How to set up ForeScout CounterACT 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 http://www.opswatgears.com.

GEARS can be leveraged by ForeScout's CounterACT policies to provide enhanced compliance checking capabilities. Once you have deployed the GEARS Client to your devices and configured your compliance policy through the GEARS configuration page, the GEARS Client will store the device's compliance status in the Windows Registry or Mac OS p-list. ForeScout CounterACT can access and use this information through custom policies to determine if a device should be granted network access.

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

Custom Policy Creation

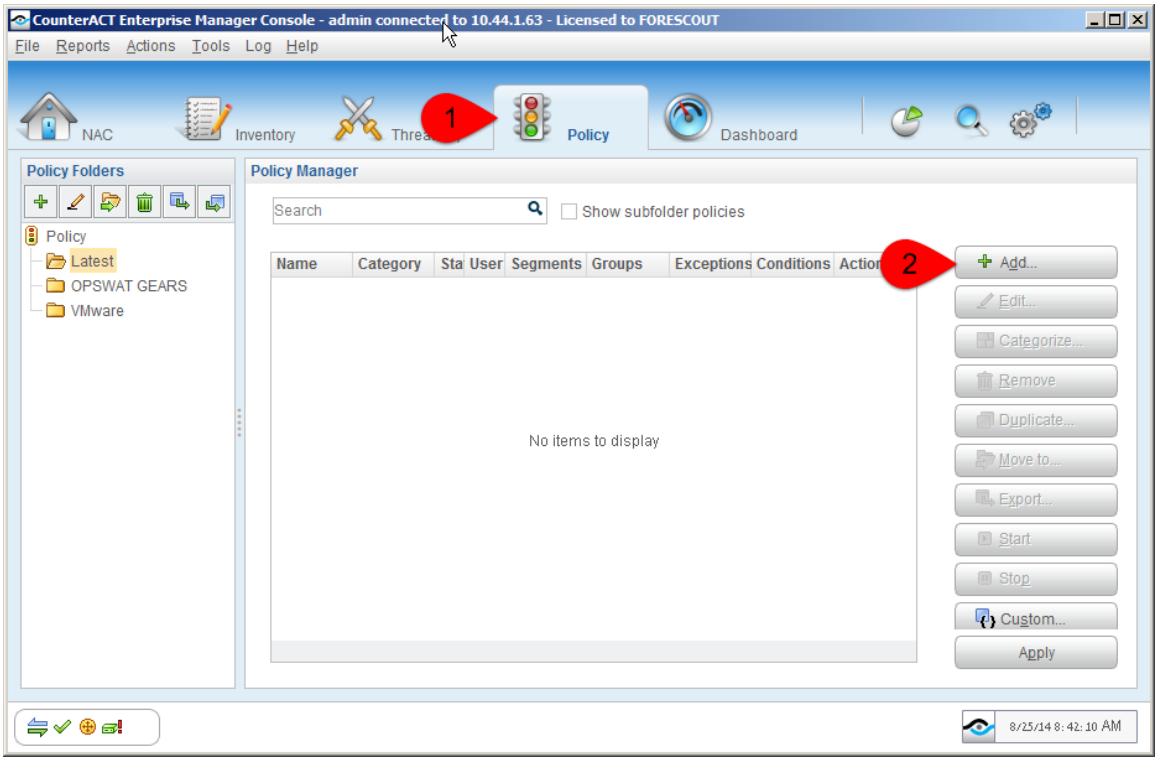
The guide provides information on how to create the policies with appropriate conditions. Each rule in the policy may have actions associated with it that are determined by corporate policy. You are expected to add actions to each sub-rule that are appropriate to your corporate policies. For example, you might want to:

1. Create groups for each rule such that as a result of these policies, endpoints end up in groups, and then have separate policies that act on these groups. The groups may be;
    a. GEARS Compliant
    b. GEARS Not Compliant
    c. GEARS Not Running
    d. GEARS Not Installed
2. Perform direct actions on non-compliant endpoints, for example:
    a. Send an email to the administrator
    b. Assign non-compliant endpoints to a quarantine VLAN
    c. Hijack the web browsing session of users not running GEARS and provide installation instructions
    d. Run an installation script on endpoints that do not have GEARS installed
    e. Run a script to start the application on endpoints which have GEARS installed but not running

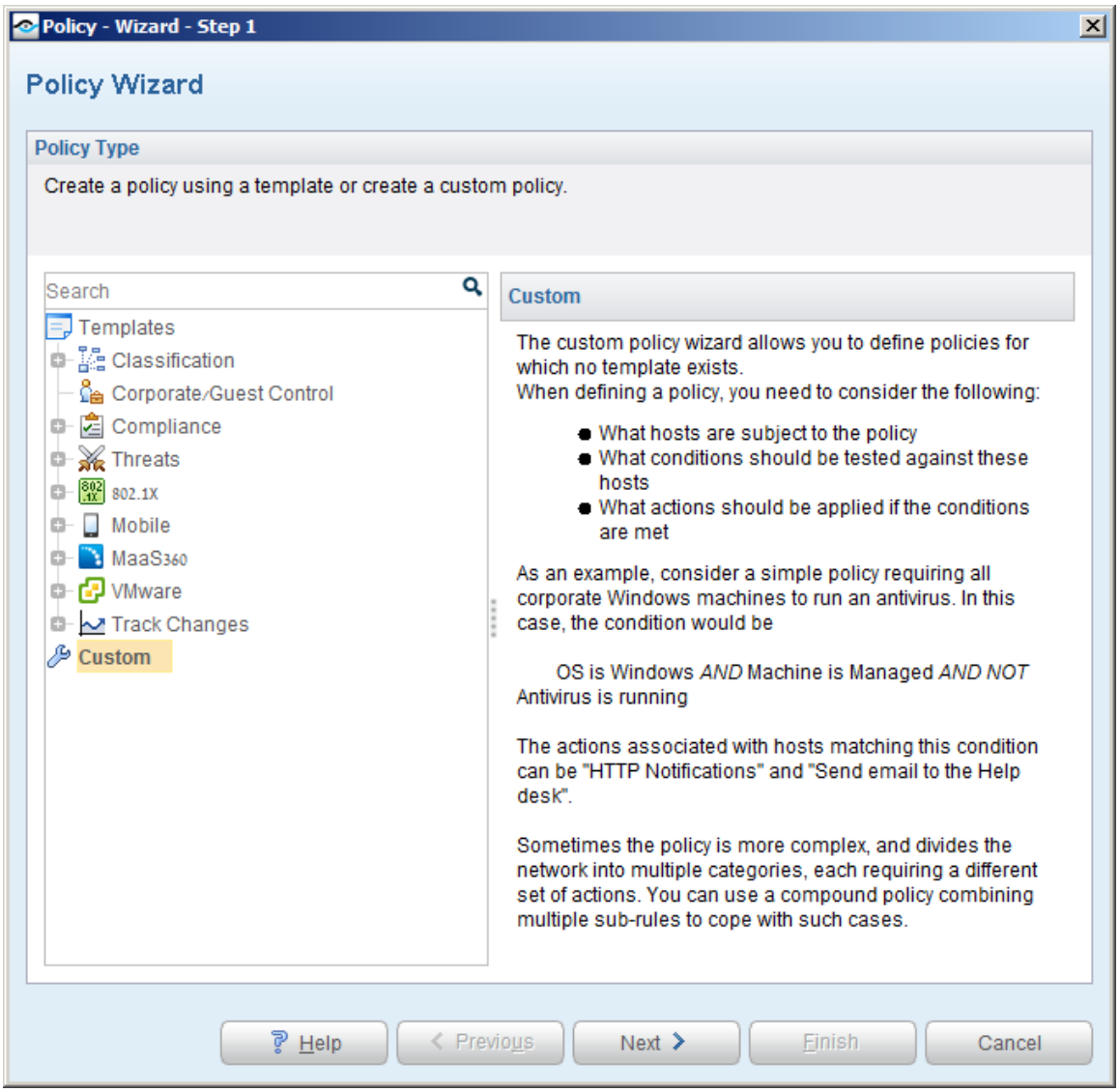
GEARS Compliance on Mac

Using CounterACT, you can create a policy which will analyse Mac computers for GEARS compliance, as follows (the steps shown are for a managed device. See appendix for differences on guest devices):

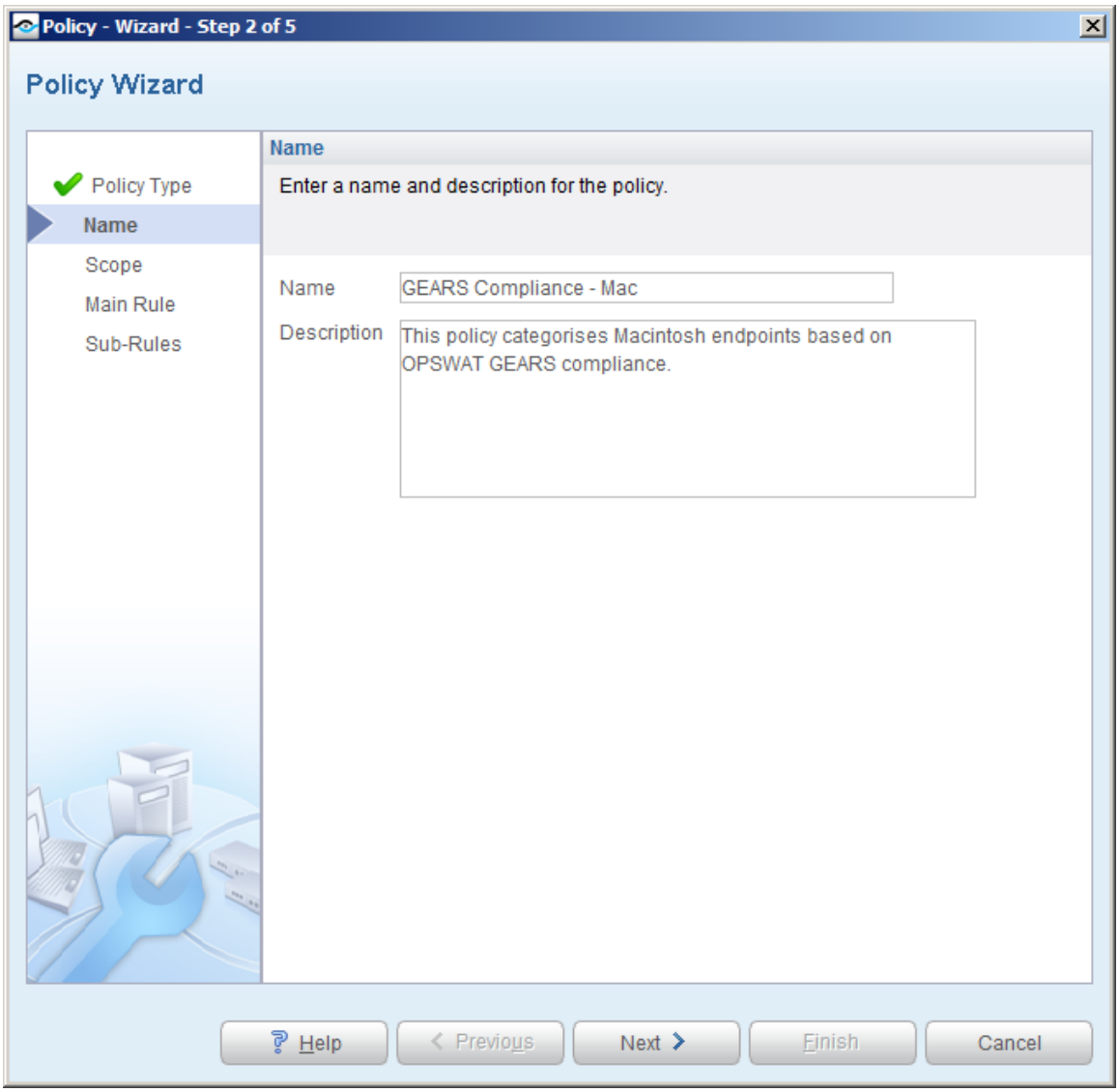
1. Open the policy manager and click on ADD to create a new policy



2. In the Policy Wizard, select CUSTOM for 'Policy Type' and click NEXT

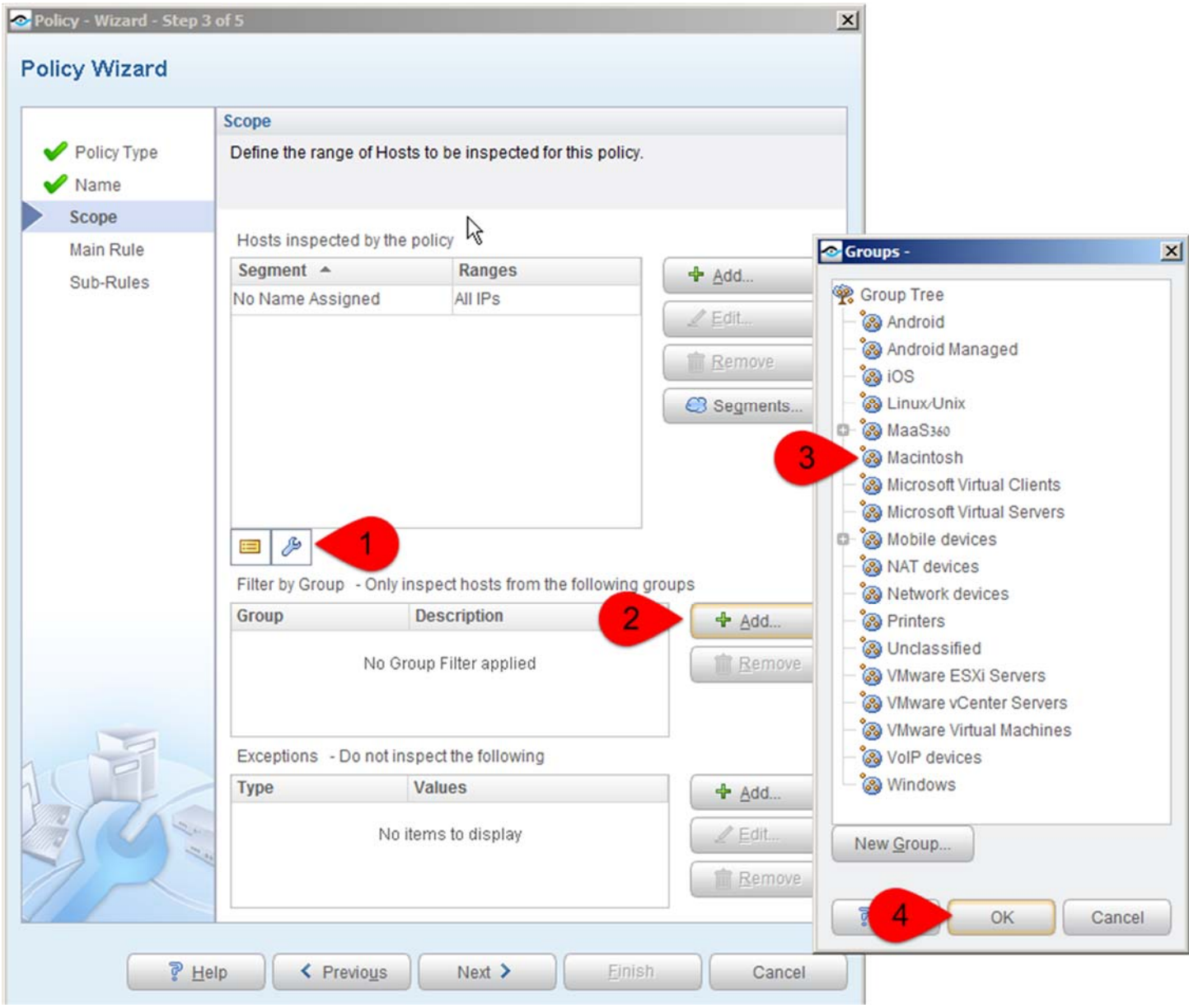


3. Give the policy a name, for example, “GEARS Compliance – Mac”



4. Select the range of IP addresses of the endpoints you want to include in the policy when prompted.

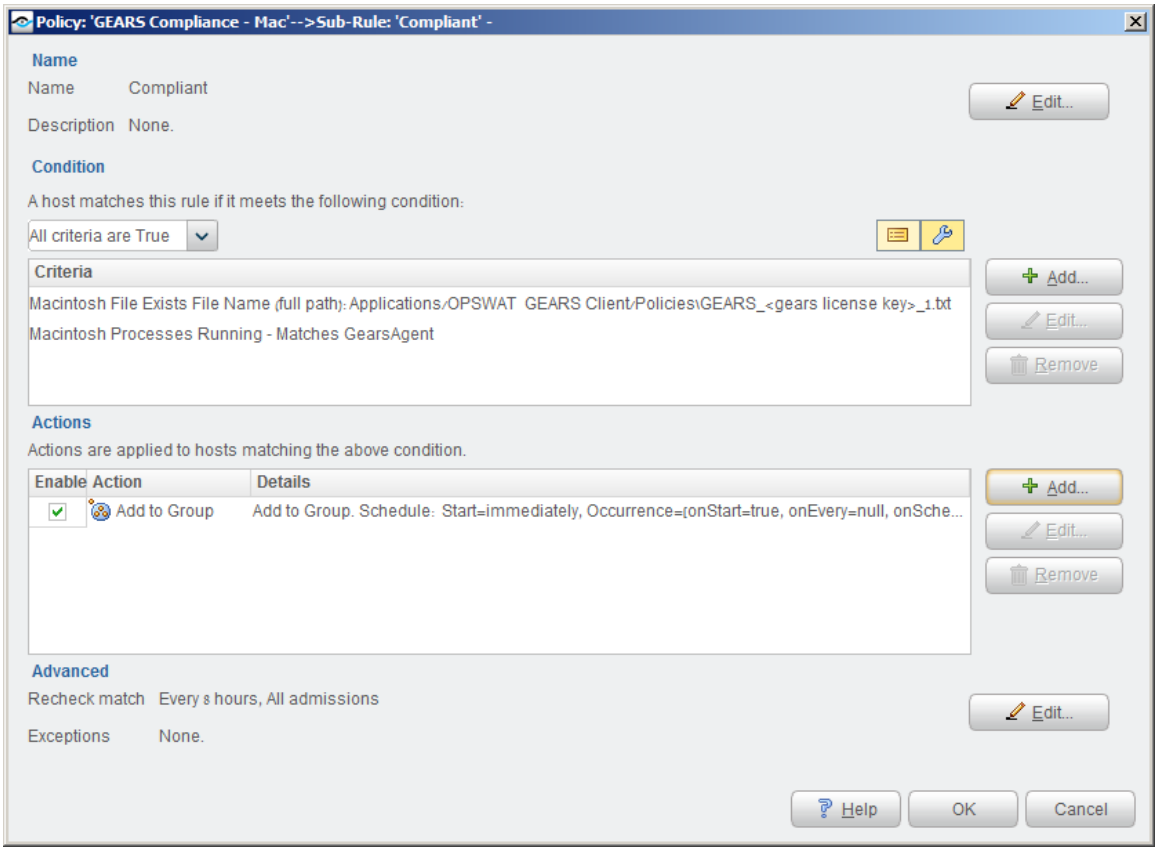
5. On step 3 of the wizard, click on the 'wrench' to open up the advanced options, then click ADD to filter by group, and select the "Macintosh" group (this assumes you have run added the standard *CounterACT Asset Classification Policy Template*)



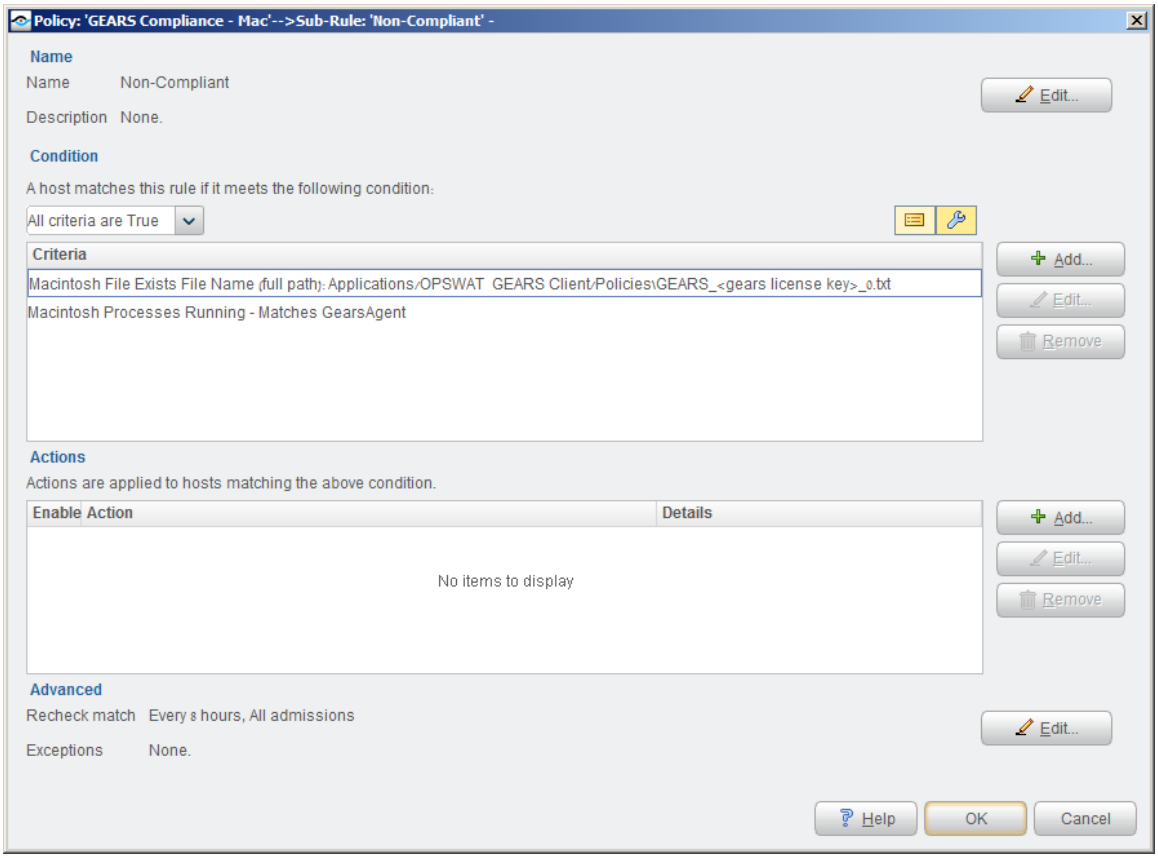
6. The main rule of the policy can be left empty, this ensures that all Macintosh endpoints will match this policy.

7. The sub-rules should be created as follows:

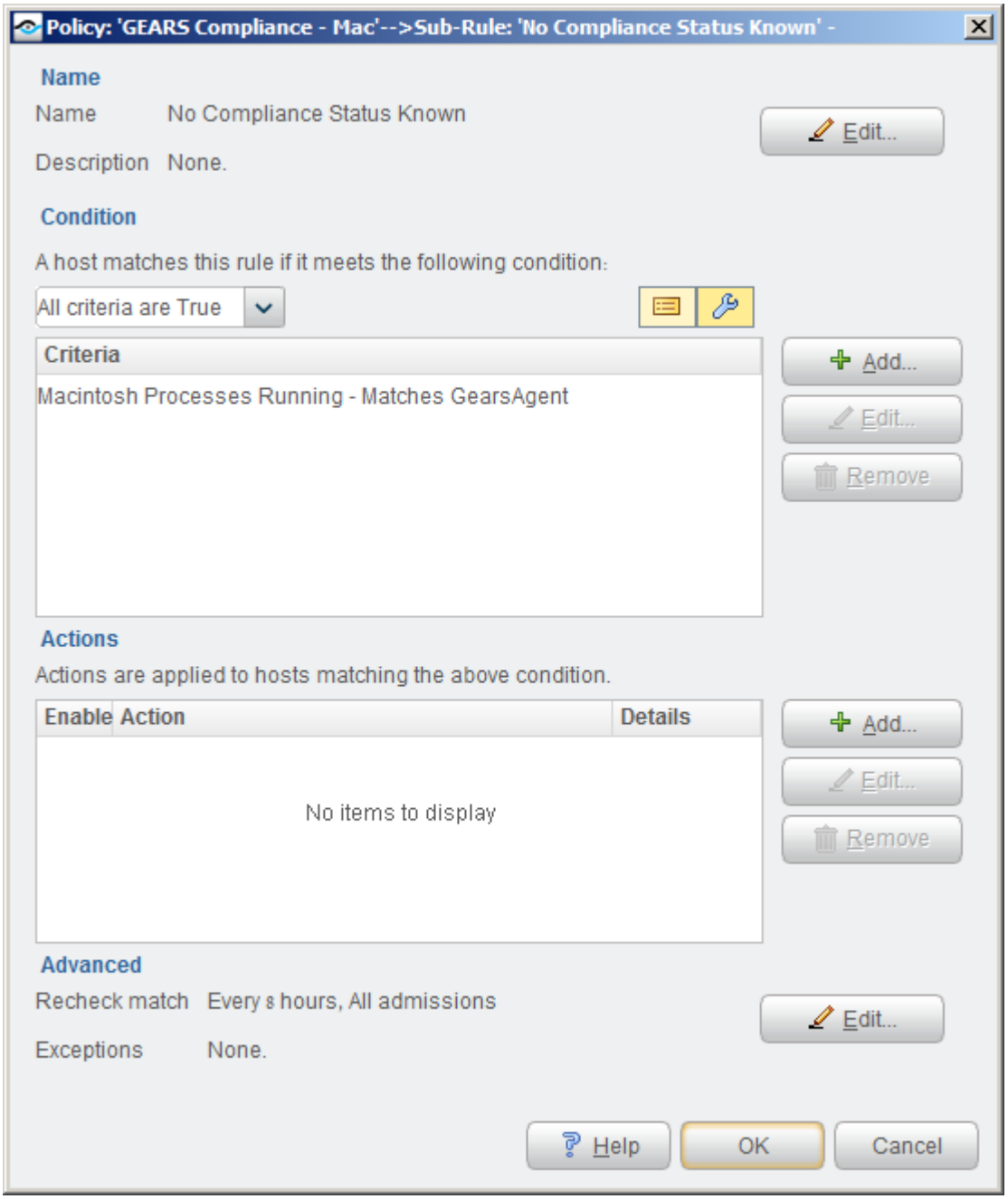
    a. The first sub-rule should check whether the OPSWAT process is running and that the policy file exists and is in the form GEARS_<license_key>_1.txt. Replace <license_key> with your license key. An action can be used here to add the endpoints to a group that indicates that the host is compliant.



b. The second sub-rule should check that the policy file exists but indicates non-compliance (0 at the end), and that the GEARS process is still running. Again, you can add non-compliant hosts to a different group or perform some other action, such as assigning them to a quarantine VLAN, hijacking their browser, or simply sending an email to the administrator.

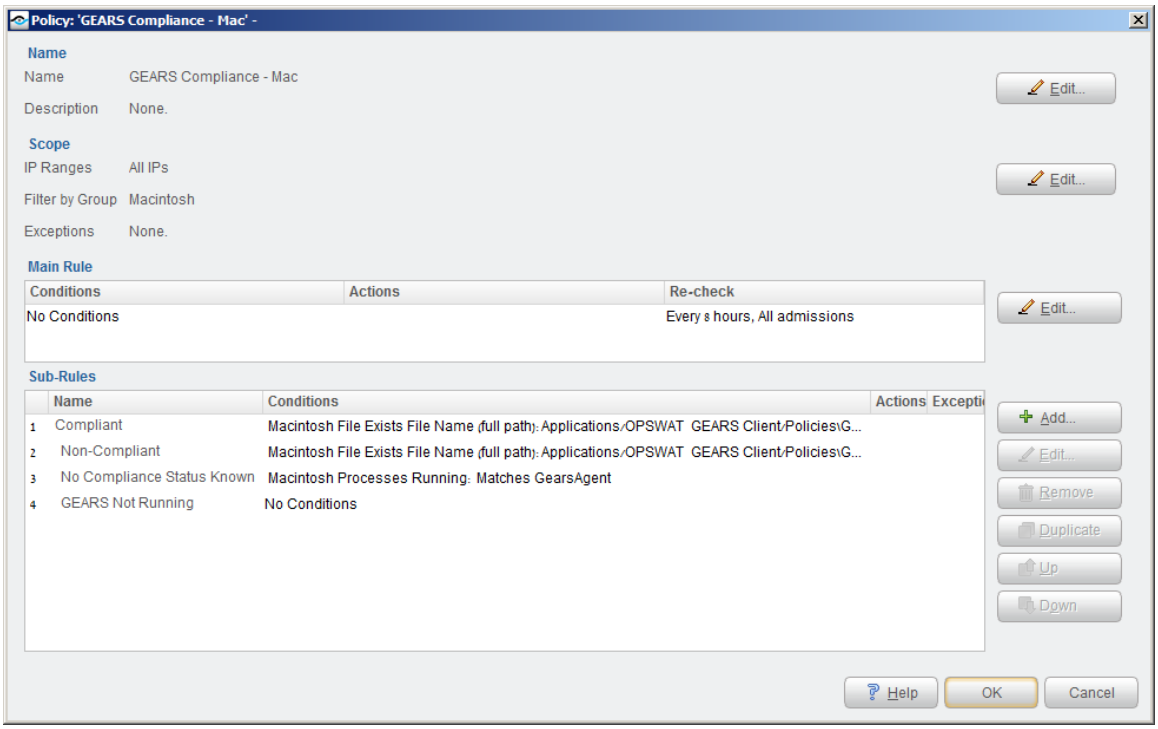


c. The third sub-rule should confirm that the agent is running, but no policy file was found in the first 2 conditions. Therefore, the compliance status cannot be determined. Again, you can add an action to notify the administrator or do something else as is appropriate.



d. The last sub-rule should have no conditions and is a catch-all for endpoints that do not have the GEARS client running. Again, you may configure automatic actions as is appropriate in your organization.

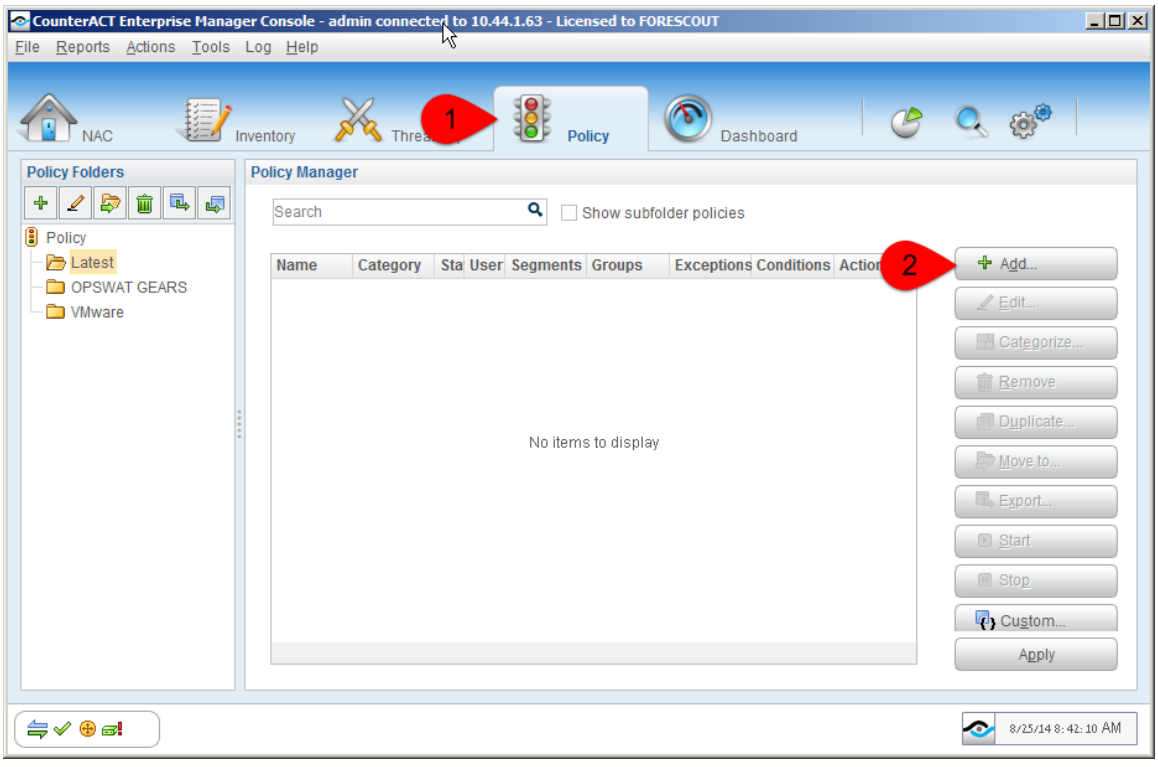
8. The final policy should look something like this:



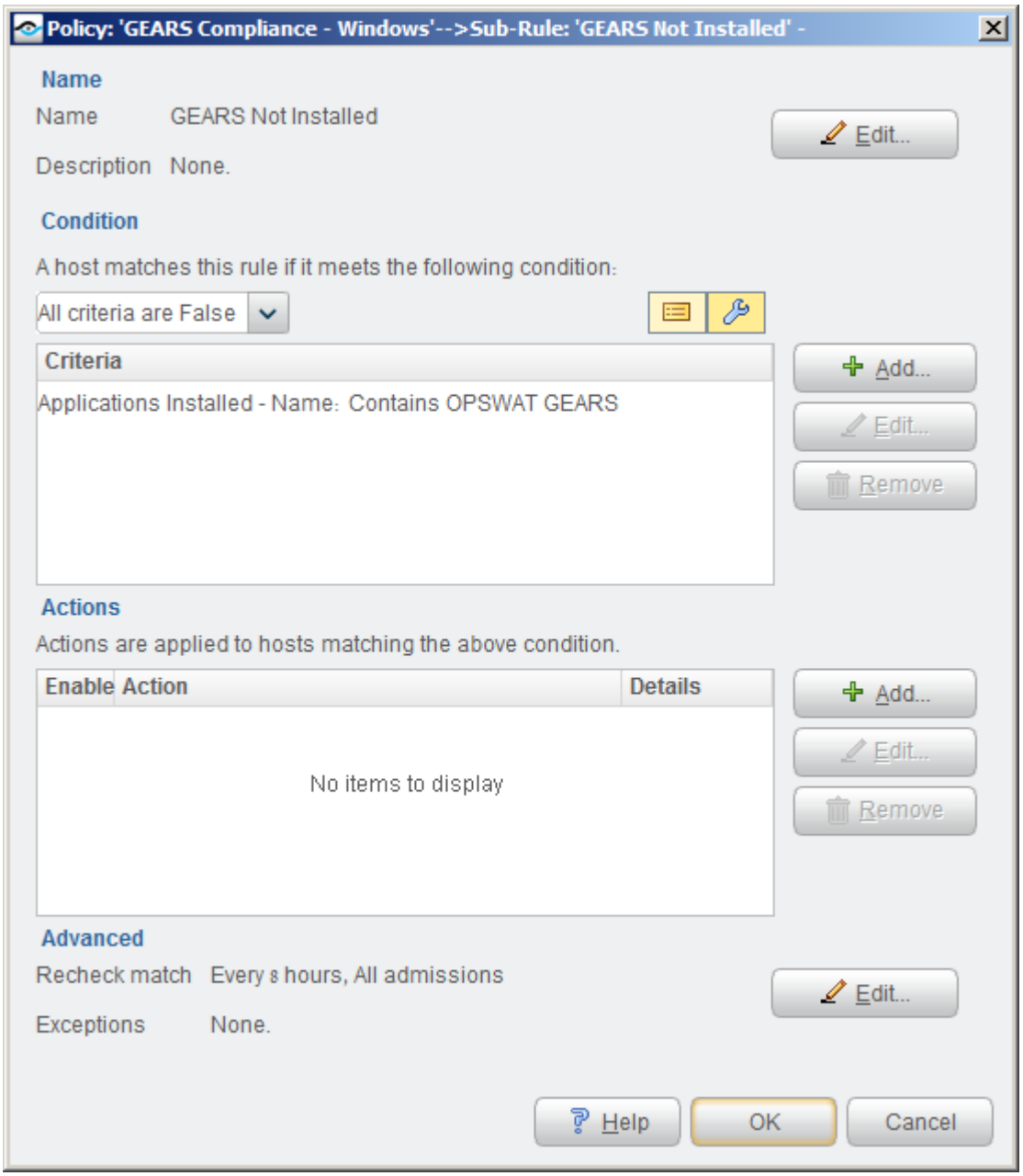
GEARS Compliance on Windows

Using CounterACT, you can create a policy which will analyze Windows computers for GEARS compliance, as follows (the steps shown are for a managed device. See appendix for differences on guest devices):

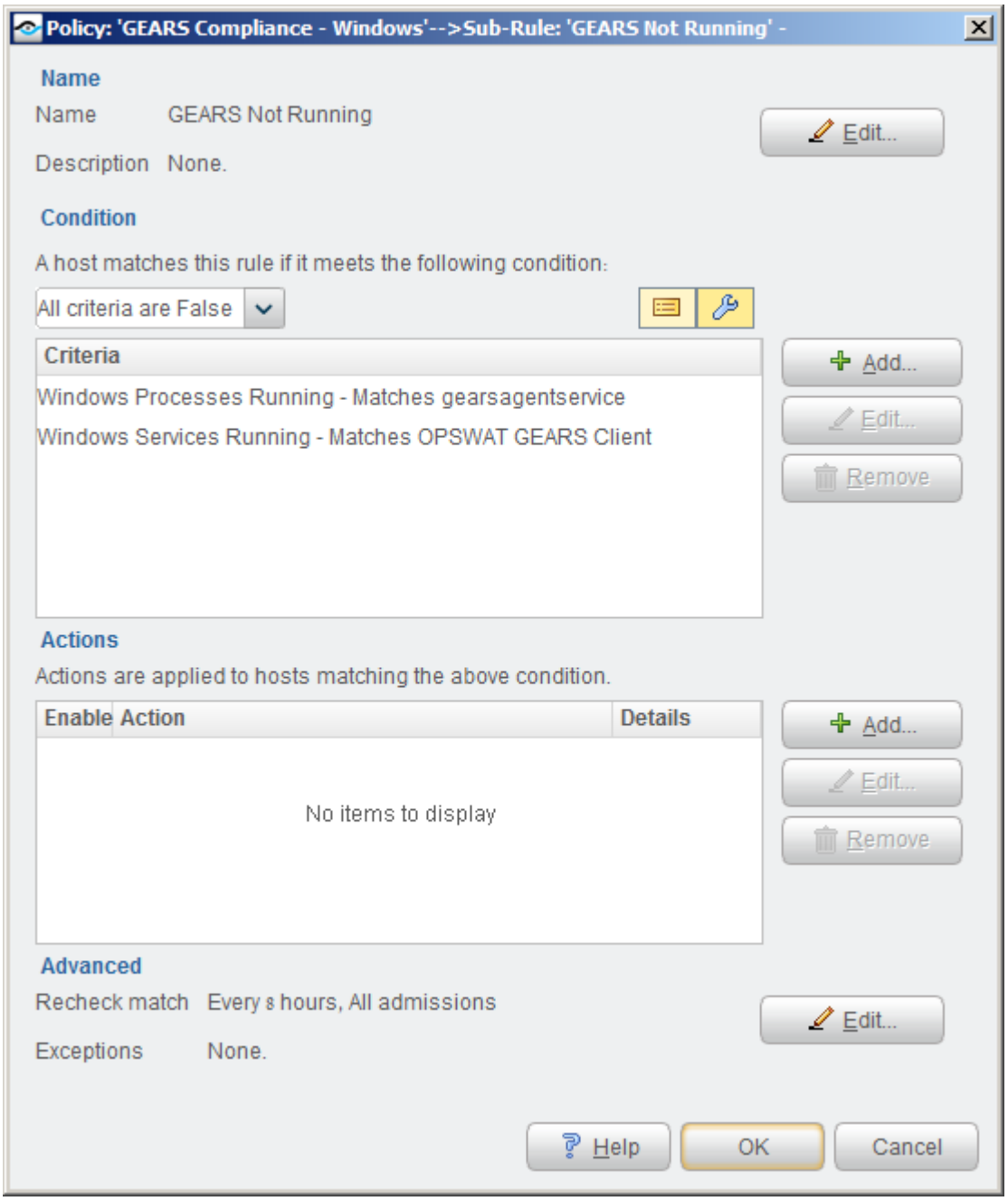
1. Open the policy manager and click on ADD to create a new policy



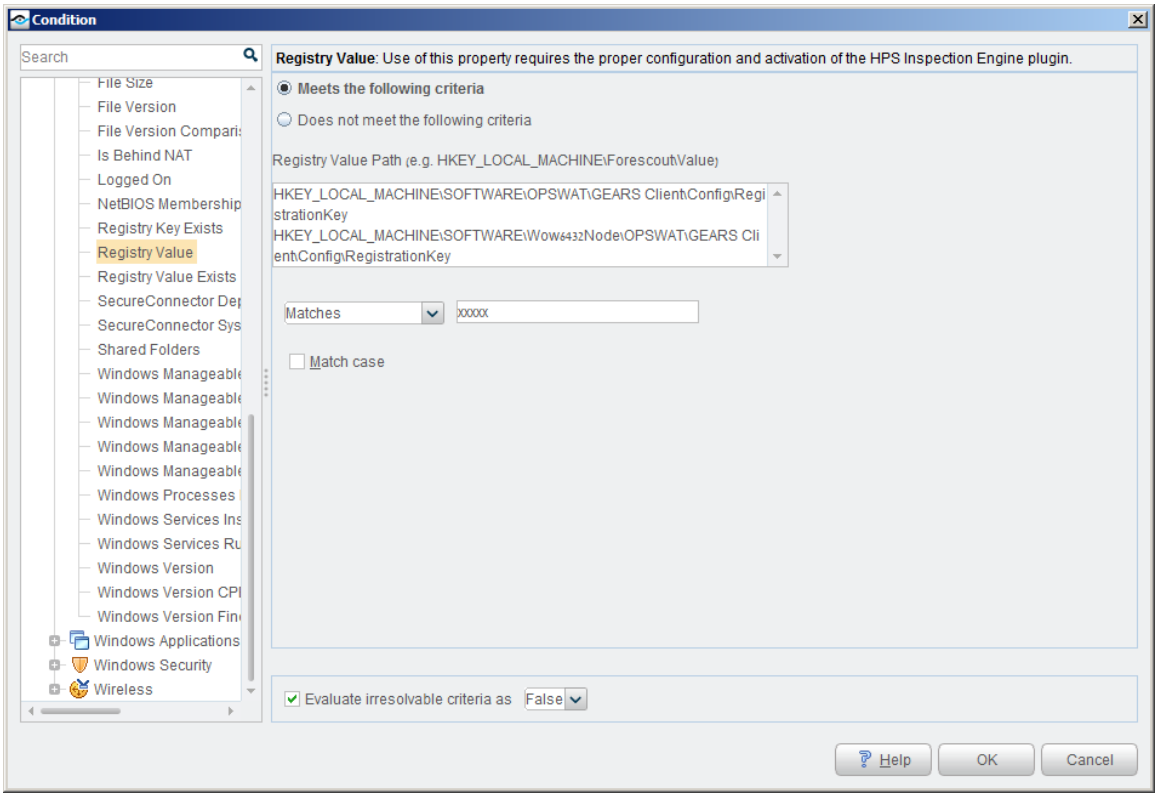
2. In the Policy Wizard, select CUSTOM for 'Policy Type' and click NEXT
3. Give the policy a name, for example, "GEARS Compliance – Windows"
4. Select the range of IP addresses of the endpoints you want to include in the policy when prompted.
5. On step 3 of the wizard, click on the 'wrench' to open up the advanced options, then click ADD to filter by group, and select the "Windows" group (this assumes you have run added the standard *CounterACT Asset Classification Policy Template*.
6. The main rule of the policy can be left empty; this ensures that all Windows endpoints will match this policy.
7. The sub-rules should be created as follows:
    a. The first sub-rule should detect Windows endpoints that do not have GEARS installed.



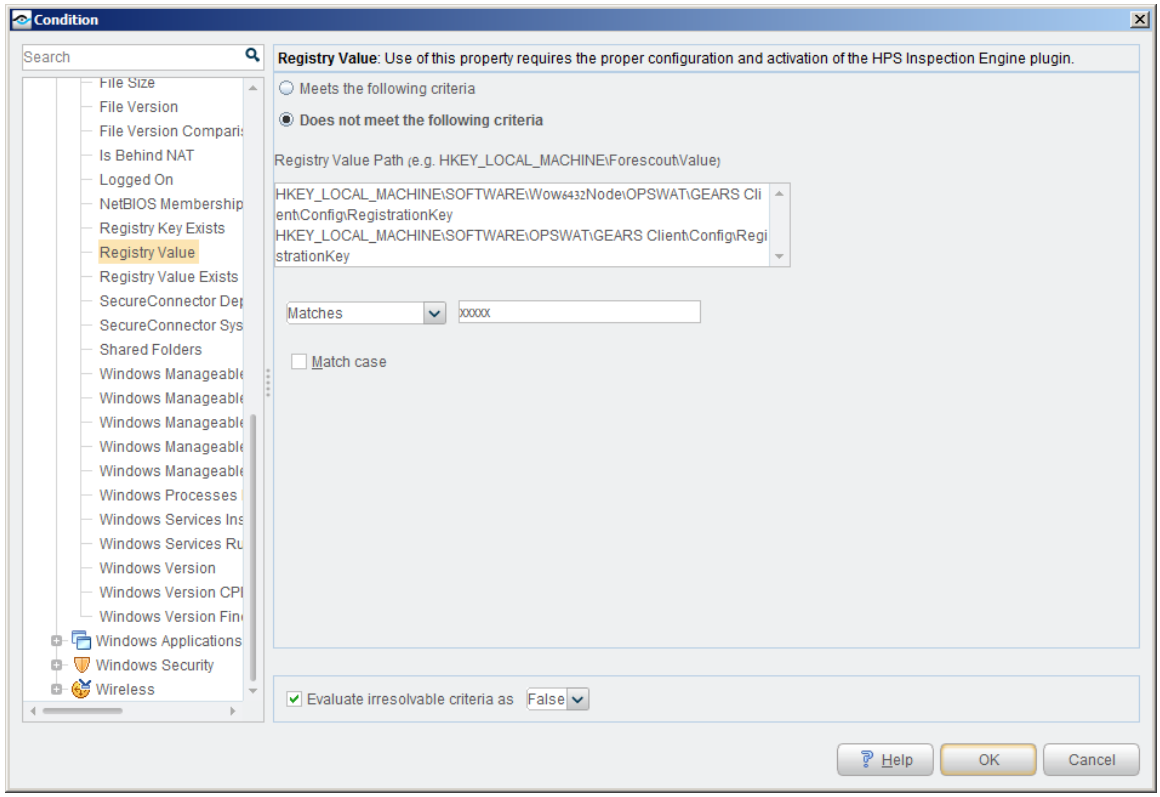
b. The second sub-rule should detect endpoints that have GEARS installed, but not running.



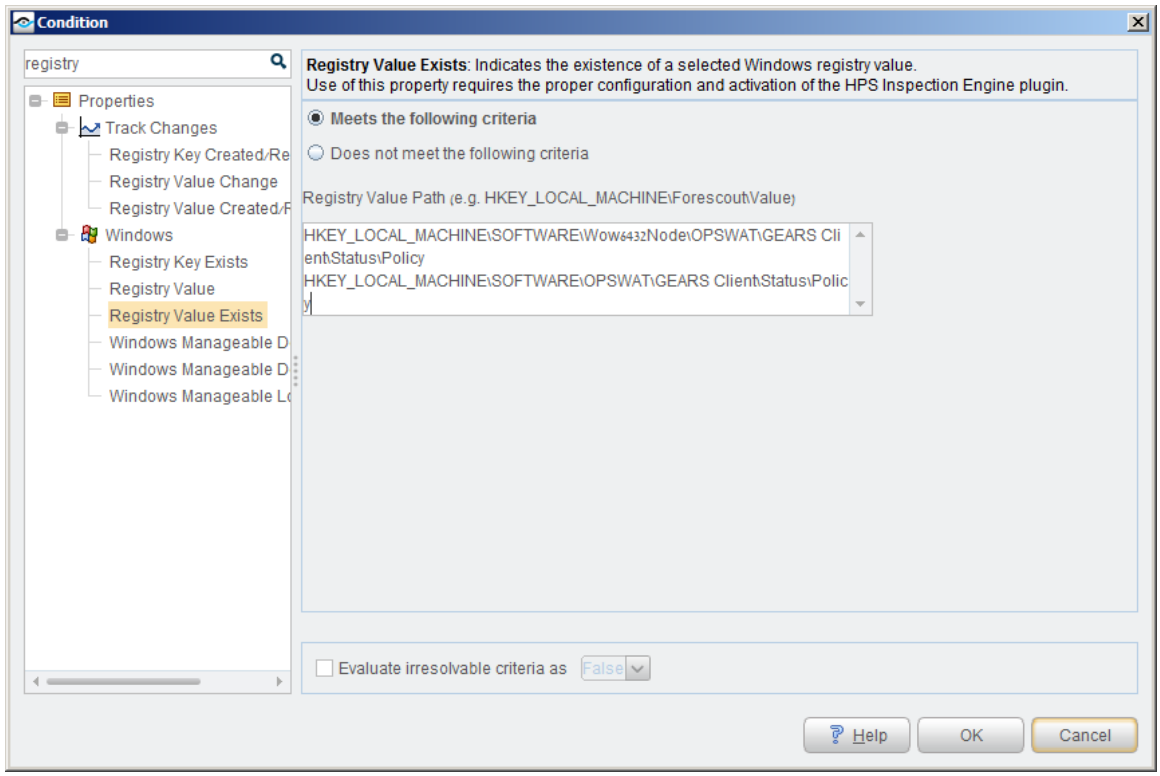
c. The third sub-rule should detect endpoints that have GEARS, but not using the corporate registration key. This can be done by creating a sub-rule that has only the following condition (where 'xxx' is replaced with the corporate registration key):



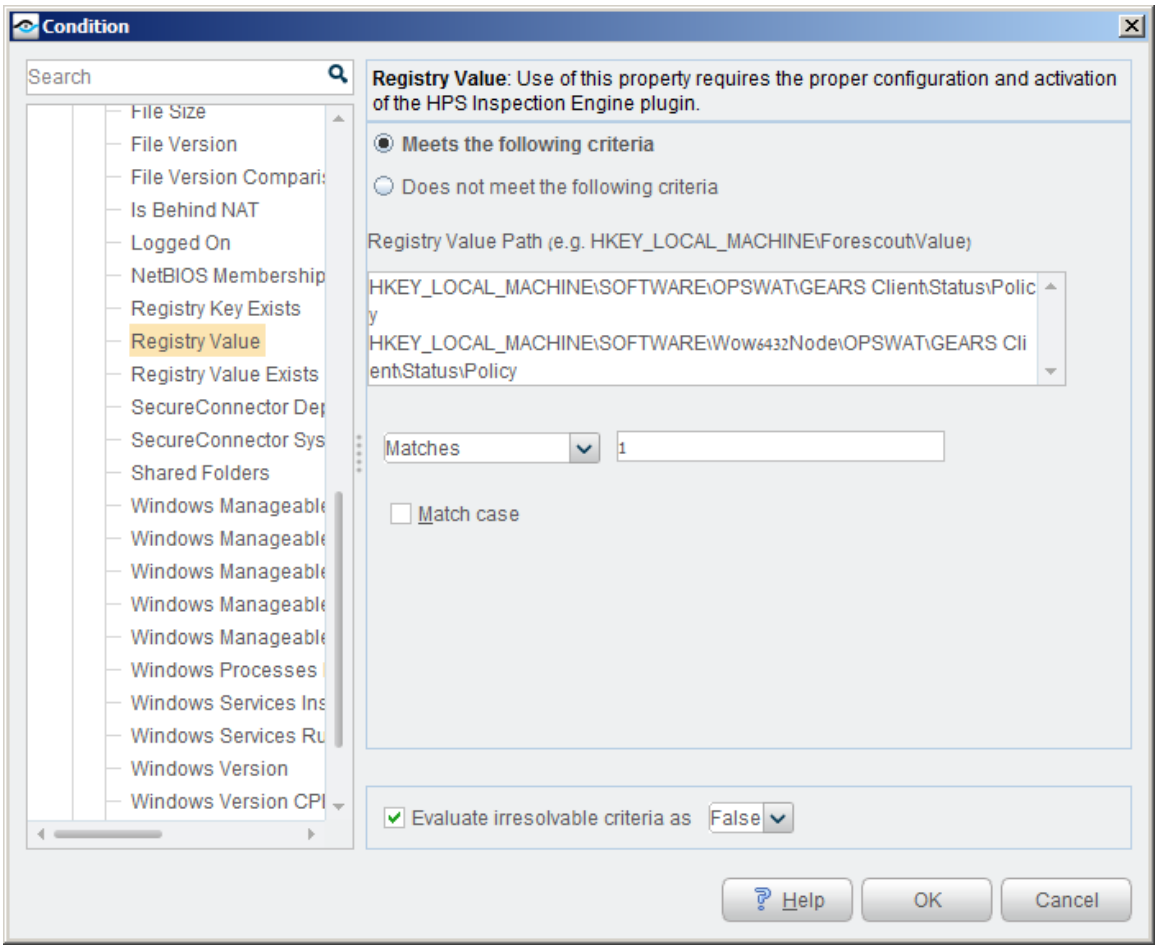
d. Only endpoints with a corporate licensed version of the GEARS client make it to the fourth sub-rule. This rule should detect endpoints which are not compliant according to GEARS. The condition for the rule looks as follows:



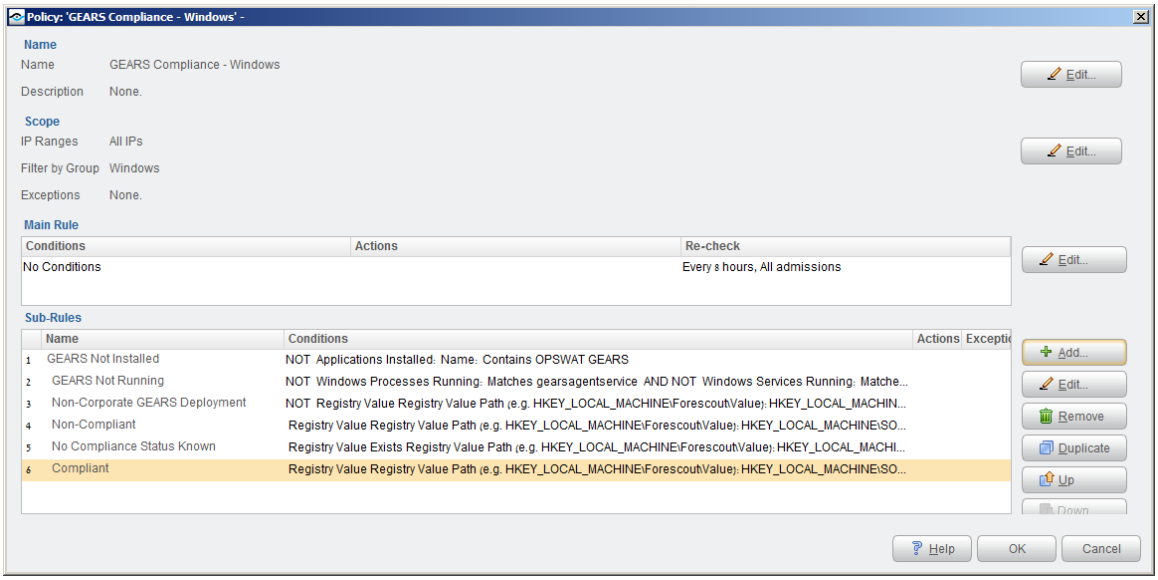
e. The fifth sub-rule should check for any endpoints which simply do not have compliance information reported in the registry. The condition is:



f. The last sub-rule has a condition to confirm that the host is compliance (though by this point, any host that gets this far must, by process of elimination, be compliant). The condition is:



8. The final policy should look something like this:



Managed vs. Guest Device

Managed devices (devices using the installed GEARS client) policies are configured as described above. Guest devices (devices using the on-demand GEARS client) policies are generally configured the same but require some minor modifications. Here is a table presenting those differences:

WINDOWS		
	MANAGED (PERSISTENT)	**GUEST (ON DEMAND)**
Process Name	GearsAgentService.exe	opswat-gears-od.exe
Service Name	OPSWAT GEARS Client	n/a
LICENSE KEY REGISTRY ENTRY		
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	------- Should match license key for the desired account -------	
COMPLIANCE STATE REGISTRY ENTRY		
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 and submit a ticket to request assistance from our support team.