

How to set up Portnox with OPSWAT GEARS

About This Guide 2

Portnox Compliance Policy Creation 3

Compliance Policy Creation: GEARS Compliance on Windows 4

Compliance Policy Creation: GEARS Compliance on Mac 7

Manual Steps to enter GEARS license key 10

Additional settings for GEARS on-demand 13

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 <http://www.opswatgears.com>.

GEARS can be leveraged by Portnox policies to provide enhanced compliance checking capabilities.

GEARS Client stores device compliance status in the Windows Registry or Mac OS p-list. This compliance information is generated by either GEARs client type: the persistent installed version, or the dissolvable version. Portnox can access and use this information through custom Portnox policies to determine if a device should be granted network access. More information on Portnox can be found at <http://www.portnox.com>.

This guide specifically illustrates how to establish GEARs policy checks for Windows and Mac OS devices through Portnox NAC. This guide assumes you have access to the Portnox configuration manual and have a basic understanding of Portnox policy creation.

©2015 OPSWAT, Inc. All rights reserved. OPSWAT, GEARs and the OPSWAT logo are trademarks of OPSWAT, Inc. Portnox is a trademark of Access Layers Inc. All other trademarks, trade names, service marks, service names and images mentioned and/or used herein belong to their respective owners.



Portnox Compliance Policy Creation

The guide provides information on how to create Portnox compliance policies to evaluate GEARS status on an endpoint. For each non-compliant status you are able to define the appropriate action to take.

The following are the possible results for compliancy check of the OPSWAT GEARS client:

- a. Not Installed
- b. Not Running
- c. Not Compliant
- d. Compliant

Upon each of the above results you can define a reaction policy to perform an action, for example:

1. Alert the administrator via an email
2. Quarantine the endpoint by changing the VLAN
3. Forward the event via syslog to Help Desk / SIEM
4. Present captive portal page for users without GEARS with manual installation instructions
5. Perform installation of GEARS on endpoint that does not have it
6. Activate GEARS on endpoint if not running

Compliance Policy Creation: GEARS Compliance on Windows

Using Portnox version 2.4 update 1, GEARS client is one of the pre-defined products and can be chosen from the list of available products. Prior versions can use the update script from the Portnox support site or manually define the product using the product configuration tool.

Creating a GEARS policy for Windows endpoints:

- 1) Add to an existing security model the GEARS client compliance check, or create a new security model from Enforce→Policy→Compliance Tab, enter a name and press add:

The screenshot shows the Portnox EnforceRules.aspx web interface. The 'compliance' tab is selected. The table below shows one rule: 'all network: 1 model'. The 'add new' form at the bottom is filled out with the following values:

field	value
hive	all network
comment	GEARS security mode
affected ports	location
location	select location
vlan	select vlan
general	general
model name	GEARS
os	select os
group	select group
auth. scheme	select auth
action	monitor
alerts	event viewer, sysLog, email

2) Add the GEARS product to the security model:

nas config **enforce** setup inventory status help | policy portnox

re-install cancel save

rules reactions compliance

no.	product	failures	affected ports	action	alerts
✓	all network: 2 models				
✓	general (all network): 2 models				
➤	patches: 1 product monitor				
✓	GEARS: 0 products monitor				

remove selected edit add

⚠ restrict and/or preconnect are defined for this rule

add new

product OPSWAT GEARS action select action alerts

failure any failure

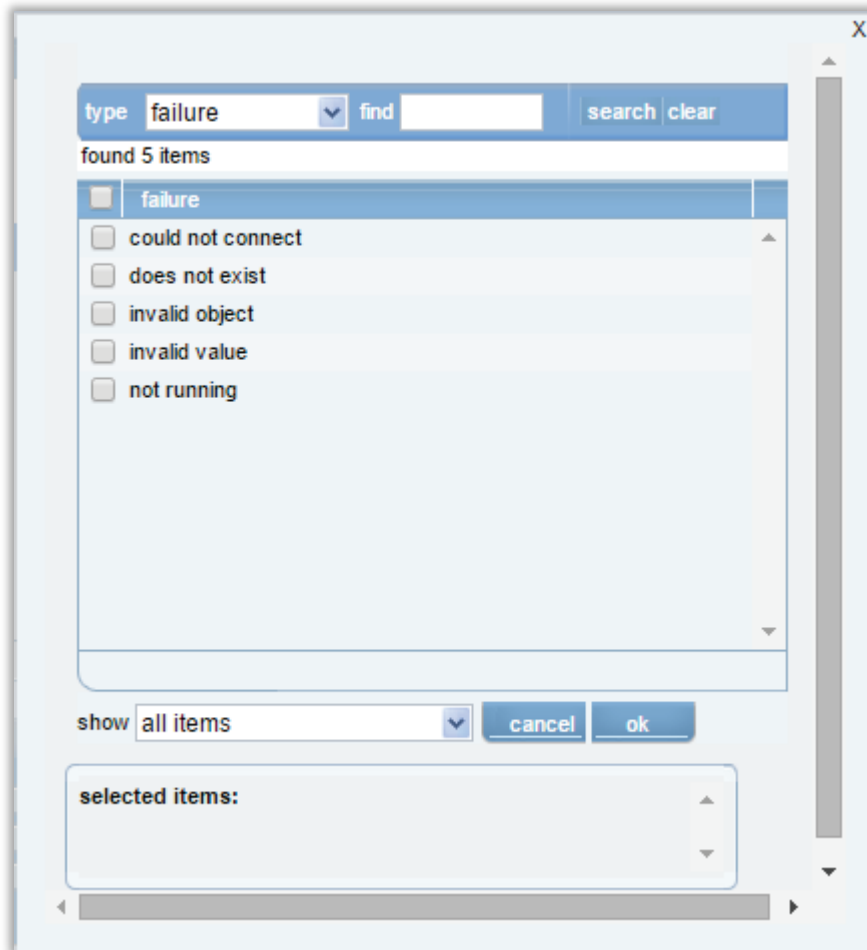
event viewer ...

sysLog ...

email ...

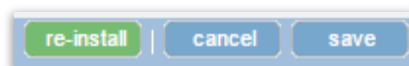
cancel add

3) Choose the relevant event to act upon:



Where:

- a. Could not connect – Could not perform the check due to an error with the remote endpoint connection
 - b. Does not exist – GEARS is not installed
 - c. Invalid object – Not applicable for GEARS
 - d. Invalid value – GEARS is not compliant*
 - e. Not running – GEARS is not running*
- 4) * **GEARS actively protects** the compliance information stored in the registry and p-list, but only as long as GEARS is running. Therefore, it's **preferred** to always check that GEARS is running in **conjunction** with whether GEARS is compliant. Choose the relevant action to take, either an existing one or create a new one at Config→Action.
- 5) Repeat the above 2-4 for each event you wish to consider
- 6) Click Save and reinstall:



Compliance Policy Creation: GEARS Compliance on Mac

Using Portnox version 2.4 Update 1, GEARS client is included in the pre-defined scripts for MAC OS compliance verification. Prior versions can use the update script from the Portnox support site or manually define the product by editing an existing one.

Creating a GEARS policy for MAC endpoints:

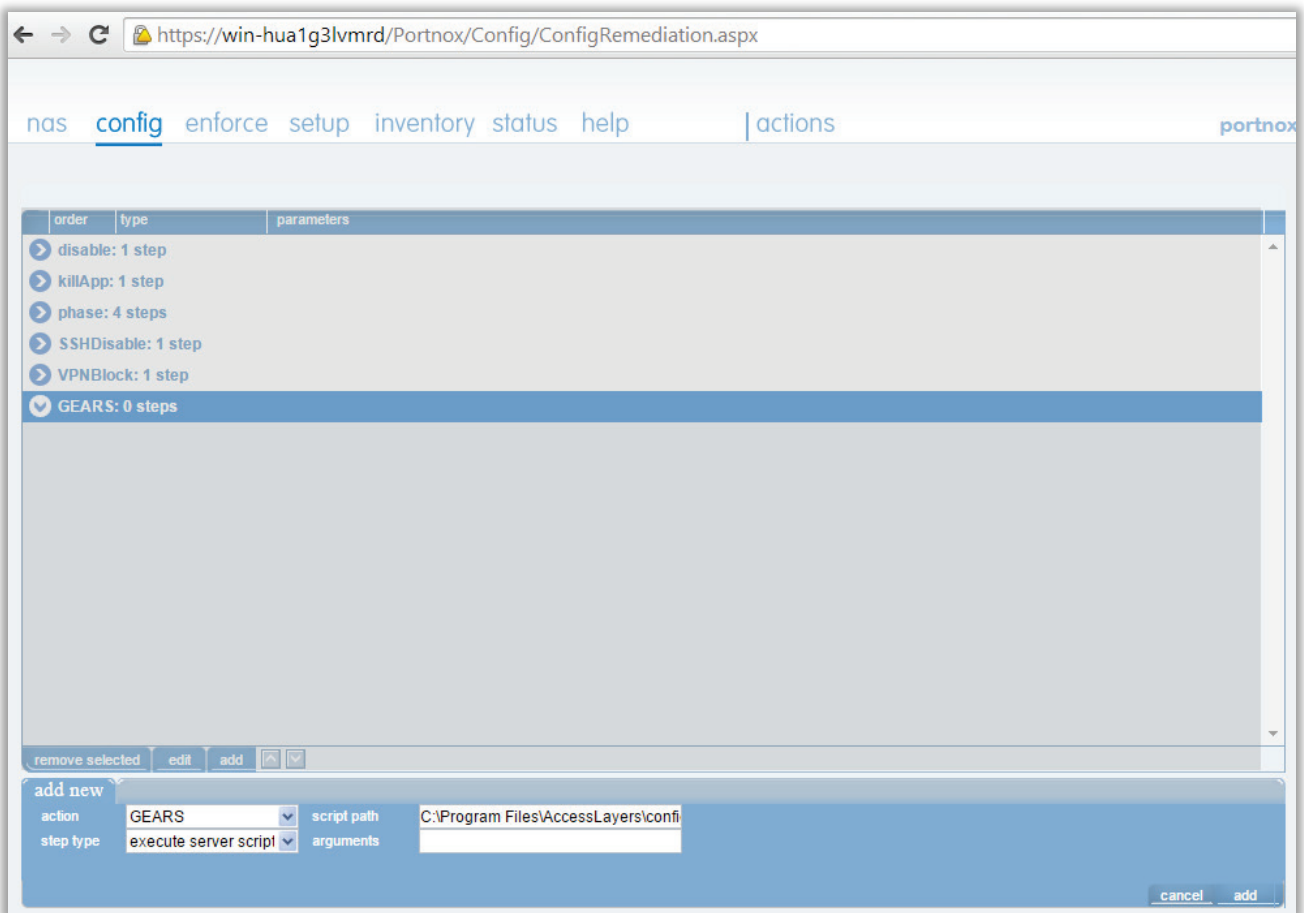
- 1) Define the Mac OS GEARS compliance action at Config→Actions:

The screenshot shows a web browser window with the URL <https://win-hua1g3lvmrdr/Portnox/Config/ConfigRemediation.aspx>. The page has a navigation bar with links: nas, config, enforce, setup, inventory, status, help, and actions. The 'inventory' tab is active, displaying a table with columns 'order', 'type', and 'parameters'. The table contains five rows of actions, each with a right-pointing arrow icon:

order	type	parameters
>	disable: 1 step	
>	killApp: 1 step	
>	phase: 4 steps	
>	SSHDisable: 1 step	
>	VPNBlock: 1 step	

Below the table is a toolbar with 'remove selected', 'edit', 'add', and a dropdown arrow. An 'add new' dialog box is open at the bottom, with fields for 'name' (containing 'GEARS') and 'retries' (containing '3'). The dialog has 'cancel' and 'add' buttons.

- 2) Highlight the newly create GEARS action and press add, in order to add the GEARS specific compliance check:



- 3) Insert the MAC OS GEARs compliance check into the policy at Policy→Enforce→reaction, choose Mac OS for the OS, device authenticated for the event and the Action of GEARs for the compliance check

The screenshot shows the Portnox EnforceRules.aspx web interface. The top navigation bar includes links for 'nas', 'config', 'enforce', 'setup', 'inventory', 'status', 'help', and a 'policy' dropdown. The 'enforce' tab is active. Below the navigation bar, there are buttons for 're-install', 'cancel', and 'save'. The main content area has tabs for 'rules', 'reactions', and 'compliance'. The 'rules' tab is selected, showing a table with columns: 'no.', 'event', 'affected ports', 'action', 'alerts', 'auth scheme', and 'os'. A single rule is listed with 'all network' as the event. Below the table, there are buttons for 'remove selected', 'edit', and 'add'. A warning message states: 'restrict and/or preconnect are defined for this rule'. The 'add new' form is displayed below the warning. It includes fields for 'hive' (set to 'all network'), 'comment', 'affected ports' (with radio buttons for 'location', 'vlan', and 'general'), 'event' (set to 'device authentication'), 'os' (set to 'Mac OS'), 'auth' (set to 'all auth'), 'action' (set to 'GEARS'), and 'alerts' (with checkboxes for 'event viewer', 'sysLog', and 'email'). The 'add' button is at the bottom right of the form.

The actual Portnox enforcement action is defined inside the Mac OS script.

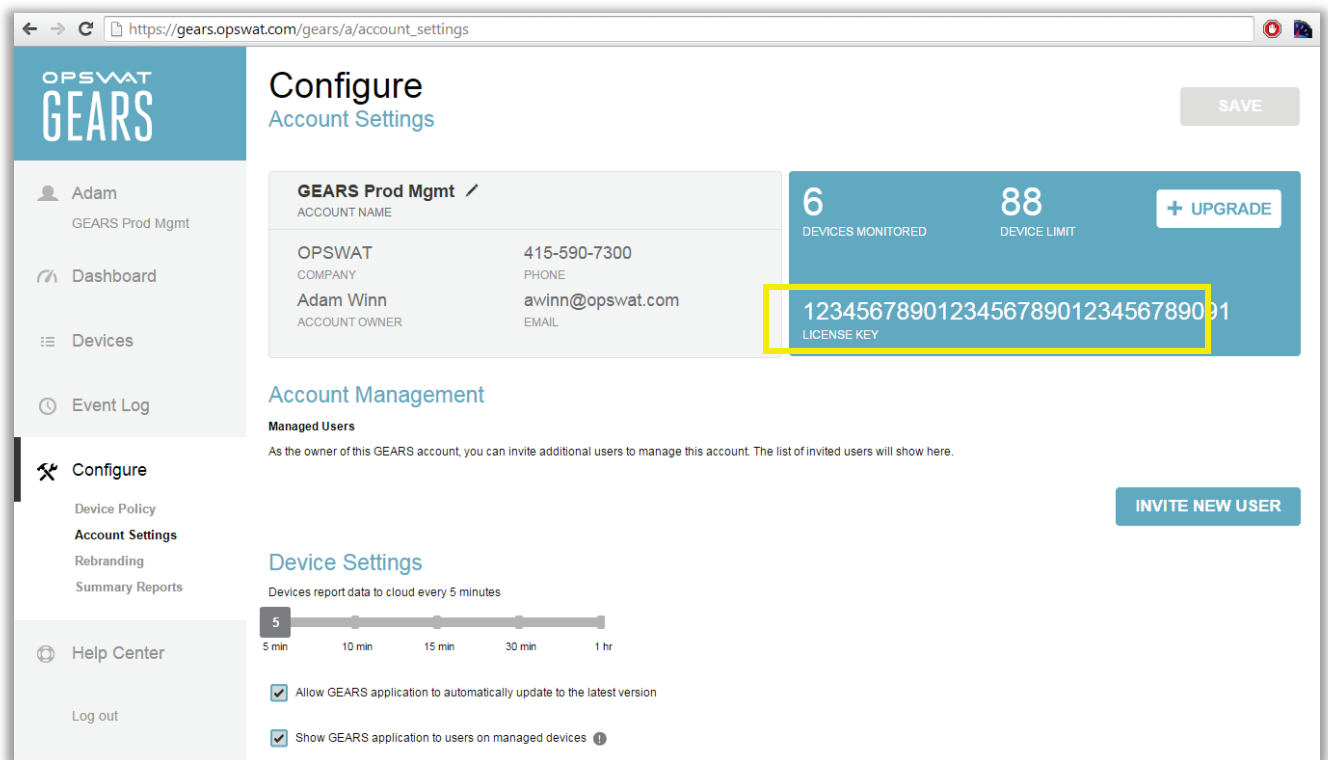
- 4) Click Save and reinstall:

A close-up of the buttons at the top right of the Portnox EnforceRules.aspx interface. There are three buttons: 're-install' (green), 'cancel' (blue), and 'save' (blue).

Manual Steps to enter GEARS license key

Portnox provides the above pre-defined compliance product policies to make configuration as easy as possible. GEARS itself provides enhanced endpoint compliance information, and this is configured in each GEARS account. GEARS accounts have a unique license key, and this must be manually entered into the Portnox configuration.

After creating a GEARS account at <https://www.opswatgears.com/>, log in and go to **Configure** → **Account Settings**. The license key will be visible on the top-right portion of the page.



This GEARS license key is **uniquely** tied your GEARS compliance policy.

After obtaining your GEARS license key, open the Portnox Deployment Helper Tool and perform the following steps:

- 1) Open the product definition page: Tools → Compliance → Manage Products, select the GEARS product from the combo box:

Manage Products

Products

Name:

Check Definition

Name: @OPSWAT Type: Value Type:

Operator: Expected Value: Delta:

Reg Value: Operating System: Regular Expression:

Service Name:

Category:

Order	Name	Type	Operator	Value Type	Regular Expr.	Expected Value	Reg Value	Key Name
Installed								
47	Install@OPSWAT ...	Value	Exists	String			RegistrationKey	SOFTWARE\OPSWAT\GEARS Client\Config
48	Install64@OPSWAT ...	Value	Exists	String			RegistrationKey	SOFTWARE\Wow6432Node\OPSWAT\...
Running								
44	Service@OPSWAT...	RunningSe...	State	Object		Started		OPSWATGEARClient
Updated								
45	Compliance32@O...	Data	Equal	Number		1	Policy	SOFTWARE\OPSWAT\GEARS Client\Status
46	Compliance64@O...	Data	Equal	Number		1	Policy	SOFTWARE\Wow6432Node\OPSWAT...

- 2) Expand the installed group and change the “Install” and “Install64” checks to verify the exact GEARS License Key. To quickly identify these, look for RegistrationKey in the ‘Reg Value’ column. Taking the GEARS License Key you copied earlier, paste it into the ‘Expected Value’ form field, and make the other changes as shown here:

The screenshot shows the 'Manage Products' window with the 'Check Definition' section. The 'Name' field is set to 'Install@OPSWAT'. The 'Type' is 'Data', 'Value Type' is 'String', and 'Operator' is 'Equal'. The 'Reg Value' is 'RegistrationKey' and the 'Key Name' is 'HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Config'. The 'Expected Value' field is highlighted in yellow. The 'Category' is 'Installed'.

Order	Name	Type	Operator	Value Type	Regular Expr.	Expected Value	Reg Value	Key Name
47	Install@OPSWAT ...	Value	Exists	String			RegistrationKey	SOFTWARE\OPSWAT\GEARS Client\Config
48	Install64@OPSWAT ...	Value	Exists	String			RegistrationKey	SOFTWARE\Wow6432Node\OPSWAT\...
44	Service@OPSWAT...	RunningSe...	State	Object		Started		OPSWATGEARSCient
45	Compliance32@O...	Data	Equal	Number		1	Policy	SOFTWARE\OPSWAT\GEARS Client>Status
46	Compliance64@O...	Data	Equal	Number		1	Policy	SOFTWARE\Wow6432Node\OPSWAT...

The screenshot shows the 'Manage Products' window with the 'Check Definition' section. The 'Name' field is set to 'Install64@OPSWAT'. The 'Type' is 'Data', 'Value Type' is 'String', and 'Operator' is 'Equal'. The 'Reg Value' is 'RegistrationKey' and the 'Key Name' is 'HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\OPSWAT\Gears Client\Config'. The 'Expected Value' field is highlighted in yellow. The 'Category' is 'Installed'.

Order	Name	Type	Operator	Value Type	Regular Expr.	Expected Value	Reg Value	Key Name
60	Install@O...	Value	Exists	String			RegistrationKey	SOFTWARE\OPSWAT\GEARS Client\Config
61	Install64...	Value	Exists	String			RegistrationKey	SOFTWARE\Wow6432Node\OPSWAT\...

- 3) In order for the change to take effect, go back to the Web GUI and from Enforce → Policy, click Save and reinstall:

The screenshot shows three buttons: 're-install' (green), 'cancel' (blue), and 'save' (blue).

Additional settings for GEARS on-demand

For the on-demand GEARS client some minor modifications may be needed in the Portnox configuration, those changes are presented in the table below. Many GEARS deployments make use of both the persistent and on-demand clients, so it is advisable to use **OR** operators when developing a Portnox policy that supports both client types. A similar configuration exists by default in the Portnox policy to support GEARS on both 32-bit and 64-bit operating systems. That use of the **OR** operator can be used as a guide.

WINDOWS		
	MANAGED (PERSISTENT)	GUEST (ON DEMAND)
Process Name	GearsAgentService.exe	opswat-gears-od.exe
Service Name	OPSWAT GEARS Client	n/a

REGISTRY ENTRY: INSTALLATION & LICENSE KEY		
Registry Root Key	HKEY_LOCAL_MACHINE	HKEY_CURRENT_USER
Subkey, 32-bit	\SOFTWARE\OPSWAT\GEARS Client\Config	\SOFTWARE\OPSWAT\GEARS OnDemand\Config
Subkey, 64-bit	\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Config	\SOFTWARE\OPSWAT\GEARS OnDemand\Config
Key Name	----- RegistrationKey -----	
Key Type	----- REG_SZ -----	
Key Value	----- GEARS Account License Key -----	

REGISTRY ENTRY: COMPLIANCE STATE		
Registry Root Key	HKEY_LOCAL_MACHINE	HKEY_CURRENT_USER
Subkey, 32-bit	\SOFTWARE\OPSWAT\GEARS Client\Status	\SOFTWARE\OPSWAT\GEARS OnDemand\Config
Subkey, 64-bit	\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status	\SOFTWARE\OPSWAT\GEARS OnDemand\Config
Key Name	----- Policy -----	
Key Type	----- DWORD -----	
Key Value	----- 0=Not Compliant 1=Compliant -----	

MAC		
	MANAGED (PERSISTENT)	GUEST (ON DEMAND)
Process Name	GearsAgent	GearsAgent
Log File Location	Applications/OPSWAT GEARS Client/Policies	/Users/<username>/Documents/OPSWAT/GEARS OnDemand
File Name	----- GEARS_<license key>_<policy value>.txt -----	
<license key>	----- Should match license key for the desired account -----	
<policy value>	----- 0=Not Compliant 1=Compliant -----	

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

