How to set up Pulse Secure Host Checker SSL VPN with OPSWAT Gears Client

About This Guide

Gears is a platform for network security management for IT and security professionals that provides visibility over all types of endpoint applications from antivirus to hard disk encryption and public file sharing, as well as the ability to enforce compliance and detect threats. More information on Gears may be found at https://www.opswatgears.com.

Gears can be leveraged by Pulse Secure's Endpoint Security Host Checker policies to provide enhanced compliance checking capabilities for the Junos Pulse application. There are three standard methods for configuring the Pulse Secure Host Checker policy to leverage Gears to control network access. Each method has its pros and cons, and each can be used in combination with the others on the same or multiple realms. The three methods covered by this guide:

1. Create an Antivirus Rule in Pulse Secure Host Checker to leverage Gears
    - Summary: Checks if Gears is running and the endpoint is in a compliant state
        - Pro: Easy setup
        - Con: Only verifies compliance state, but not to which account/policy it complies
2. Create a Custom Process and Registry Check in Pulse Secure Host Checker to leverage Gears
    - Summary: Checks if Gears is running, endpoint belongs to a certain account, and is in a compliant state
        - Pro: Works with all client types; Checks state and require a specific account/policy
        - Con: Setup is marginally more complicated than #1
3. Create a Third Party Policy in Pulse Secure Host Checker to leverage Gears
    - Summary: Similar to #2 but first automatically distributes Gears portable to the endpoint
        - Pro: No need to separately deploy Gears to the endpoints
        - Con: Only supported for Windows endpoints; limited auto-remediation options*

          * Auto-remediation for guest devices is being added in Q4/2014-Q1/2015

More information on the benefits of integrating Gears with Pulse Secure Host Checker can be found at https://www.opswatgears.com/integration/secure-access.

This guide specifically illustrates how to establish Gears policy checks for Windows and Mac OS devices through Pulse Secure Host Checker. Please note that in order to leverage these checks additional configurations must be made to the Realms, Roles, and Profiles. These standard Pulse Secure device configurations options are outside the scope of this guide.

Method #1: Antivirus Policy

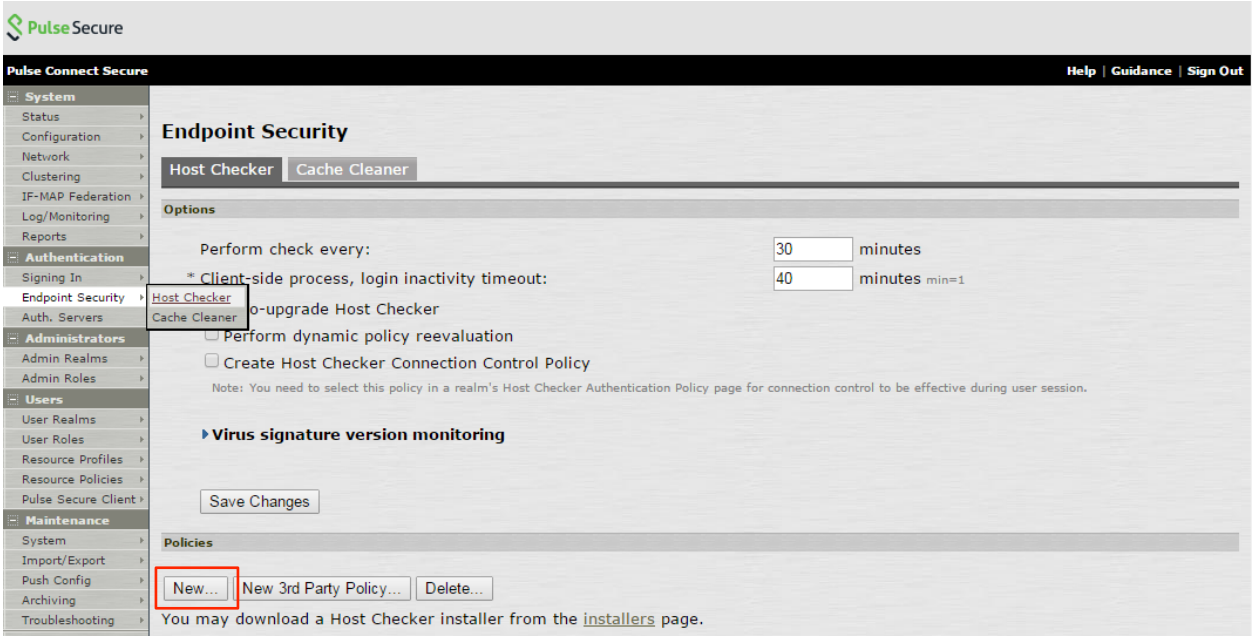
The first method of configuring Pulse Secure Host Checker to utilize Gears for compliance checks uses an Antivirus rule in the Endpoint Security/Host Checker portion of Junos Pulse.

Once completed, if the Gears client is installed and running on an endpoint, it will be detected as an antivirus. When a check for real-time-protection is performed, the Gears client will return *Enabled* only if Gears client is currently running and the endpoint device is meeting all policy* requirements established within Gears.

*Note: This method cannot check *to which* account/policy an endpoint is compliant, only that it is or isn't compliant.

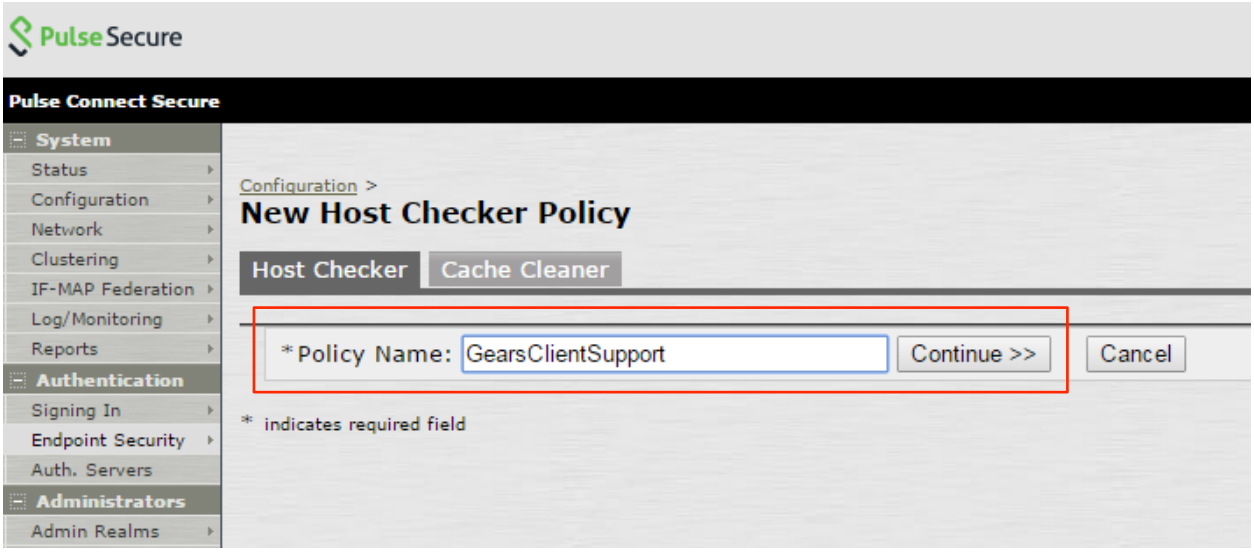
Step 1:

Under *Endpoint Security*, select the *Host Checker* tab.



Step 2:

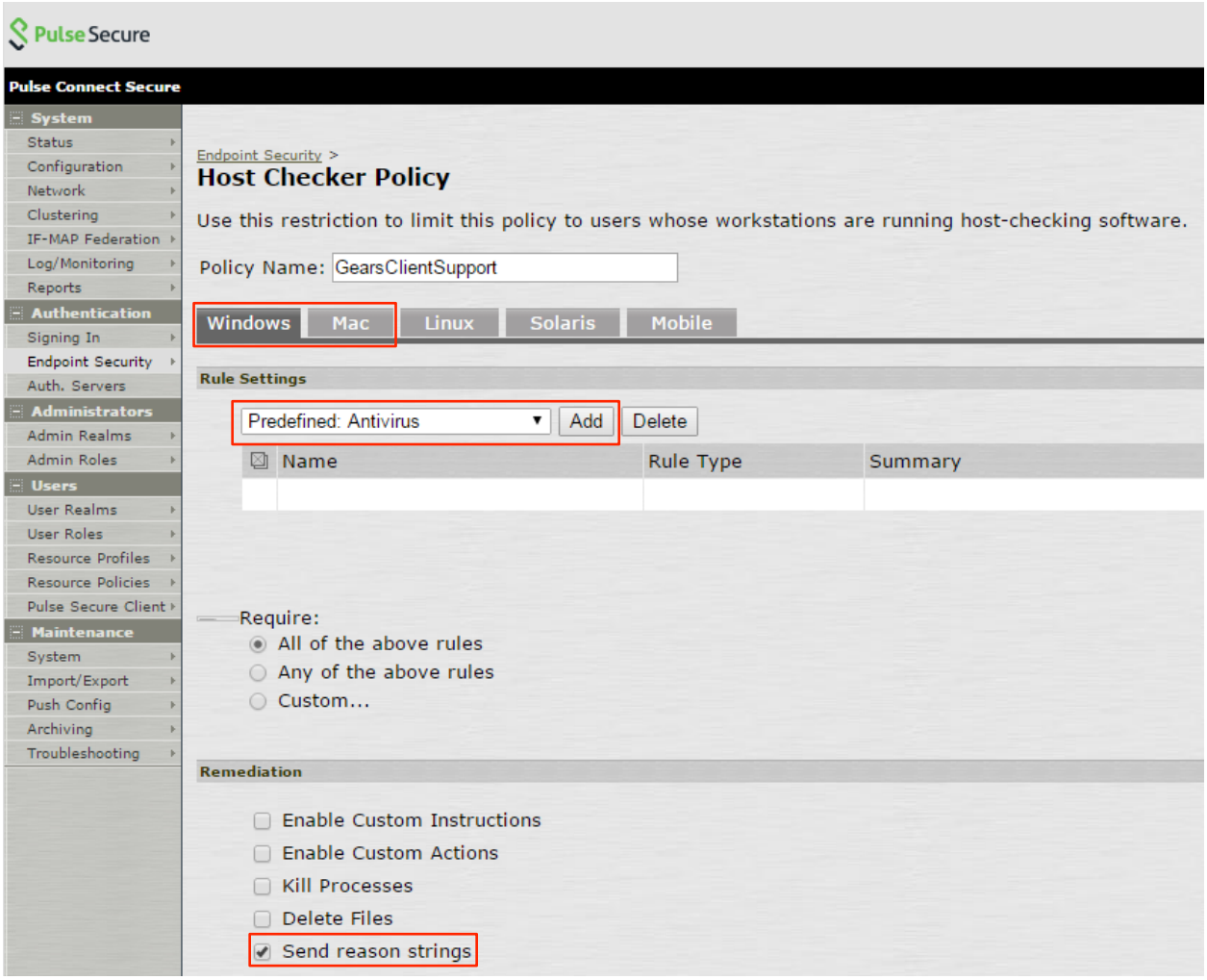
Under *Policies*, you can create a New policy or Edit an existing one. When creating a new policy, users will be prompted to provide a policy name.



Step 3:

This step allows you to add a rule for the Antivirus. Please note that by default Windows will be selected. For a Mac OS rule please select Mac and enter the same information outlined below.

Select *Predefined: Antivirus* from the drop down and click Add. Ensure under *Require* that *All of the above rules* is selected and under *Remediation* you have selected *Send Reason Strings* (the default configuration).

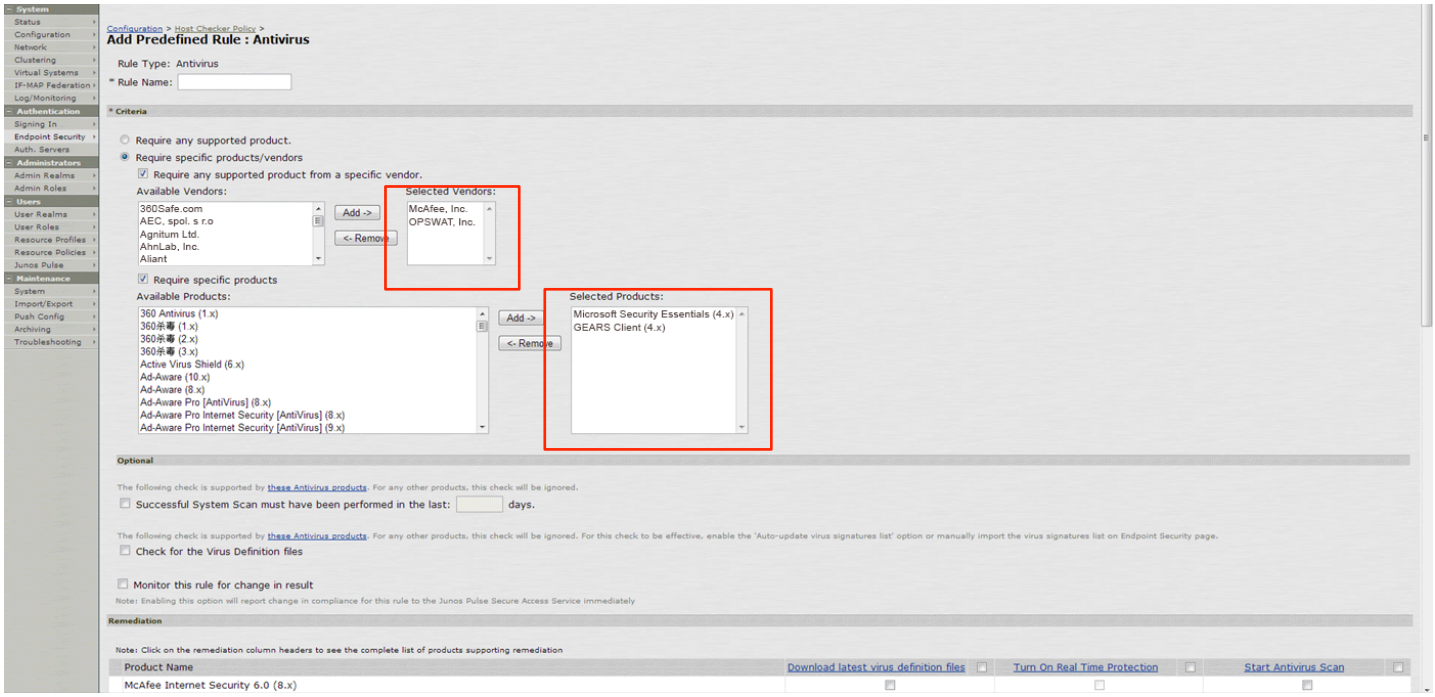


Step 4:

Establish a name for the rule and set the criteria along with any optional checks.

A User may require any supported product or go with a specific set of vendors and or products. For Gears specifically, users will select the following:

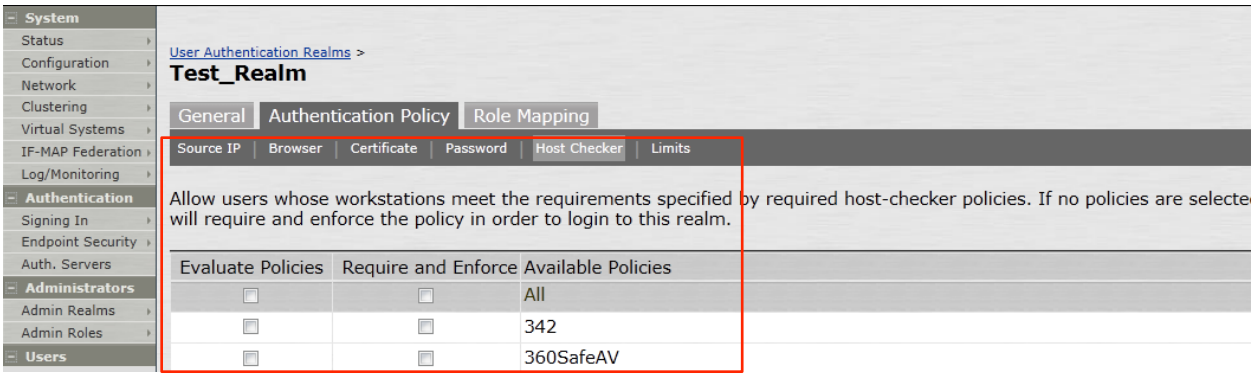
- Vendor – OPSWAT, Inc.
- Product – Gears Client



Step 5:

You can setup any other compliance requirements relevant to your organization at this time. Under *Save Changes*, click Save Changes.

Host Checker is now setup for the Antivirus Compliance policy and will check for the presence of Gears Client as well as the status of real time protection. An endpoint will only pass this antivirus compliance policy if Gears client is installed, running and reporting that the endpoint is compliant with the policy set in Gears Cloud. The next step will be to apply this policy to the Administrative and or User Realms as necessary.


System
Status
Configuration
Network
Clustering
Virtual Systems
IF-MAP Federation
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Authentication Realms >
Test_Realm
General
Authentication Policy
Role Mapping
Source IP
Browser
Certificate
Password
Host Checker
Limits
Allow users whose workstations meet the requirements specified by required host-checker policies. If no policies are selecte
will require and enforce the policy in order to login to this realm.
Evaluate Policies
Require and Enforce
Available Policies
All
342
360SafeAV

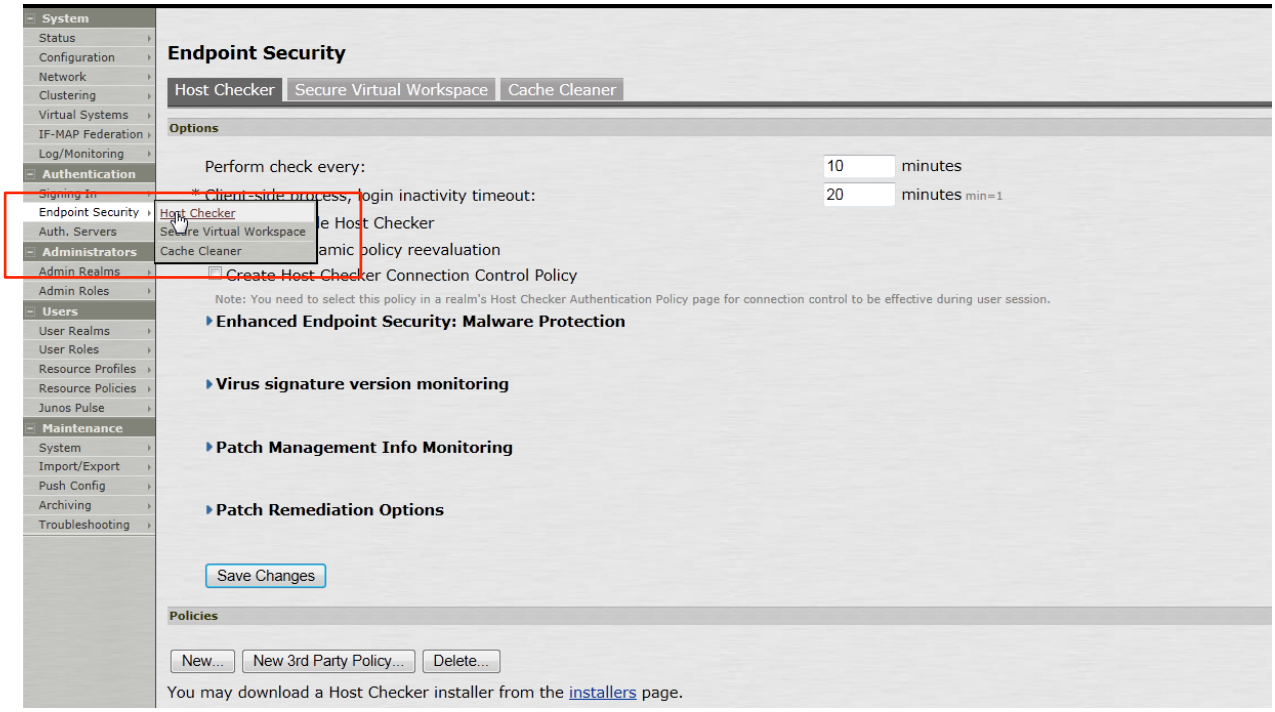
Method #2: Custom Process and Registry Check

Pulse Secure Host Checker can also be configured to utilize Gears for compliance checks using a combination of custom process and registry checks in the Endpoint Security/Host Checker portion of Junos Pulse. This requires more configuration than method #1, but has the benefit of also checking *to which* account/policy an endpoint is compliant.

Together, these checks will ensure that endpoint devices are meeting all compliance requirements established by the organization through the Gears admin console. The process check first ensures that the Gears Client is actively running on the device; second, the registry check determines whether the device is compliant with the defined Gears policy.

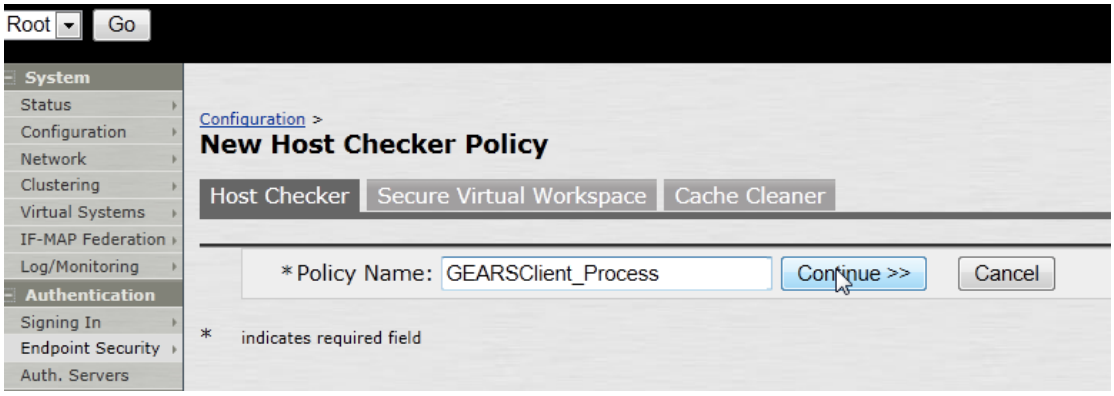
Step 1:

Under *Endpoint Security*, select the *Host Checker* tab.



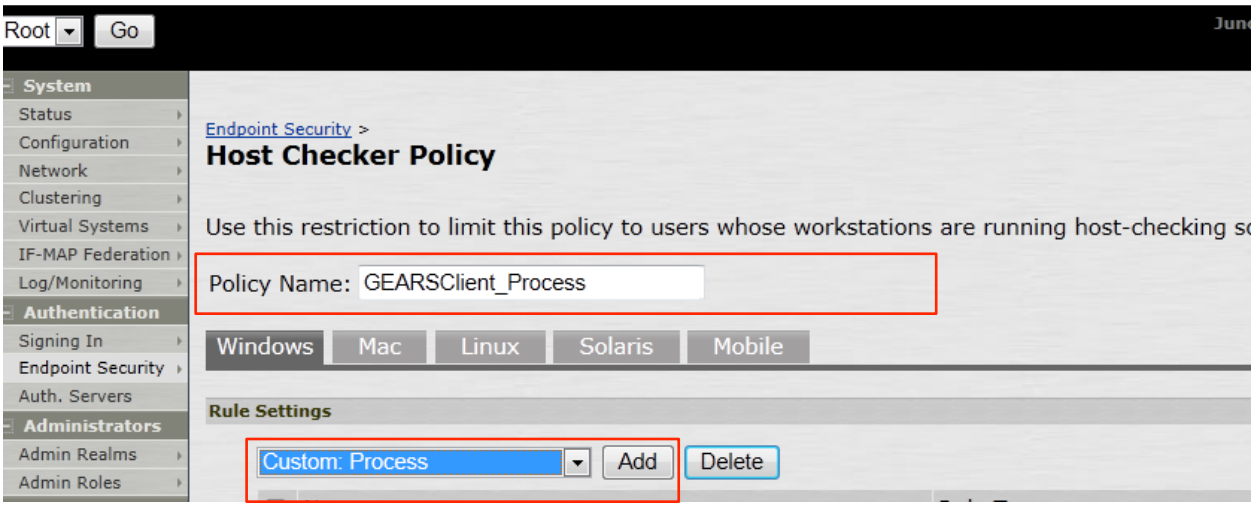
Step 2:

Under *Policies*, either create a New policy or Edit an existing one. When creating a new policy, users will be prompted to provide a policy name.



Step 3:

This step allows you to add a Custom Process. Please note that by default Windows will be selected. For the Mac configuration, select the *Mac* tab. Select *Customer: Process* from the drop down and click *Add*. Please note that for Mac devices within Host Checker Policy, you are currently only able to monitor the running Gears process, not the service.



Step 4:

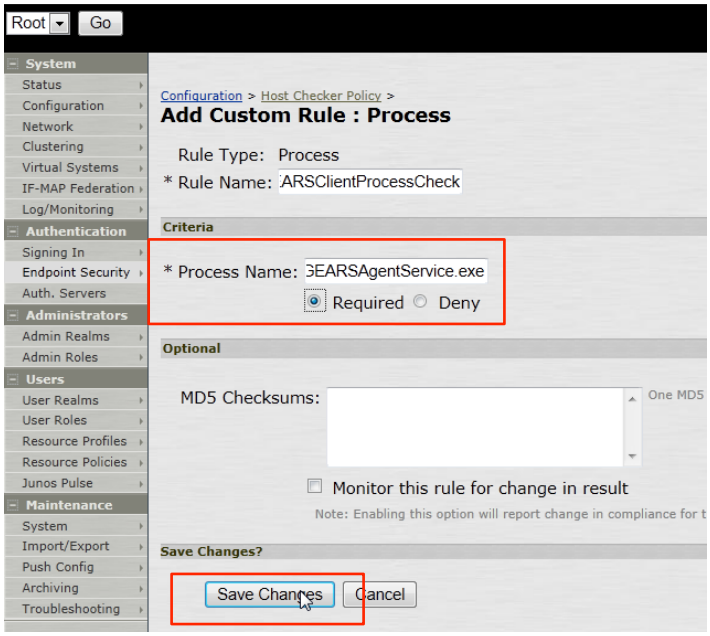
In Host Checker Policy we are creating a new custom rule. Here we will create the new rule name and add a requirement for the Gears process to be running.

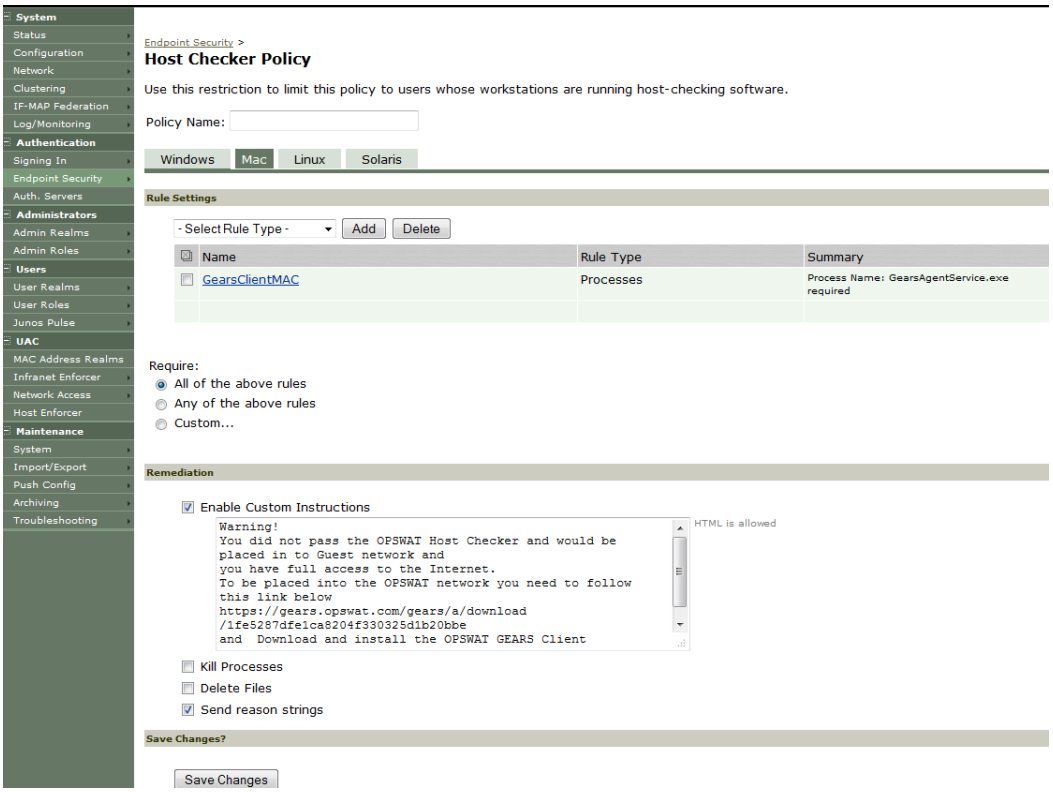
Windows

- **For the persistent, installed Gears client**, check for the process GEARSAgentService.exe
- **For the on demand, portable Gears client**, check for the process opswat-gears-od.exe

Mac

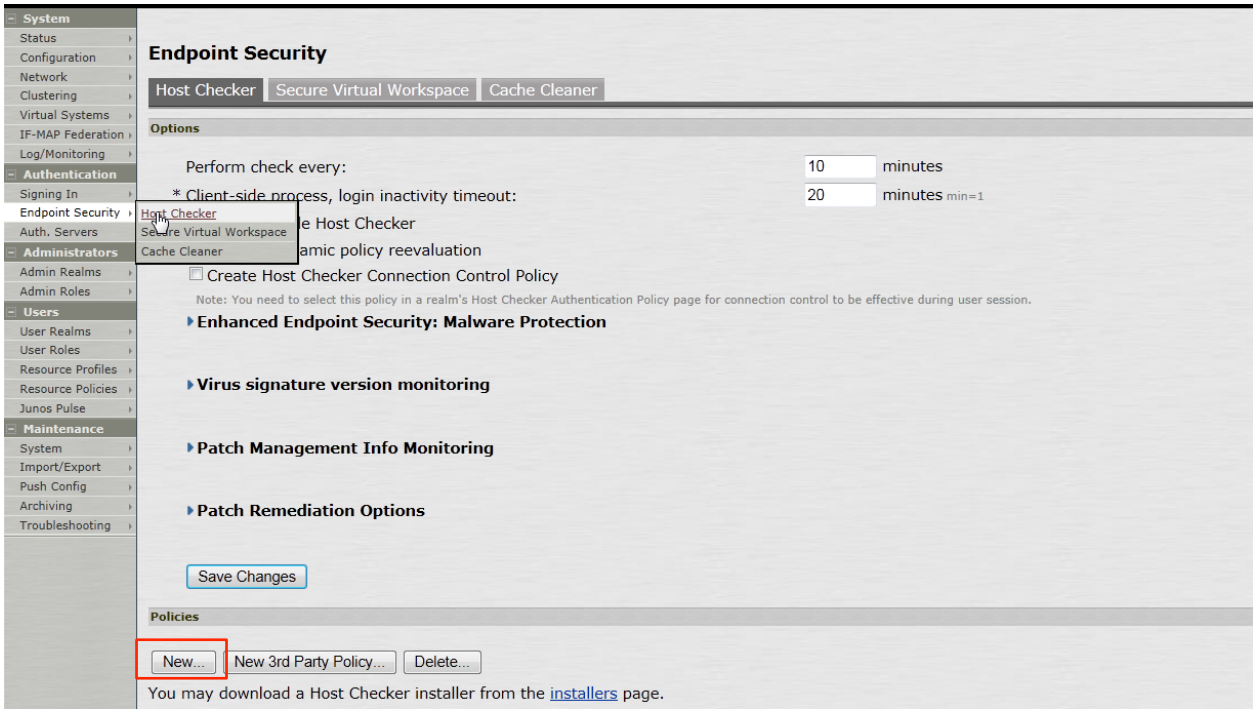
- **For the persistent, installed Gears client**, check for the process GearsAgent
- **For the on demand, portable Gears client**, check for the process opswat-gears-od





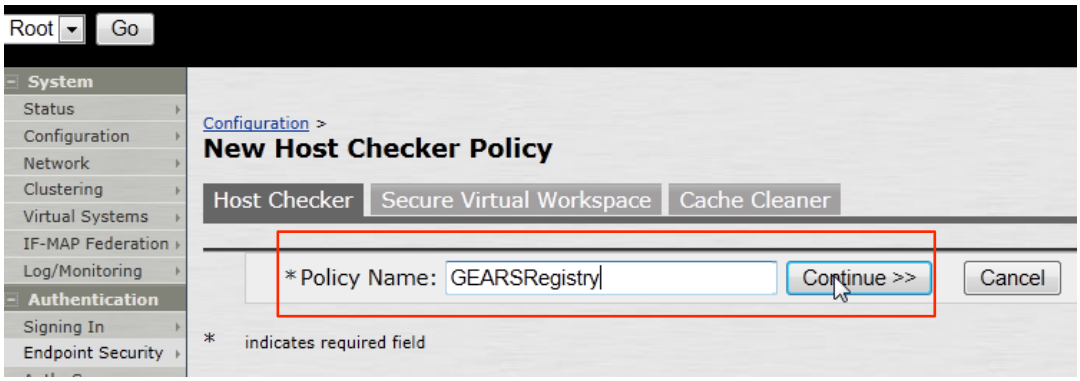
Step 5:

Once setup is complete click on *Save Changes,* then return to the Host Checker policy page.



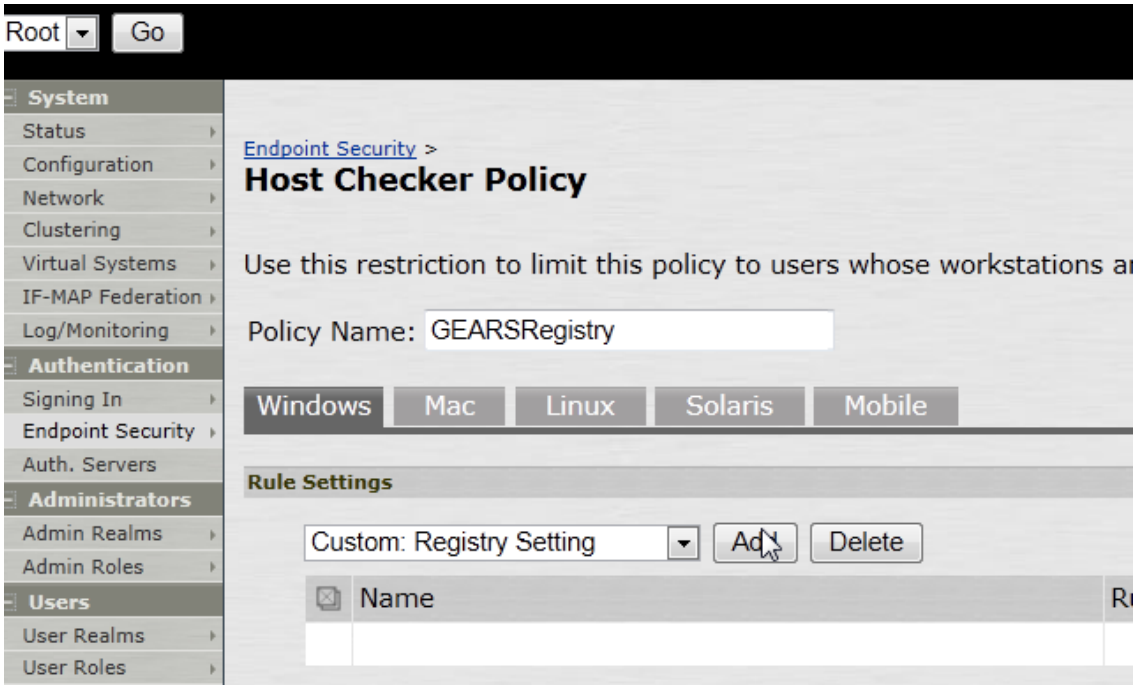
Step 6:

Under 'Policies', either create a new policy or edit an existing one. When creating a new policy, users will be prompted to provide a policy name.



Step 7:

This step allows you to create a Custom Registry Setting. Select *Custom: Registry Setting* from the drop down and click Add. By default *Windows* will be selected.



The following steps will outline the how to establish the registry check for both 32-bit and 64-bit Windows devices.

Step 8:

Establish the registry setting for the 64-bit system by first creating the rule name for the check. This name should be unique to designate the difference between the two checks. Now add requirements for the following Registry details.

Confirm the Registration Key on the Client matches the Account.

1. **For the persistent, installed Gears client:**
    - Registry root key – HKEY_LOCAL_MACHINE
    - Registry subkey – \SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Config
    - Name – RegistrationKey
    - Type – REG_SZ
    - Value should match the account Registration Key
2. **For the on demand, portable Gears client:**
    - Registry root key – HKEY_CURRENT_USER
    - Registry subkey – \SOFTWARE\OPSWAT\GEARS OnDemand\Config
    - Name – RegistrationKey
    - Type – REG_SZ
    - Value should match the account Registration Key

Check the Compliance state on the endpoint.

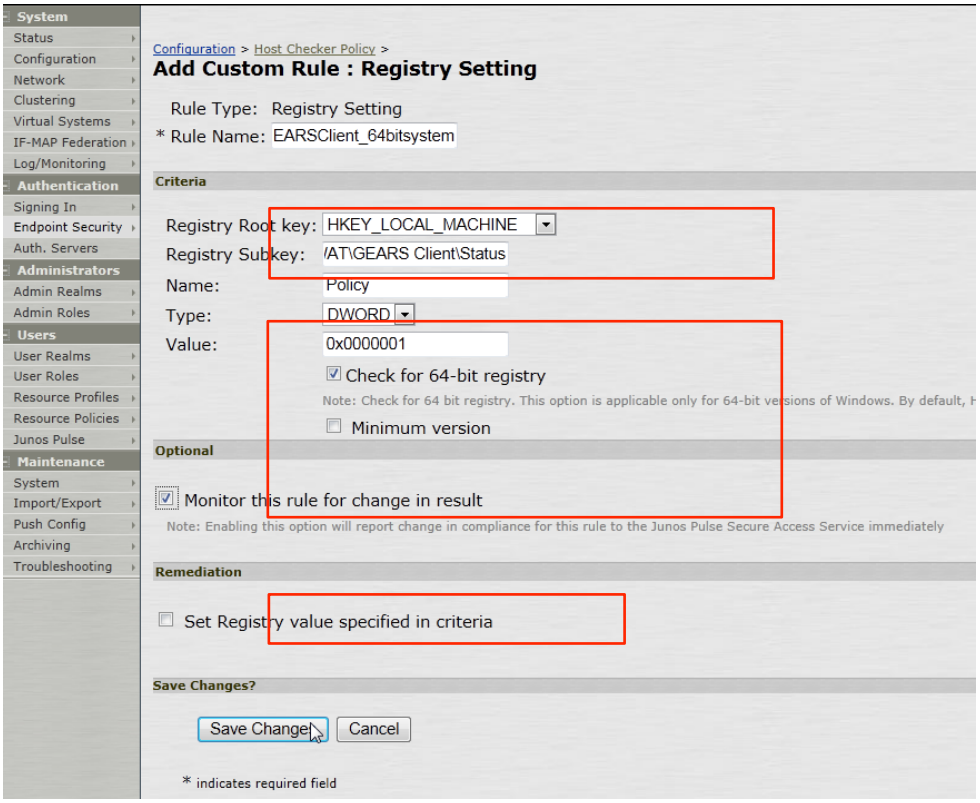
1. **For the persistent, installed Gears client:**
    - Root key – HKEY Local Machine
    - Subkey – \SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status
    - Name – Policy
    - Type – DWORD
    - Value – 0x0000000 (1)
2. **For the on demand, portable Gears client:**
    - Root key – HKEY Current User
    - Subkey – \SOFTWARE\OPSWAT\GEARS OnDemand\Config
    - Name – Policy
    - Type – DWORD
    - Value – 0x0000000 (1)

Policy Key Values:

a. 0 = NOT in compliance with policy, check Gars Cloud for details on the device
b. 1 = in compliance with policy, check Gears Cloud to view the defined policy

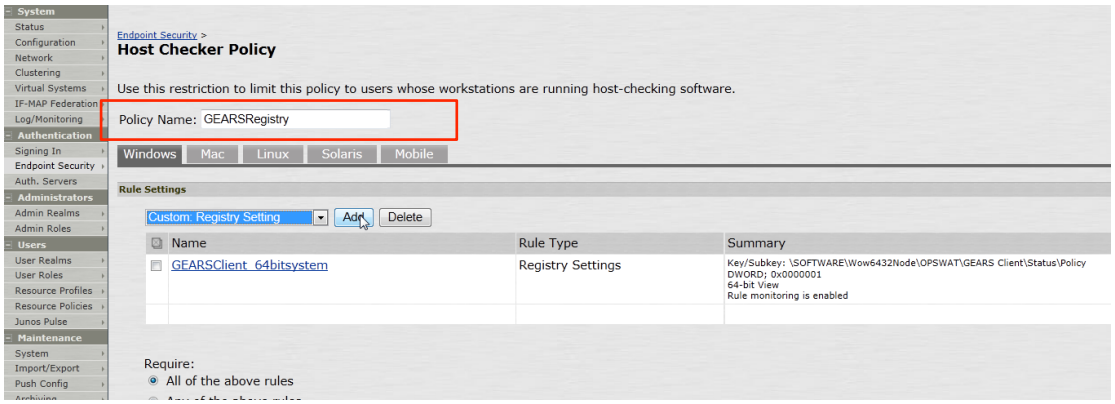
Save changes to enable the check for a 64-bit registry.

The combination of the two values, both Policy and Registration Key, ensure that the client installed is assigned to the Account that manages the defined Polices.



Step 9:

To create the 32-bit check, create a Custom Registry Setting. Select *Custom: Registry Setting* from the drop down and click Add.



Step 10:

Establish the registry setting for the 32-bit system by first creating the rule name for the check. This name should be unique to designate the difference between the two checks. Then add requirements for the following Registry details.

Confirm the Registration Key on the Client matches the Account.

1. **For the persistent, installed Gears client:**
    - Registry root key – HKEY_LOCAL_MACHINE
    - Registry subkey - HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Config
    - Name – RegistrationKey
    - Type – REG_SZ
    - Value should match the account Registration Key
2. **For the on demand, portable Gears client:**
    - Registry root key – HKEY_CURRENT_USER
    - Registry subkey – \SOFTWARE\OPSWAT\GEARS OnDemand\Config
    - Name – RegistrationKey
    - Type – REG_SZ
    - Value should match the account Registration Key

Check the Compliance state on the endpoint.

1. **For the persistent, installed Gears client:**
    - Root key – HKEY Local Machine
    - Subkey – \SOFTWARE \OPSWAT\GEARS Client\Status
    - Name – Policy
    - Type – DWORD
    - Value – 0x0000000 (1)
2. **For the on demand, portable Gears client:**
    - Root key – HKEY Current User
    - Subkey – \SOFTWARE\OPSWAT\GEARS OnDemand\Config
    - Name – Policy
    - Type – DWORD
    - Value – 0x0000000 (1)

Policy Key Values:

a. 0 = NOT in compliance with policy, check Gears Cloud for details on the device
b. 1 = in compliance with policy, check Gears Cloud to view the defined policy

The combination of the two values, both Policy and Registration Key, ensure that the client installed is assigned to the Account that manages the defined Polices.

Step 11:

For Mac devices, the client provides a file with the Registration Key and Policy value. To configure for the Mac:

1. Select the *Mac* tab within *Host Check Policy.*
2. Under *Rule Settings*, Select *Custom: Process*, the select *Add*.
3. Create a *New Process*
4. Add file:
    a. **For the persistent, installed Gears client:** *Applications/OPSWAT GEARS Client/Policies*.
    b. **For the on demand, portable Gears client:** */Users/username/Documents/OPSWAT/GEARS OnDemand*
5. Look for file named:
    a. **For the persistent, installed Gears client**: *GEARS_<gears license key>_<policy value>.txt*, where the *gears license key* will be where you add your *Account Registration Key*, and Policy Value would be 1 if the device passes the policy defined in the Gears dashboard.
    b. **For the on demand, portable Gears client**: GEARS_<gears license key>_<policy value>, where the gears license key will be where you add your Account Registration Key, and Policy Value would be 1 if the device passes the policy defined in the Gears dashboard.

This file includes a combination of two values, Policy and LicenseKey, to ensure that the client installed is assigned to the Account that manages the defined Polices.

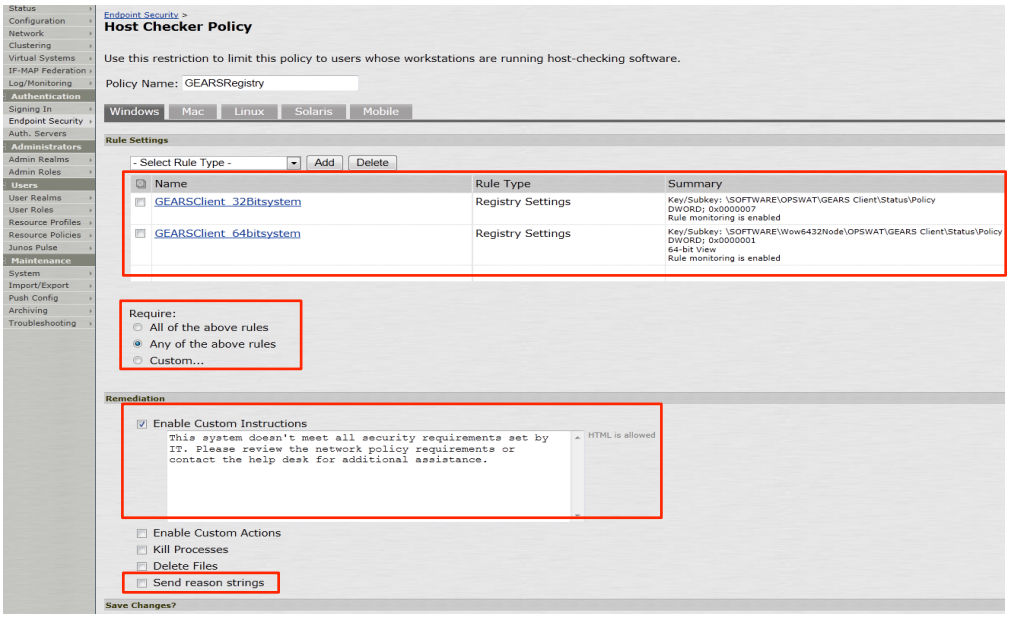
The Policy value will be defined as the following:

a. **0** = NOT in compliance with policy, check Gears Cloud for details on the device
b. **1** = in compliance with policy, check Gears Cloud to view the defined policy

Step 12:

To finalize the configuration of the Host Checker Policy, confirm the following:

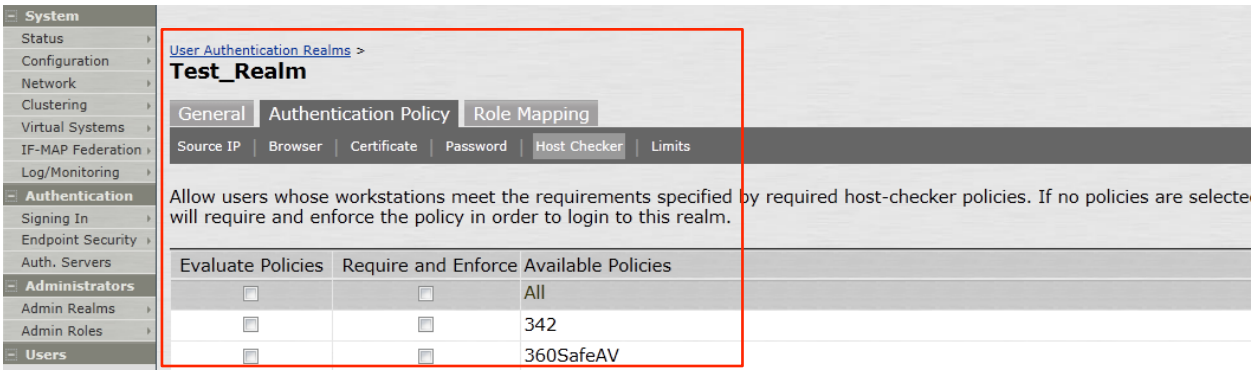
- Ensure that *Require* is checked with *Any of the Above Rules*
- Enable *Custom instructions* - The Custom Instructions should include a brief note on why a user may be running into issues passing this compliance check and next steps they may take.
- Disable *Send Reason Strings* - This will ensure that registry key information is not sent to the user and avoids further confusion.



Step 13:

Complete setup of any other requirements and save the changes. Once completed, this check will determine if Gears policies are being met by the endpoint device.

Host Checker is now setup for the Custom Process and Registry Compliance policies. The next step will be to apply these policies to the Administrative and or User Realms as necessary.



Method #3: Third Party Policy: Distribute Gears for Guest Devices

Gears for Guest Devices can be integrated with Pulse Secure Host Checker as a *third party policy*. With this option, Host Checker will cause Windows endpoints to download a ~3MB portable Gears client and perform an on-demand compliance and malware scan. When the VPN session is ended, the Gears client will automatically be deleted from the endpoint.

The portable Gears client must be manually uploaded (one-time) by the network admin to the Pulse Secure device. The format of the upload is a ZIP file with an INI for configurations, and a DLL for executing the process. **Automatic updates are not supported**. To update the client version, the network admin must download the latest Gears for Guest Devices client, put it in the ZIP package, and upload to the Pulse Secure device.

Method #3 **only** works with **Windows** endpoints.

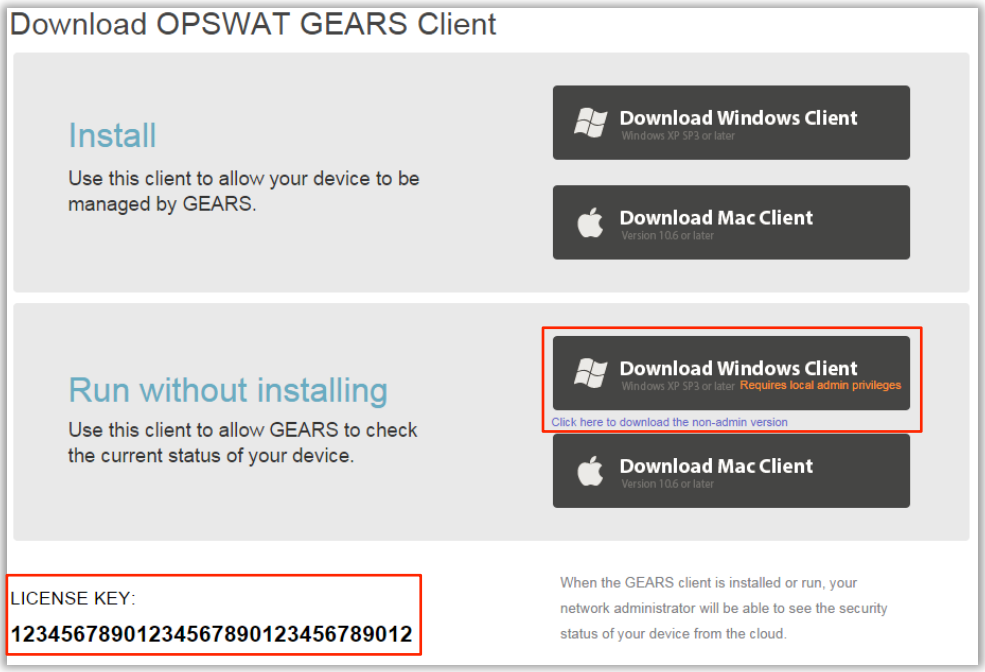
The screenshots included here are from a Pulse Secure SA2500 running 8.0R5.

Step 1: Download the third party policy

Contact OPSWAT to get a copy of the DLL

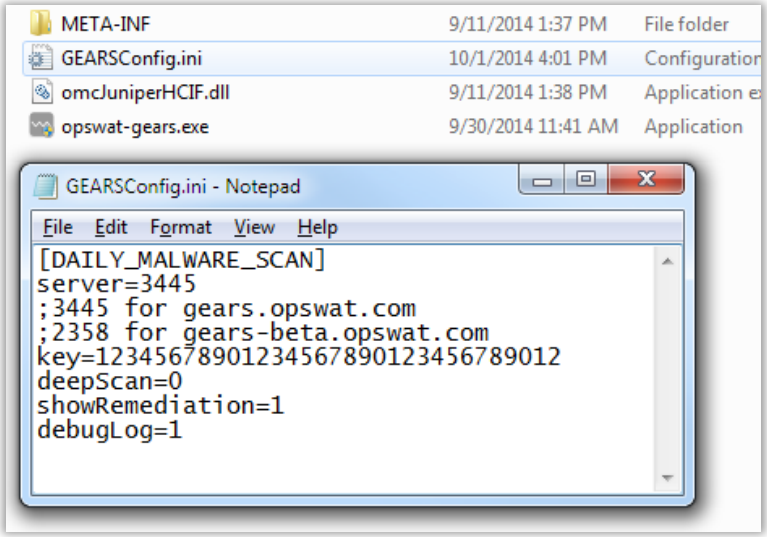
Step 2: Retrieve Gears portable EXE and license key

- Log in to your Gears account at www.opswatgears.com
- Go to the dashboard and click ***+ DEVICES*** in the header bar
- Click ***Enable Gears client on this device*** in the dialog box
- On the resulting page, copy down the license key displayed on the bottom left
- Download the Windows Client from *Run without installing* (admin or non-admin version)
- Rename the downloaded file opswat-gears.exe



Step 2: Prepare the policy package

- Unzip the file
- Move the downloaded gears-opswat.exe file into the directory
- Open *GEARSConfig.ini* in a text editor
- Change the configuration options
    - server: Which Gears environment you are using (regular or beta)
    - key: Your account license key
    - deepScan:
      0 – Malware scan only listed running processes;
      1 – Also scan linked libraries. Enabling this (1) increases scan time from < 60 seconds to ~2-3 minutes
    - showRemediation:
      0 – Only display summary remediation message in Pulse Secure webpage;
      1 – Also show detailed and user-friendly self-remediation instructions in a new webpage
    - debugLog:
      0 – Disable debug log on local machine
      1 – Enable debug log on local machine (log is deleted when session ends)

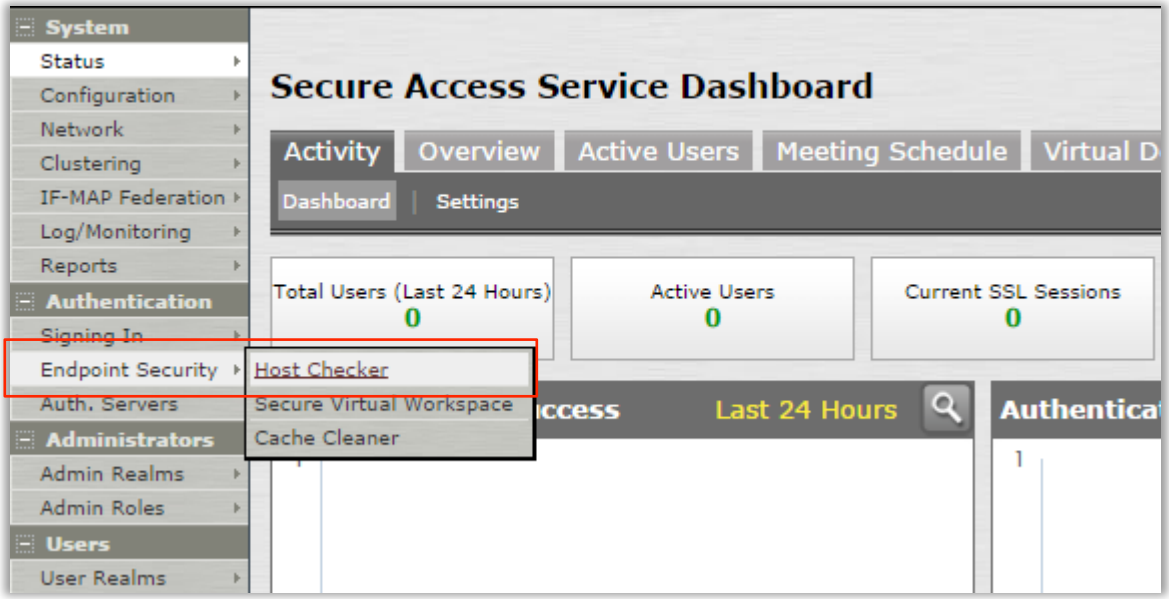


Step 3: Rezip the package

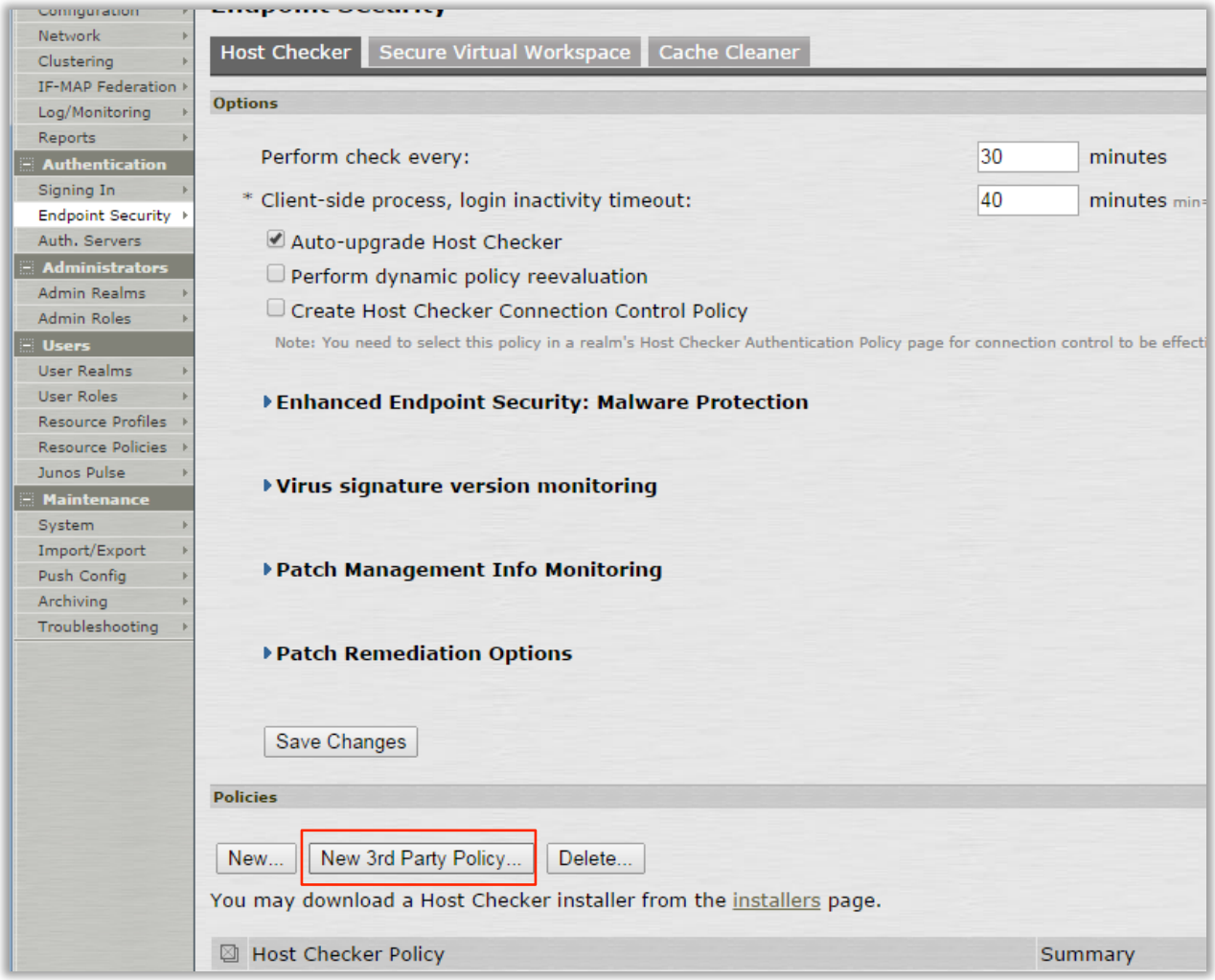
Rezip the package, without further changing any files names or folder structure. The zip file itself can be given any name. Expected package contents:

META-INF/MANIFEST.HCIF
GEARSConfig.ini
omcJuniperHCIF.dll
opswat-gears.exe

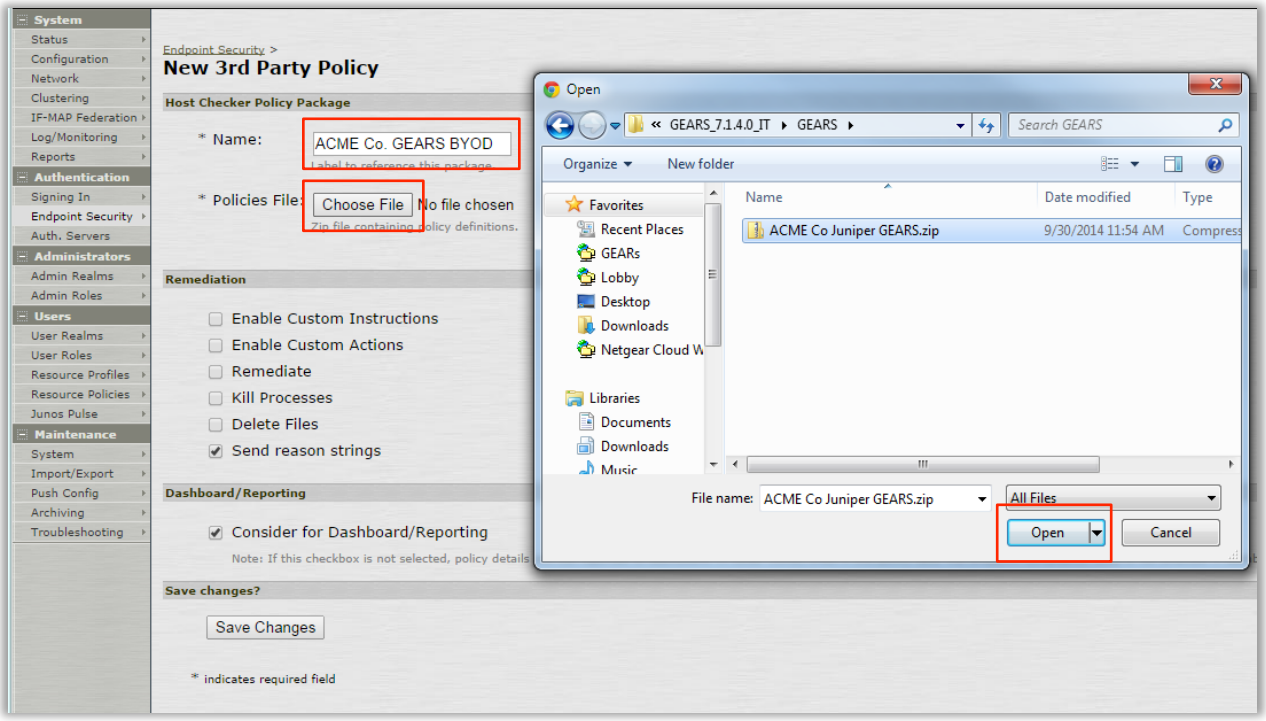
Step 4: Log in to Pulse Secure console, Navigate to *Endpoint Security* > *Host Checker*



Step 5: Create a *New 3rd Party Policy*

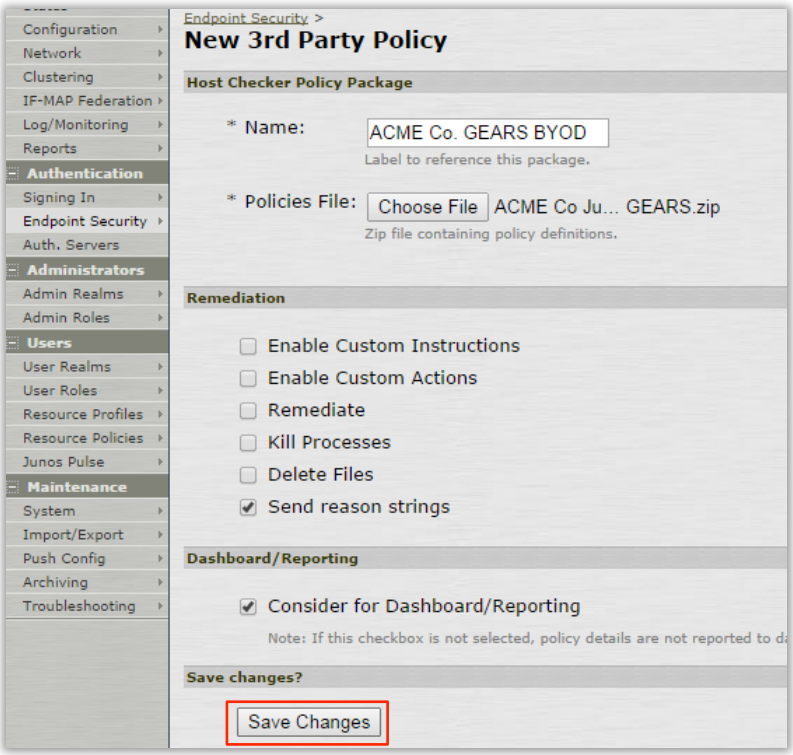


Step 6: Name the policy and upload the ZIP package



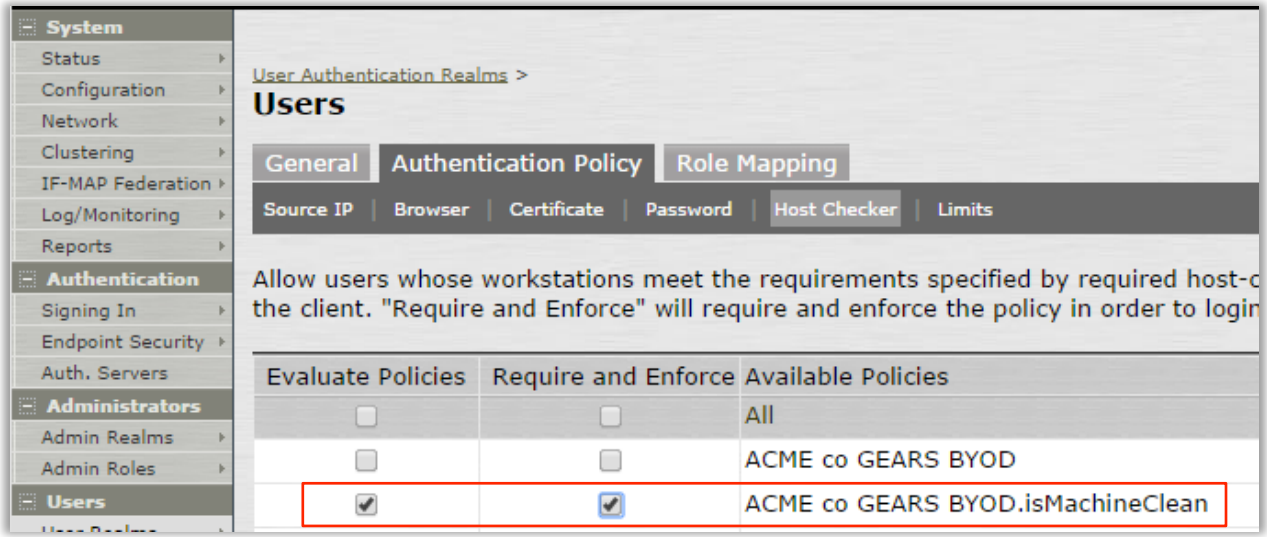
Step 7: Click 'Save Changes'

Leave *Remediation* options at default settings



Step 8: Assign the Host Checker Policy to a User Realm

(Using a User Realm that you have already created) Assign the new Host Checker Policy to the target User Realm. The policy to use will be called <Name Given in Step 6>.isMachineClean



For more information, or if you have any questions about the steps above, please log into the OPSWAT Portal at https://portal.opswat.com and submit a ticket to request assistance from our support team.