How to Configure a Client-Side Integration with OPSWAT GEARS

Contents

About This Guide

GEARS provides IT Administrators with Security Compliance, Management, Remediation and Monitoring tools, including infection detection for use with managed or unmanaged devices.

The GEARS platform allows administrators to define robust policies that can be leveraged by third-party solutions for additional authentication and enforcement. You can read more about GEARS at http://www.opswatgears.com.

A Network Access Control (NAC) or Secure Remote Access application can easily leverage GEARS for pre-authentication policies through a *Process* and *Registry* or *P-list* check.. At a high level the steps are:

- Configure pre-authentication policy
- Install or run GEARS Clients on endpoints
- Configure GEARS policy for specified check (e.g. Antivirus installed and running, encrypted hard disk, password protected, etc.)

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 if the device is out of compliance then the device will be rejected or fall back to a default state – depending on the appliance or software configuration.

- Requirement: The ability to check running processes and read a registry key (Windows), and p-list or txt file name (Mac)
- Typical Uses: VPN-SSL, NAC, NGFW, other Secure Remote Access solutions, enterprise software
- Estimate Time to Configure: 1-2 hours depending on the capabilities of the device or software

Registry and Process Check - Windows

This outlines the custom Registry Checks you can perform on Windows endpoints. We provide two paths, one for 32-bit and one for 64-bit, as the registry locations are different in each. Your registration key should match your account key. This key can be found when you add new devices from your GEARS dashboard.

1. First check whether GEARS Client is running to ensure that the compliance information stored in the registry is current.
    a. For the persistent, installed GEARS client, look for either the running
        i. Process '**GearsAgentService.exe**'
        ii. Service '**OPSWAT GEARS Client**'
    b. For the on demand, portable GEARS client, look for running process '**opswat-gears-od.exe**'

    Confirm that process and service are signed by OPSWAT and the certificate is valid.

2. Next, confirm the Registration Key on the Client matches the intended GEARS Account.
    a. For the persistent, installed GEARS client:
        i. Registry root key – **HKEY_LOCAL_MACHINE**
        ii. Registry subkey (32-bit)– **HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Config**
        iii. Registry subkey (64-bit)– **\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Config**
        iv. Name – **RegistrationKey**
        v. Type – REG_SZ
        vi. Value should match the account license key
    b. For the on demand, portable GEARS client:
        i. Registry root key – **HKEY_CURRENT_USER**
        ii. Registry subkey (32/64-bit)– **HKEY_CURRENT_USER\SOFTWARE\OPSWAT\GEARS OnDemand\Config**
        iii. Name – **RegistrationKey**
        iv. Type – REG_SZ
        v. Value should match the account license key

3. Finally, check the compliance state on the endpoint with the following:
    a. For the persistent, installed GEARS client:
        i. Registry root key – **HKEY_LOCAL_MACHINE**
        ii. Registry subkey (32-bit)– **HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Status**
        iii. Registry subkey (64-bit)– **\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status**
        iv. Name – **Policy**

v. Type – **DWORD**
vi. Value should match **0x0000000 (1)**

b. For the on demand, portable GEARS client:
i. Registry root key – **HKEY_CURRENT_USER**
ii. Registry subkey (32/64-bit)– **HKEY_CURRENT_USER\SOFTWARE\OPSWAT\GEARS OnDemand\Config**
iii. Name – **Policy**
iv. Type – **DWORD**
v. Value should match **0x0000000 (1)**

c. Policy Key Values
i. 0 = NOT in compliance with policy, check GEARS Cloud for details on the device
ii. 1 = in compliance with policy, check GEARS Cloud to view the defined policy

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

The endpoint compliance parameters are configured within the GEARS dashboard. Once the Policies are configured and the clients installed across all of the endpoints, you can begin using GEARS as part of the additional security and compliance enforcement.

Additional references are included below:

1. Key Values “Installed” (DWORD):
   a. Missing = Client not installed, check Status of Client
   b. 1 = installed
   c. Other = ERROR CONDITION
2. Key Values: "Policy" (DWORD):
   a. Missing = Client not installed, check Status of Client
   b. 0 = NOT in compliance with policy, check GEARS Cloud for details on the device
   c. 1 = in compliance with policy, check GEARS Cloud to view the defined policy
   d. Other = ERROR CONDITION

P-list or Txt File and Process Check - Mac

This outlines the custom check you can perform on Mac endpoints. While the policy value can be simply read, it’s very important to also: (1) check the license key to ensure the device is compliant with the expected account, and (2) check that the GEARS process is running to ensure the integrity of the policy value.

The account license key is alternately called the client registration key. This value is available in the account configuration section of the GEARS console. It is unique per-account.

Check that GEARS is running:

1. Confirm that the GEARS client is installed and running, look for the Process named **GearsAgent**. This ensures the integrity of the file or p-list

Check the license key and policy state:

1. Validate compliance of the endpoint by checking the GEARS log file:
    a. For the persistent, installed GEARS client, there are two options:
        i. Reading the name of a txt file
            1. File location: **Applications/OPSWAT GEARS Client/Policies**
            2. File name: **GE*ARS_<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.
        ii. Reading the contents of a p-list
            1. PLIST location: /Library/Preferences/SystemConfiguration/
            2. PLIST name: com.opswat.gearsagent.plist
            3. Sample PLIST contents (condensed):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>AgentConfig</key>
  <dict>
    ...
    <key>HardwareID</key>
    <string>1234567890ABCDEF</string>
    <key>LicenseKey</key>
    <string>12345678901234567890123456789012</string>
    ...
  </dict>
  ...
  <key>Status</key>
  <dict>
    ...
    <key>Policy</key>
    <integer>0</integer>
    ...
  </dict>
</dict>
</plist>
```

b. For the on demand, portable GEARS client:
    i. File location: **/Users/<username>/Documents/OPSWAT/GEARS OnDemand.**
    ii. File name: **GE*ARS_ <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.
    iii. *There is no* **p-list** *option for portable GEARS client*

The endpoint compliance parameters are configured within the GEARS dashboard. Once the Policies are configured and the clients installed across all of the endpoints, you can begin using GEARS as part of the additional security and compliance enforcement.

Client-Side GEARS Integration

Flow Diagram for Compliant Endpoint