How to set up Cisco Secure Access Solutions 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://gears.opswat.com/.

GEARS can be leveraged by the Cisco ASA 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. The Cisco ASA firewall can access and use this information through a *Process Scan* within the *Host Scan* configuration to determine if a device should be granted network access. The steps found within this document assume that this configuration is occurring with the ADSM console.

More information on the benefits of integrating GEARS with CISCO ASA's can be found at https://gears.opswat.com/integration/secure-access.

Host Scan Configuration

A Cisco ASA firewall can be configured to utilize GEARS for advanced compliance checks for remote users via the Remote Access VPN. These checks will help enforce that endpoint devices are meeting all compliance requirements established by the organization.

The policies can be easily configured via the GEARS Dashboard, and ensure that the security and compliance requirements of an organization are met on a continuous basis. The Process Scan first ensures that the GEARS Client is actively running on the device; then the additional policy compliance state can be validated via the Dynamic Access Policies.

Process Scan

The initial configuration will focus on the Process Scan functionality. This ensures that the GEARS Client is running on the endpoint.

Step 1:

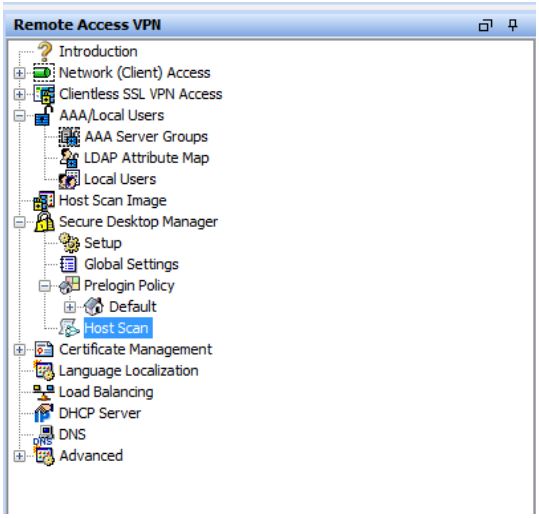
Validate that the OPSWAT GEARS client is running.

The active process will be:

- For Windows: GearsAgentService.exe
- For Mac: GearsAgent

To configure this validation step and save for use in a Default Access Policy, go to *Remote Access VPN* within the ADSM console; and select *Host Scan* under *Secure Desktop Manager*.

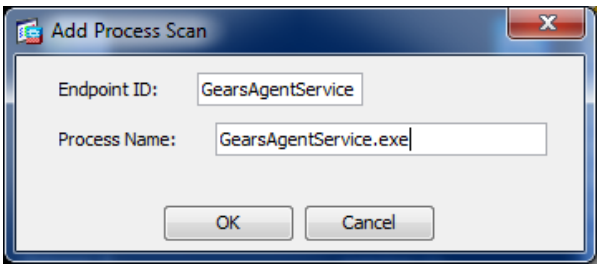
Select *Add*.



Step 2:

Select *Process Scan*, and name the *Endpoint ID* something that you will affiliate with this check (i.e. GearsAgentService).

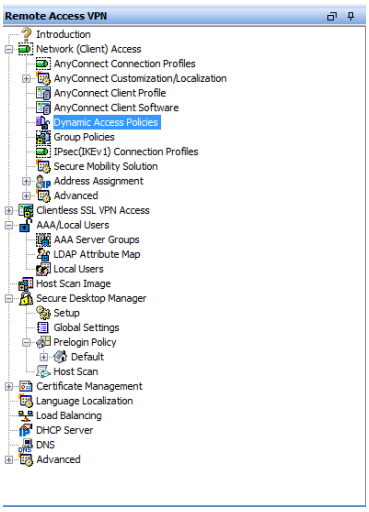
Enter GearsAgentService.exe in the *Process Name* box.



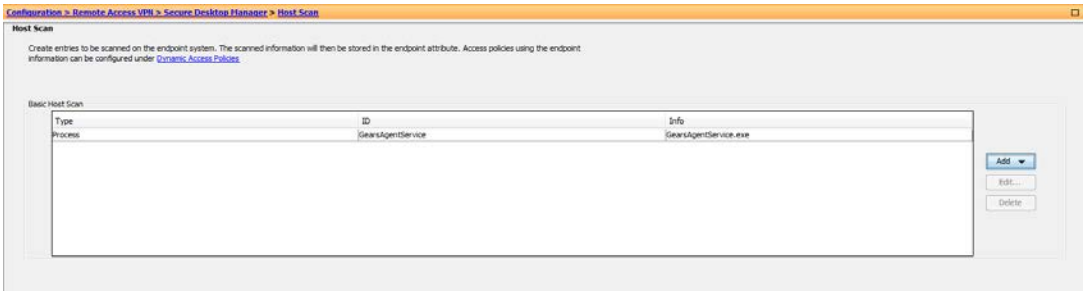
Apply these changes to your running configuration prior to continuing to the next step.

Step 3:

Navigate to *Network (Client) Access* and select *Dynamic Access Policies*.



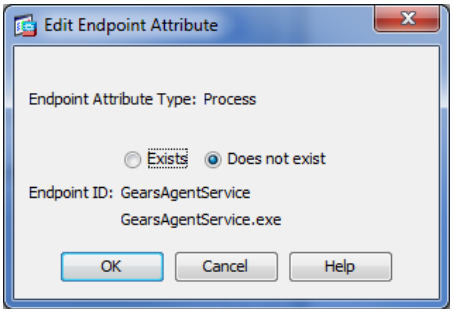
Select *Add*, then *Policy*.



Step 4:

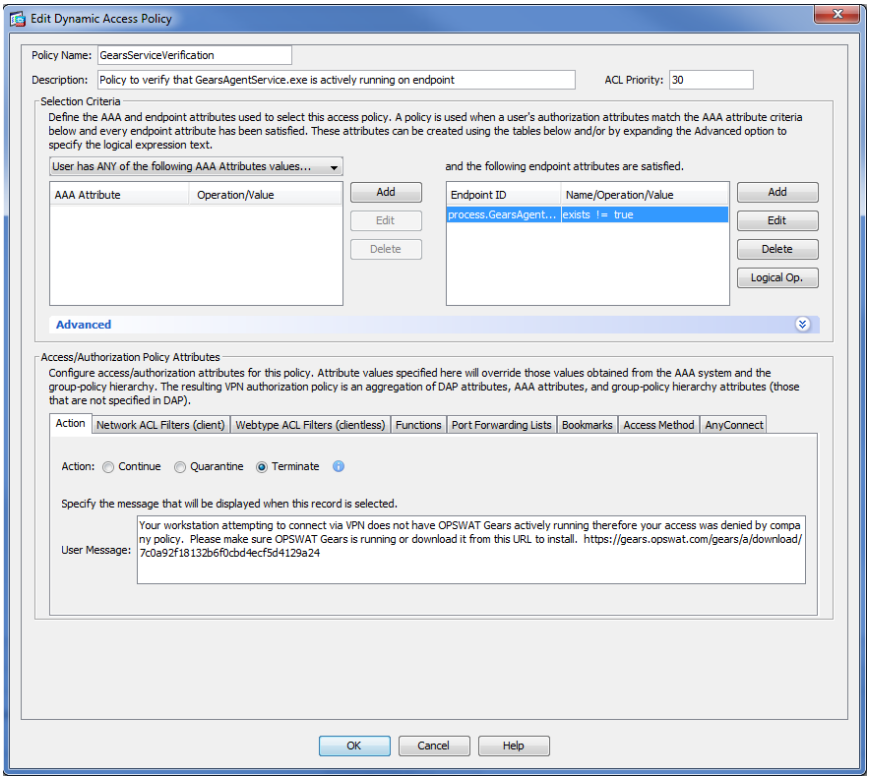
Give your new Policy a meaningful name (i.e. GearsServiceVerification), and describe as appropriate. Provide an ACL priority as appropriate to your existing configuration.

Select Add in the "*and the following endpoint attributes are satisfied*". For the "*Endpoint Attribute Type*", select *Process;* then select the previously created "*Endpoint ID*" of "GearsAgentService".



Select "*Terminate*" for the "*Action*".

Please note, this *Dynamic Access Policy* will not allow a tunnel to be created if the GearsAgentService.exe is NOT running. If the process is running, you will continue to the next *Dynamic Access Policy*.



You have now configured a posture assessment and Dynamic Access Policy that will verify that the GEARS client is running, prior to allowing the remote device into a network.

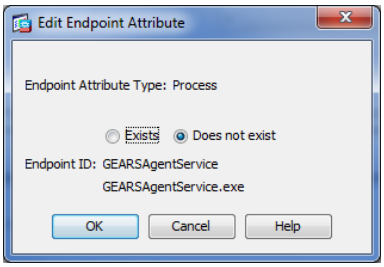
Registry Scan

The configuration includes the Registry Scan functionality. This ensures that the endpoint meets the predefined compliance requirements prior to allowing access to the network.

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

Step 1:

Edit the *Endpoint* Attribute previously created – "GearsAgentService". Establish the *Registry Scan* for the 64-bit system by first creating the *Endpoint Name* for the check. This name should be unique to designate the difference between the two checks (32-bit versus 64-bit). Now add requirements for the following *Registry Scan* details.



Confirm the Registration Key on the Client matches the Account:

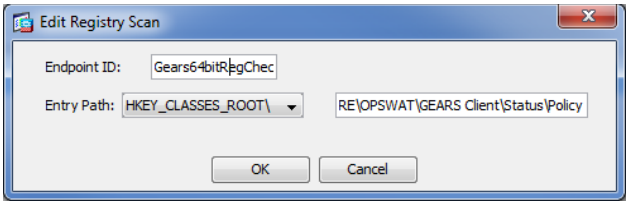
- Registry root key – HKEY_LOCAL_MACHINE
- Registry subkey – \SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Config
- Name – RegistrationKey
- Type – REG_SZ
- Value should match the account Registration Key

Check the Compliance state on the endpoint with the following:

- Root key – HKEY Local Machine
- Subkey – \SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status
- 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



Select *Ok* to save the changes to enable the check for a 64-bit registry.

Step 2:

Repeat Step 1 to create an additional *Endpoint Attribute* for the 32-bit Registry. Now add requirements for the following *Registry Scan* details.

Confirm the Registration Key on the Client matches the Account:

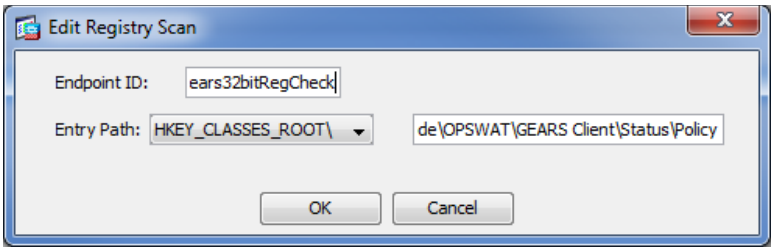
- Registry root key – HKEY_LOCAL_MACHINE
- Registry subkey – \SOFTWARE\OPSWAT\GEARS Client\Config
- Name – RegistrationKey
- Type – REG_SZ
- Value should match the account Registration Key

Check the Compliance state on the endpoint with the following:

- Root key – HKEY Local Machine
- Subkey – \SOFTWARE\OPSWAT\GEARS Client\Status
- Name – Policy
- Type – DWORD
- Value – 0x0000000 (1)

Policy Key Values:

c. 0 = NOT in compliance with policy, check GEARS Cloud for details on the device
d. 1 = in compliance with policy, check GEARS Cloud to view the defined policy

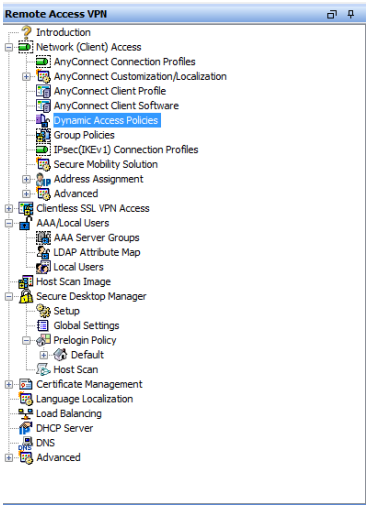


Select *Ok* to save the changes to enable the check for a 32-bit registry.

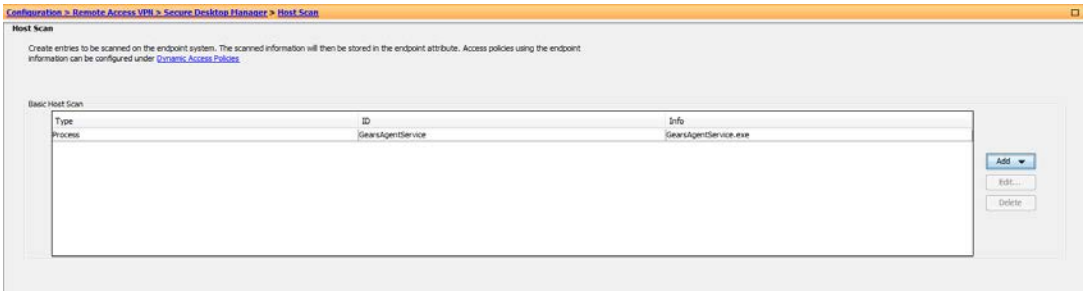
Step 3:

For Mac devices, the client provides a file with the Registration Key and Policy value. To configure for the Mac, first you need to create a new *Host Scan*.

Navigate to *Secure Desktop Manager* and *Host Scan*.



Under *Host Scan*, select *Add*; then *File*.



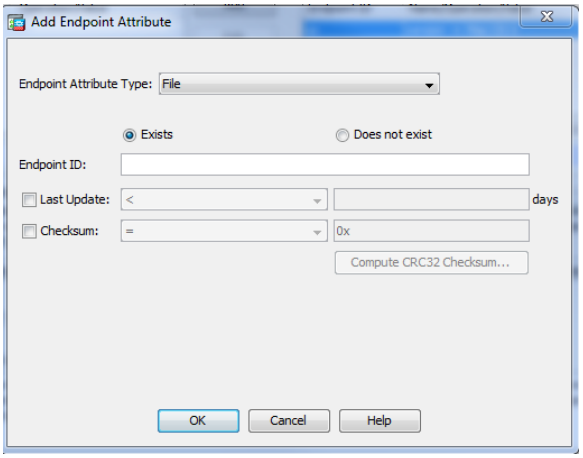
Step 4:

Add a new file - ***Applications/OPSWAT GEARS Client/Policies/ GEARS_ <gears license key>_1.txt.*** The *gears license key* will be where you add your *Account Registration Key*, and the "1" represents the Policy Value of a device that passes the policy defined in the GEARS dashboard.

This file includes a combination of 2 values, Policy and LicenseKey, to ensure that the client installed is assigned to the Account that manages the defined Polices.

Step 5:

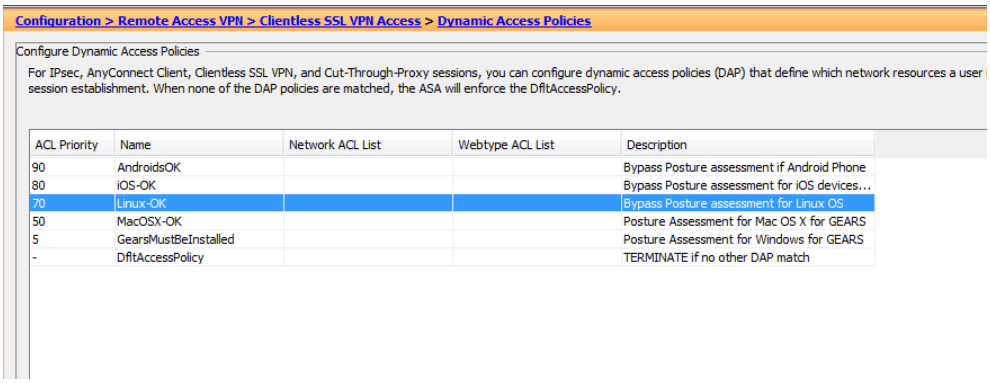
Add the *Endpoint Attribute* based on the file you previously created – *Endpoint Attribute Type* – File. The value that will be shown, is the full path added when the File was created -***Applications/OPSWAT GEARS Client/Policies/ GEARS_<gears license key>_1.txt.***



Select Ok.

Step 6:

Complete setup of any other requirements you wish to include in the Host. Once completed, go to *Dynamic Access Policies* to determine the priority of the *Policies*.



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.