How to Configure Citrix NetScaler Gateway with OPSWAT GEARS Client

About This Guide

GEARS provides IT Administrators the ability to provide Advanced Threat Detection and Advanced Compliance with existing secure remote access solutions. The GEARS platform allows authentication and enforcement to be defined according to the policies defined by an organization. You can read more about GEARS at http://www. opswatgears.com/.

GEARS can be easily leveraged by Citrix's Netscaler Gateway Pre-Authentication Policy through a C*ustom Registry* and *Process check*. At a high level the steps are:

- Configure NetScaler Gateway Pre-Authentication Policy
- Configure GEARS policy for specified check (i.e. Antivirus installed, No Malware detected, Password set, etc)
- Install or run GEARS Clients on endpoints

If you are running Access Gateway version 4.5, 5.0.3, or 5.0.4 you can also configure the GEARS functionality via the Endpoint Analysis Plug-in. Configuration steps can be found in the NetScaler Gateway Endpoint Analysis Plug-in section. Additional details on the Policy Generator can be found at the Citrix Endpoint Analysis Portal: http://citrix.opswat.com/home.jsp.

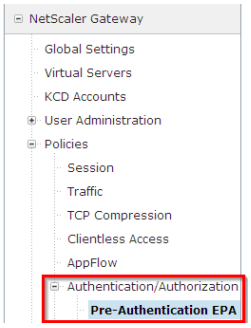
Following the implementation and configuration, the authentication process is now in place to automatically validate each endpoint meets the defined security and compliance checks prior to access. If the GEARS client is missing or out of compliance then the device will be rejected or fall back to a default state – depending on the NetScaler Gateway configuration.

This document specifically illustrates how to setup a policy check for the GEARS Client with Citrix NetScaler version 10.x; however the set-up for version 9.x is broadly similar. In order to leverage these checks the Gateway Service must also be setup to enforce Pre-Authentication and access control, which is beyond the scope of this guide. More information may be found at http://support.citrix.com/proddocs/topic/netscaler-gateway/ag-ee-10-edocs-landing.html. These configurations are only available for Windows clients at this time.

NetScaler Gateway Pre-Authentication Policies – Process and Registry Checks

Step 1:

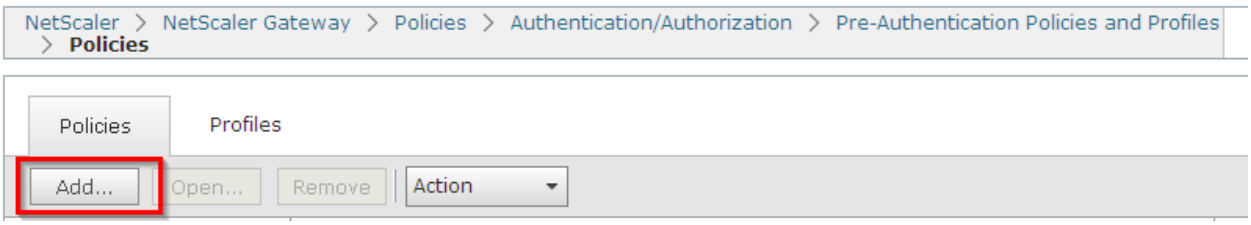
Under *NetScaler Gateway*, expand the *Policies* tab as well as the *Authentication/Authorization* tab and



select *Pre-Authentication EPA*.

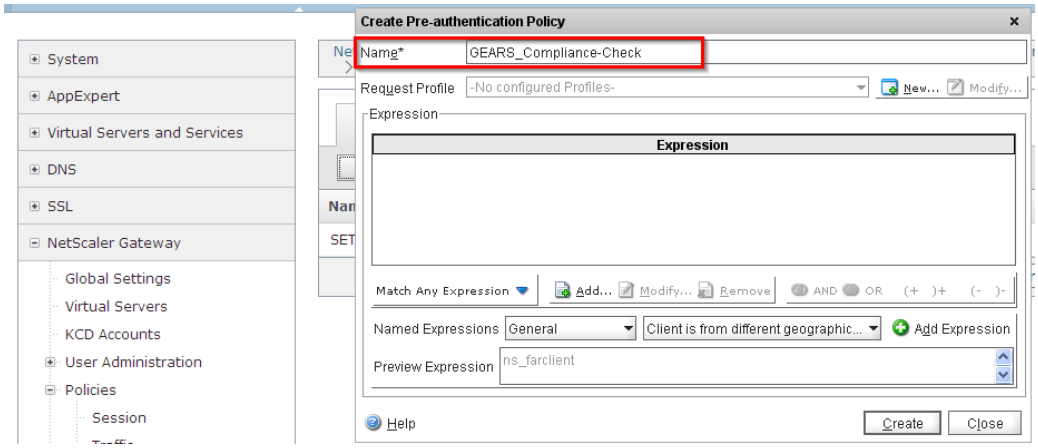
Step 2:

Under *Policies*, either create a **New** policy by selecting the add button.



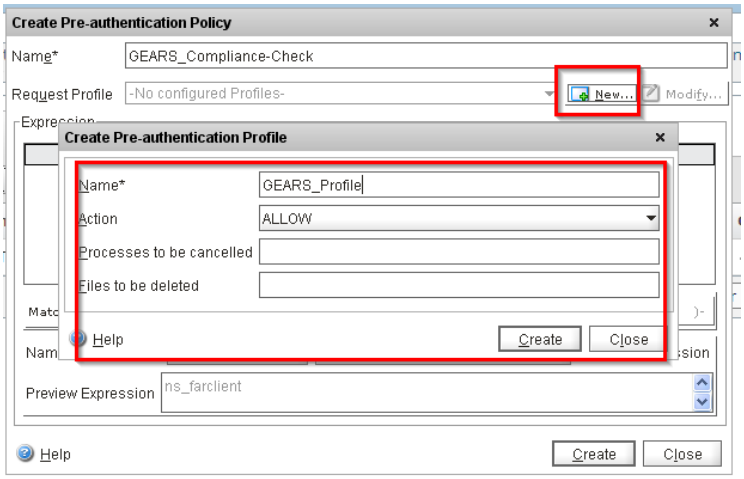
Step 3:

Within 'Create Pre-authentication Policy', provide a name for the new policy.



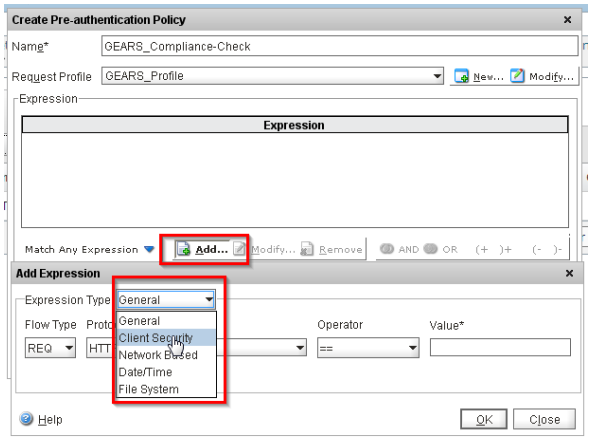
Step 4:

Create a new *Profile* or use an existing one, ensuring *Action* is set to *ALLOW*.



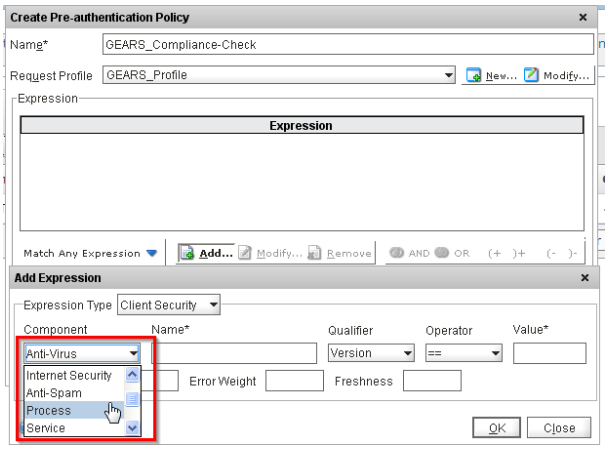
Step 5:

Create a new expression by selecting *Add*. In the expression type drop-down select *Client Security*.



Step 6:

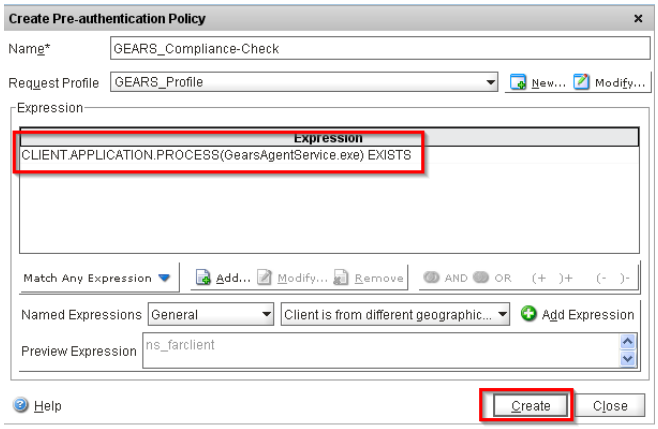
Select *Process* from the *Component* drop-down.



Step 7:

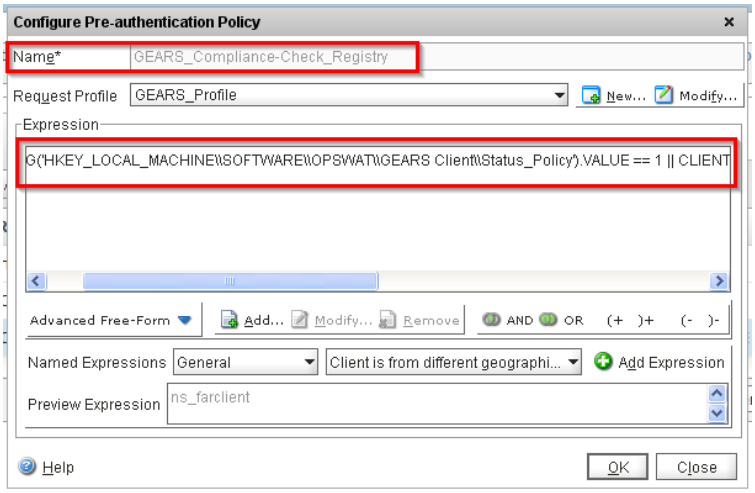
If you are using the persistent, installed GEARS client, enter ***GearsAgentSerivce.exe*** under *Name*, leave *Qualifier* blank and ensure EXISTS is listed in the *Operator* drop-down. If you are using the on demand, portable GEARS client, use the name GearsAgent.

Once completed click OK in the add expression dialog and select *Create*. This will create a rule to check that the GEARS agent is running on the endpoint.



Step 8:

Now that the process check has been created we will add the compliance registry value check. Simply edit the Pre-authentication Policy name and remove the process expression previously configured.



Step 9:

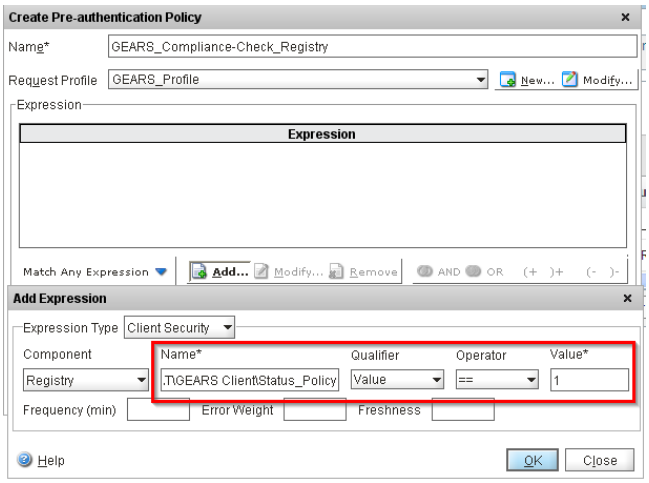
Create a new expression, selecting the type as *Client Security* and the component as *Registry*.

Step 10:

Enter the following information for the check:

1. For the persistent, installed GEARS client:
   - Name – HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Status_Policy
   - Qualifier – Value
   - Operator – ==
   - Value – 1
2. For the on demand, portable GEARS client:
   - Name – HKEY_CURRENT_USER\SOFTWARE\OPSWAT\GEARS OnDemand\Config_Policy
   - Qualifier – Value
   - Operator – ==
   - Value – 1

Select *OK* to add the expression and begin another in the same policy.

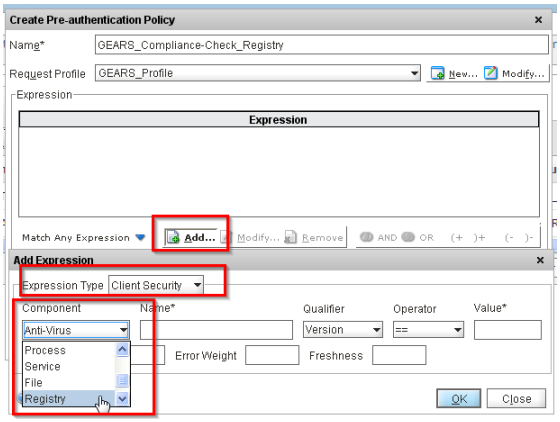


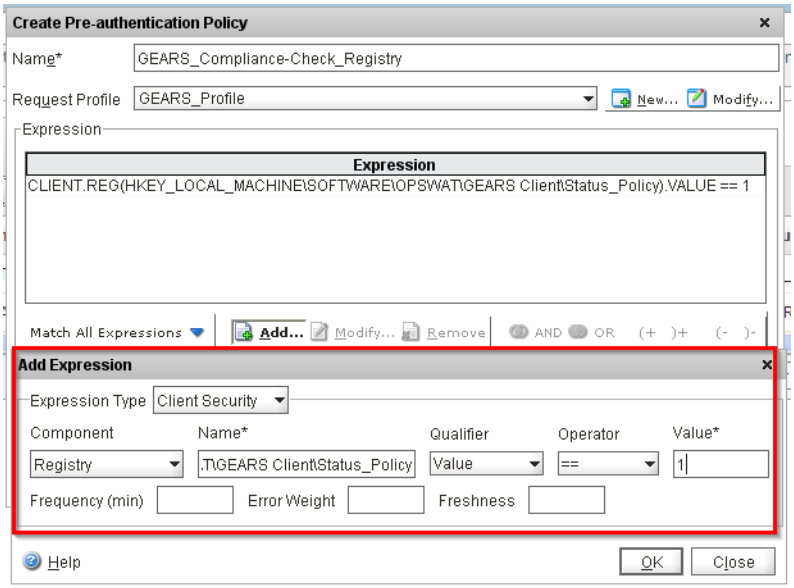
Step 11:

In the second expression, set the expression type to *Client Security* and the component as *Registry* then add the following information:

1. For the persistent, installed GEARS client:
   - Name – HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status_Policy
   - Qualifier – Value
   - Operator – ==
   - Value – 1
2. For the on demand, portable GEARS client:
   - Name – HKEY_CURRENT_USER\SOFTWARE\OPSWAT\GEARS OnDemand\Config_Policy
   - Qualifier – Value
   - Operator – ==
   - Value – 1

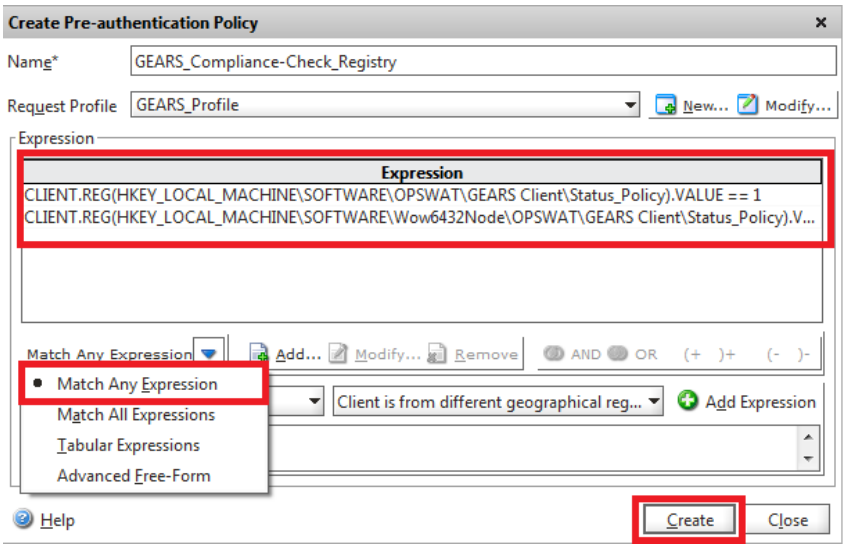
Select *OK*.





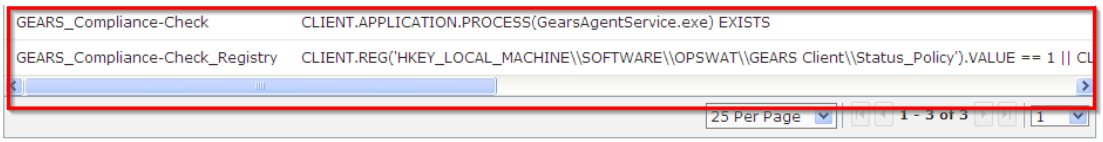
Step 12:

Set the two expressions created in the policy to allow either registry entry, if present with a value of 1, to be accepted. To accomplish this ensure *Match Any Expression* is selected in the appropriate field. Once this has been setup, complete the policy by selecting *Create*.



Step 13:

Both the ***Process*** and ***Registry*** Pre-Authentication EPA policies must be added as a requirement to connect to the NetScaler Gateway virtual server.



NetScaler Gateway Endpoint Analysis Plug-in

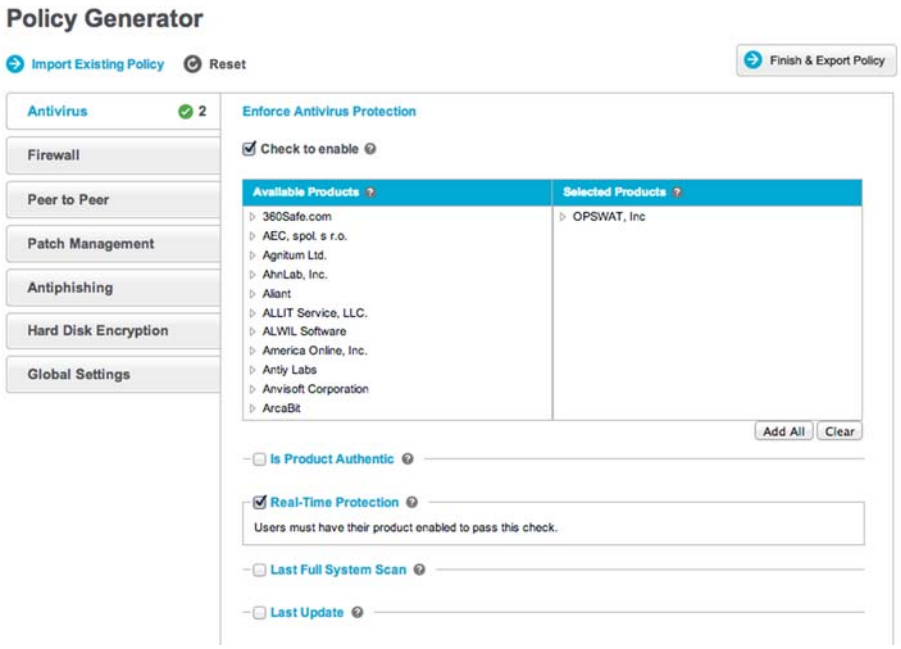
You can configure the NetScaler Gateway through the Endpoint Analysis Plug-in. The steps to configure the NetScaler can easily be performed via the Policy Generator, and include at a high level:

1. Download the Endpoint Analysis Plug-in
2. Create a Policy
3. Save and Export your Policy
4. Import your Policy to the Access Gateway

You can download the Endpoint Analysis Plug-in at http://citrix.opswat.com/download.jsp. Once the plug-in has been downloaded and installed, you can create your Policy via the Policy Generator at http://citrix.opswat.com/policyGenerator.jsp.

Within the Policy Generator you can easily add the GEARS Client by selecting *Antivirus* category.

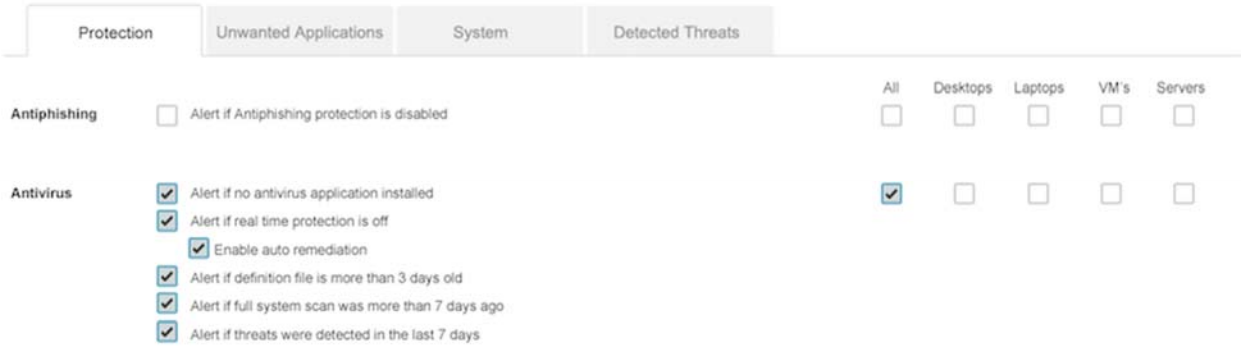
Under *Enforce Antivirus Protection*, select *Check to enable*, and then add "OPSWAT, Inc." as a *Selected Product*. Ensure that *Real-Time Protection* is enabled. Once all are selected, click *Finish & Export Policy*.



Once you have exported your Policy, you can then import into the Access Gateway, and add this as part of your pre-authentication check.

GEARS Configuration

Before endpoints can connect to NetScaler Gateway they must have GEARS Client running on the system as well as meet all security and compliance requirements configured by the Administrators in the GEARS dashboard.



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