm evaluate. You can check user-level processes only at realm evaluate.

- If you have user-level processes at realm evaluate, create a separate VPN Tunneling role featuring only system-level policy checks that can be performed before Windows has completely launched on the client. Ensure that this role allows connectivity to the Windows Domain infrastructure in your secure network to support drive mapping, software updates, and group policies, for example. Mapping your users to this role allows the GINA authentication to complete. This role is in addition to the final role that you want the user to be mapped.

Installing Host Checker Automatically or Manually

To automatically install Host Checker on client computers:

1. In the admin console, choose **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. Here is a summary of what happens when the Auto-upgrade Host Checker option is selected or not selected:
   - 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 Global Support Center (PSGSC) Center.
     - If a user uninstalls Host Checker and then signs in to a device for which the Auto-upgrade Host Checker option is not enabled, the user no longer has access to Host Checker.
3. Click **Save Changes**.

   An administrator may choose to download and install Host Checker manually on their client systems. The Maintenance > System > Installers page of the admin console provides several applications and a service for download. You can download an application 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.

Using Host Checker Reports and Logs

You can use the admin console to learn details about Host Checker policy violations.

Figure 17 shows the Compliance report. Note that the type of rule that has been violated is shown.

Figure 17 Compliance Report

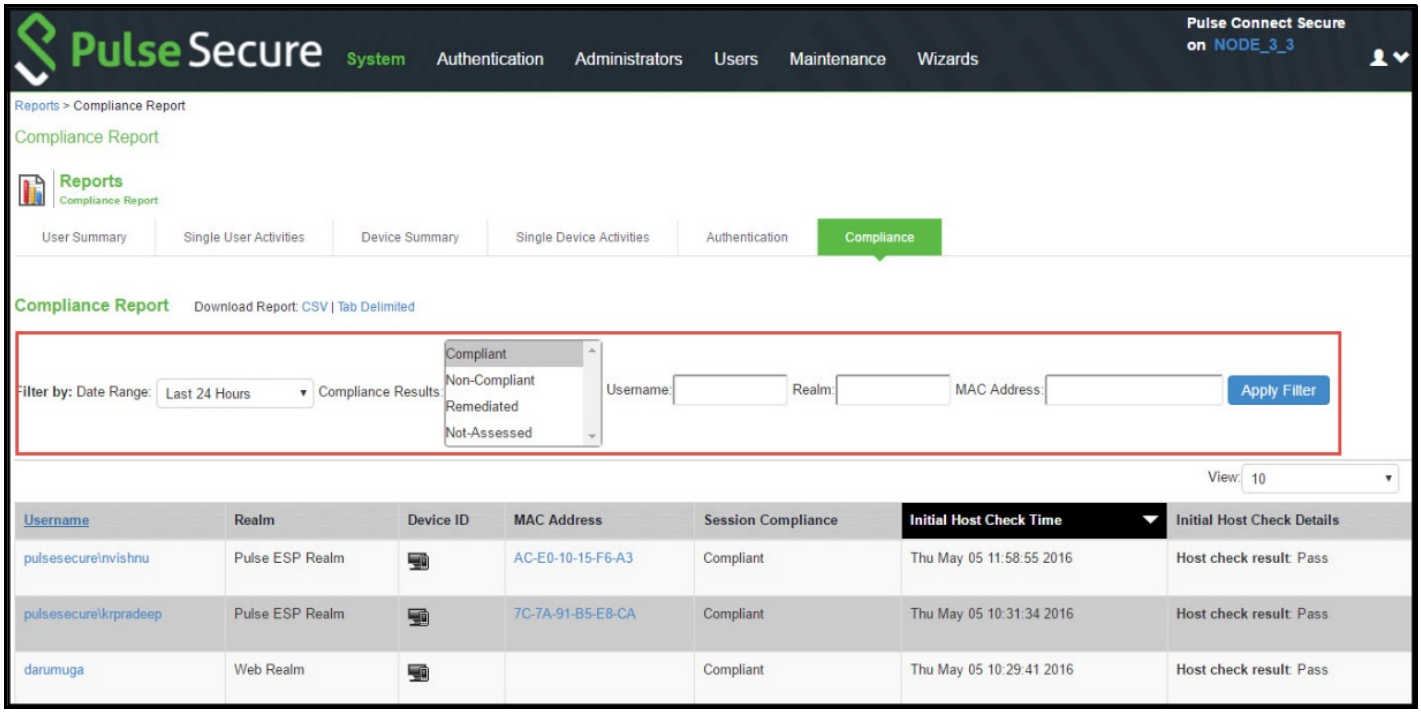
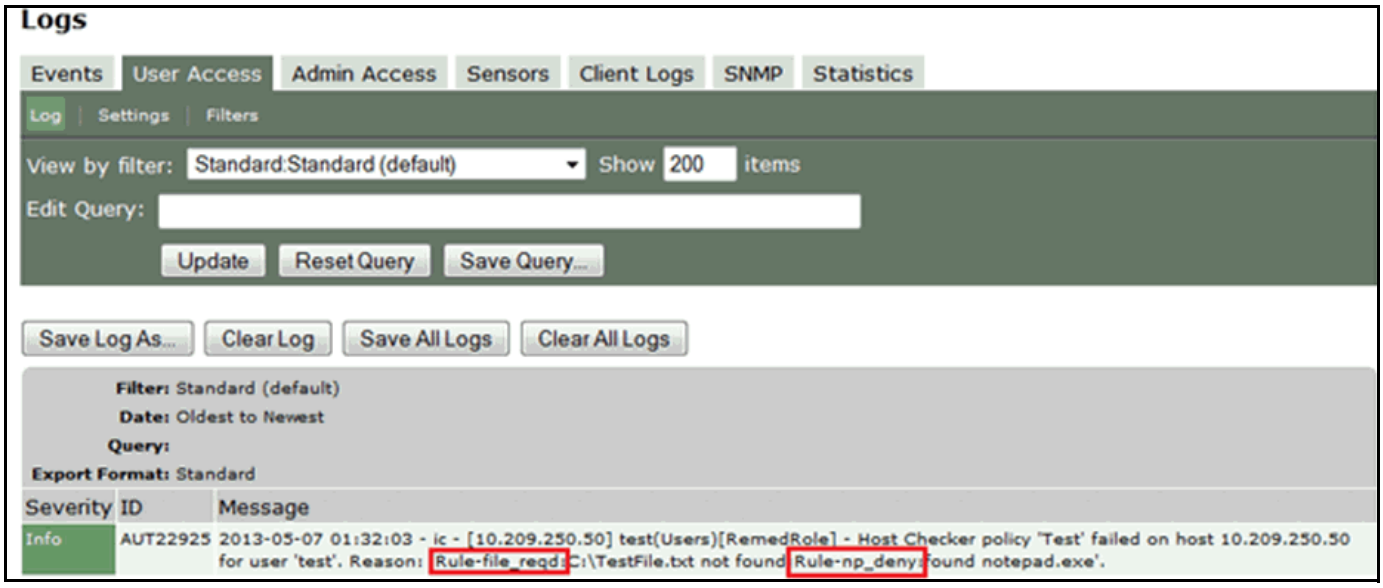


Figure 18 shows a log entry for a session that violates a Host Checker rule. Note the names of the configured rules that have been violated are shown in the log.

Figure 18 User Access Log - Host Checker



To display the Compliance report:

1. Select **System > Reports > Compliance.**
2. Select a filter:
   - **Compliant**
   - **Non-Compliant**
   - **Remediated**
   - **Not Assessed**

To display User Access logs:

1. Select **System Log/Monitoring.**
2. Click the **User Access** tab.
3. Click the **Log** tab.

Host Checker for Apple iOS

Host Checker for Pulse iOS Clients

Host Checker is a component of Pulse Secure client that reports the integrity of iOS endpoints that are attempting to connect to the system. Host Checker runs as a Trusted Network Connect (TNC) client on the endpoint. The client evaluates the endpoint according to predefined criteria and reports to the Trusted Network Connect server, which is a part of Connect Secure. If the endpoint is not in compliance with the Host Checker policies, then the user might not get access to the network or might get limited access to the network depending upon the enforcement policies configured by the administrator.

For iOS clients, Host Checker can evaluate client compliance based on the following predefined criteria:

- **OS Checks** - You can specify the iOS version or minimal version that must be installed on the device.
- **Jail Breaking Detection** - Jail breaking is a process that allows Apple iPhone, iPad and iPod Touch users to gain root access to the iOS operating system and bypass usage and access limitations imposed by Apple. With a jail broken device, an iOS user can install applications that are not available through the Apple App Store. Jail broken devices expose the device to a greater risk of running malicious applications.

Host Checker evaluation policies can be part of a larger Host Checker configuration that applies to many different types of clients or to iOS devices only.

Configuring Host Checker for Pulse iOS Clients

Host Checker policies can be part of a larger Host Checker configuration that applies to many different types of clients or to iOS devices only. However, you might find it easiest to create a separate Host Checker policy specifically for iOS devices.

To create a Host Checker policy for iOS devices:

1. From the admin console, select **Authentication > Endpoint Security > Host Checker.**
2. In the Policies section, click **New** to open a New Host Checker Policy page.
3. Specify a name for the new policy and then click **Continue** to open the Host Checker Policy page.

   The name appears in lists when you implement the policy so be sure to use a descriptive name, such as **iOS HC Policy.**
4. Click the **Mobile** tab, and then click the **iOS** tab.
5. In the Rule Settings section, click **Select Rule Type** and select one of the following options and then click **Add**:

   - **OS Checks** - To specify the iOS version that must be installed on the device:

   a. Specify a descriptive name for this rule. For example, **Must-Be-iOS-4.1-or-higher**. Rule names cannot include spaces.

   b. Specify the criteria. For example, to enforce iOS 4.1 and later, create two conditions: Equal to 4.1 and Above 4.1.
   Host Checker supports iOS versions 4.1 through 4.3.X.

   c. Click **Save Changes**.

   - **Jail Breaking Detection** - Jail breaking is a process that allows Apple iPhone, iPad and iPod Touch users to gain root access to the iOS operating system. and bypass usage and access limitations imposed by Apple. With a jail broken device, an iOS user can install applications that are not available through the Apple App Store. Jail broken devices possess a greater risk of running malicious applications.

   a. Specify a descriptive name for this rule. For example, **No-iOS-Jailbreak**.

   b. The **Don't allow Jail Broken devices** check box is enabled by default.

   c. Click **Save Changes.**
6. After you have configured all of your rules, specify how you want to enforce them by choosing one of the following options:

   - All of the rules
   - Any of the rules
   - Custom

     For Custom requirements, you can specify a custom expression using Boolean operators AND and OR and also group and nest conditions using parenthesis.
7. Specify remediation options:

- **Enable custom instructions** - If you enable this check box, a text box appears and allows you to type information that appears on the user's device if Host Checker discovers an issue.
- **Send reason strings** - Select this option to display a message to users (called a reason string) that explains why the client machine does not meet the Host Checker policy requirements. For example, if the jailbreak detection policy fails, Pulse appears, **A jailbroken device is not allowed to access the network. Please contact your network administrator.**

8. When you are finished, click **Save Changes**.

   A host checker policy configured for a VPN tunnel is not triggered if the VPN tunnel is launched automatically by VPN on Demand on an Apple iOS device. If the VPN session is started through the Pulse client, the host checker policy is applied correctly. A VPN on Demand configuration enables an iOS device to automatically initiate a VPN connection when any application running on the phone initiates a connection to a host in a predefined set of hosts. A VPN on Demand connection uses client certificate-based authentication, so the user does not have to provide credentials every time a VPN connection is initiated.

Implementing Host Checker Policies for Pulse for iOS Devices

After you create one or more Host Checker policies for iOS devices, you must implement them. The system can use Host Checker policies at the realm or the role level.

Realm Authentication-You can configure a realm authentication policy to download and run Host Checker with a particular Host Checker policy. If the iOS device does not meet the Host Checker requirements, then the system can deny access. You can provide remediation information in the Host Checker policy to describe the requirement and help users take steps to solve the issue.

To enable a Host Checker policy for a realm:

1. From the admin console, select **Users > User Realms > SelectRealm > Authentication Policy > Host Checker.** The Host Checker page displays all of the available Host Checker policies.
2. Select the check box next to each policy you want to include. Select one or both of the following check boxes next to the policy:
   - **Evaluate Policies** -Evaluates without enforcing the policy on the iOS device and allows access.
   - **Require and Enforce** - Requires that the iOS device be in compliance with the Host Checker policy. The system downloads Host Checker to the iOS device 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.
3. Optionally select **Allow access to realm if any ONE of the selected "Require and Enforce" policies** is passed. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an iOS device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to iOS devices.
4. Click **Save Changes**.

Role-You can configure a role to download and run Host Checker with a particular Host Checker policy. If the iOS device does not meet the Host Checker requirements, then the system can deny access or assign the user to a remediation role that has limited access. You can provide remediation information in the Host Checker policy to help users take steps to solve the issue.

To enable a Host Checker policy for a role:

1. From the admin console, select **Users > User Roles > SelectRole > General > Restrictions > Host Checker**. The Host Checker page displays all of the available Host Checker policies.
2. Select **Allow users whose workstations meet the requirements specified by these Host Checker policies**.
3. In the Available Policies list, select the policies that you want to apply to select them, and then click **Add** to move them to the Selected Policies list. To select a policy click it. To select more than one policy, use Ctrl+click.
4. Optionally select **Allow access to the role if any ONE of the selected policies (except cache-cleaner) i**s passed. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an iOS device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to iOS devices.
5. Click **Save Changes.**

Host Checker for Android

Host Checker for Pulse Android Clients

Host Checker is a component of Pulse Secure client that reports the integrity of Android endpoints that are attempting to connect to the system. Host Checker runs as a Trusted Network Connect (TNC) client on the endpoint. The client evaluates the endpoint according to predefined criteria and reports to the Trusted Network Connect server, which is a part of Connect Secure. If the endpoint is not in compliance with the Host Checker policies, then the user might not get access to the network or might get limited access to the network depending upon the enforcement policies configured by the administrator.

For Android clients, Host Checker can evaluate client compliance based on the following predefined criteria:

- **OS Checks**- You can specify the Android version or minimal version that must be installed on the device.
- **Rooting Detection**-Rooting is a process that allows Android users to gain root access to the Android operating system and bypass usage and access limitations imposed by Android. With a Rooting device, an Android user can install applications that are not available through the Play Store. Rooted devices expose the device to a greater risk of running malicious applications.

Host Checker evaluation policies can be part of a larger Host Checker configuration that applies to many different types of clients or to Android devices only.

Configuring Host Checker for Pulse Android Clients

Host Checker policies can be part of a larger Host Checker configuration that applies to many different types of clients or to Android devices only. However, you might find it easiest to create a separate Host Checker policy specifically for Android devices.

To create a Host Checker policy for Android devices:

1. From the admin console, select **Authentication > Endpoint Security > Host Checker.**
2. In the Policies section, click **New** to open a New Host Checker Policy page.
3. Specify a name for the new policy and then click Continue to open the Host Checker Policy page. The name appears in lists when you implement the policy so be sure to use a descriptive name, such as **Android HC Policy.**
4. Click the **Mobile** tab, and then click the **Android** tab.
5. In the Rule Settings section, click **Select Rule Type** and select one of the following options and then click Add:

- OS Checks-To specify the Android version that must be installed on the device:
    1. Specify a descriptive name for this rule. For example, **Must-Be-Android-4.4-or-higher.** Rule names cannot include spaces.
    2. Specify the criteria. For example, to enforce Android 4.4 and later, create two conditions: Equal to 4.4 and Above 4.4.

       Host Checker supports Android versions 4.4 through 4.4.X.
    3. Click **Save Changes**.
- **Rooting Detection**- Rooting is a process that allows Android users to gain root access to the Android operating system and bypass usage and access limitations imposed by Android. With a Rooting device, an Android user can install applications that are not available through the Play Store. Rooted devices expose the device to a greater risk of running malicious applications
    1. Specify a descriptive name for this rule. For example, **No-Android-Rooting**.
    2. The **Don't allow Rooted devices** check box is enabled by default.
    3. Click **Save Changes.**

6. After you have configured all of your rules, specify how you want to enforce them by choosing one of the following options:
    - All of the rules
    - Any of the rules
    - Custom

    For Custom requirements, you can specify a custom expression using Boolean operators AND and OR and also group and nest conditions using parenthesis.
7. Specify remediation options:
    - **Enable custom instructions**-If you enable this check box, a text box appears and allows you to type information that appears on the user's device if Host Checker discovers an issue.

- **Send reason strings**-Select this option to display a message to users (called a reason string) that explains why the client machine does not meet the Host Checker policy requirements. For example, if the Rooting detection policy fails, Pulse appears, **A Rooting device is not allowed to access the network. Please contact your network administrator.**

8. When you are finished, click **Save Changes**.

Implementing Host Checker Policies for Pulse for Android Devices

After you create one or more Host Checker policies for Android devices, you must implement them. The system can use Host Checker policies at the realm or the role level.

Realm Authentication-You can configure a realm authentication policy to download and run Host Checker with a particular Host Checker policy. If the Android device does not meet the Host Checker requirements, then the system can deny access. You can provide remediation information in the Host Checker policy to describe the requirement and help users take steps to solve the issue.

To enable a Host Checker policy for a realm:

1. From the admin console, select **Users > User Realms > SelectRealm > Authentication Policy > Host Checker.** The Host Checker page displays all of the available Host Checker policies.
2. Select the check box next to each policy you want to include. Select one or both of the following check boxes next to the policy:
   - **Evaluate Policies-**Evaluates without enforcing the policy on the Android device and allows access.
   - **Require and Enforce**-Requires that the Android device be in compliance with the Host Checker policy. The system downloads Host Checker to the Android device 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.
3. Optionally select **Allow access to realm if any ONE of the selected "Require and Enforce"** policies is passed. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an Android device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to Android devices.
4. Click **Save Changes**.

Role - You can configure a role to download and run Host Checker with a particular Host Checker policy. If the Android device does not meet the Host Checker requirements, then the system can deny access or assign the user to a remediation role that has limited access. You can provide remediation information in the Host Checker policy to help users take steps to solve the issue.

To enable a Host Checker policy for a role:

1. From the admin console, select **Users > User Roles > SelectRole > General > Restrictions > Host Checker**. The Host Checker page displays all of the available Host Checker policies.
2. Select **Allow users whose workstations meet the requirements specified by these Host Checker policies.**
3. In the Available Policies list, select the policies that you want to apply to select them, and then click Add to move them to the Selected Policies list. To select a policy click it. To select more than one policy, use Ctrl+click.

4. Optionally select **Allow access to the role if any ONE of the selected policies (except cache-cleaner)** is passed. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an Android device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to Android devices.
5. Click **Save Changes.**

Host Checker and the Lightweight Pulse Secure Apps and Plugins for Windows

Pulse Secure offers a variety of lightweight apps and plugins for simplified VPN connectivity to a Pulse Connect Secure gateway from a Windows endpoint. These offerings include:

- Pulse Secure "Universal App" for Windows 10
- Pulse Secure "Inbox" VPN Plugin for Windows 8.1
- Pulse Secure Mobile Client for Windows Phone 8.1

The Pulse Secure "Universal App" for Windows 10 currently provides just one built-in Host Checker function: The "OS Check". The "Inbox" VPN Plugin for Windows 8.1 and the Mobile Client for Windows Phone 8.1 support the "OS Check" and the Host Checker "Statement of Health" (SoH) policy. For more information on these apps and their interaction with Host Checker, see the Pulse Secure Universal App for Windows - Quick Start Guide.

Host Checker on Google Chrome OS

At the Google Chrome OS Store, Pulse Secure offers a lightweight Pulse Secure mobile client app. As with the "Universal App" for Windows, this Google Chrome OS App provides only the "OS Check" Host Checker functionality. For more information, see the Pulse Secure Client for Chrome OS - Quick Start Guide.

Using Proxy Exceptions

Connect Secure clients parse Internet Explorer's static proxy exception list. The system supports most exceptions that Internet Explorer supports with the following limitations:

- For IP address exception, we support n.*.*.*, n.n.*.*, n.n.n.*. For example, 10.*.*.*, 10.10.*.*, 10.10.10.*, or 10.10.10.10. We do not support 10* or 10.*.10.* even though Internet Explorer may support them.
- For string expression, we support specific strings such as my.company.net,or a wild card at front of the string, for example, *.my.company.net or *.company.net. We do not support *.company.*, *.company*, *.company. *.com, *.net *.com and so forth.

Host Checker on Pulse Linux Client

Pulse Secure client for Linux provides secure connectivity between a device running Linux and Pulse Connect Secure. Pulse Secure client for Linux provides File, Process and Port Host Checker functionality. For more information, see the Pulse Secure Client for Linux - Quick Start Guide