How to set up Dell SonicWALL Aventail® SRA Appliance 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 advanced threats. More information on GEARS may be found at http://www.opswatgears.com/.

GEARS can be leveraged by the Dell SonicWALL Aventail® Secure Remote Access (SRA) Appliance End Point Control to provide enhanced compliance checking capabilities. Once you have deployed the GEARS Client to your devices and configured your compliance policy through the GEARS Policy configuration page, the GEARS Client will store the device's compliance status within the Windows Registry or Mac OS p-list. The Dell SonicWALL Aventail® appliance can access and use this information through a simple End Point Control function, and can be used to determine if a device should be granted network access, or on a continuous basis to ensure that a device should retain network access based on the predefined security and compliance policies established by the organization.

The steps found within this document assume that this configuration is occurring with the Aventail Management Console. More information on the benefits of integrating GEARS with Dell SonicWALL Aventail® Secure Remote Access (SRA) Appliance can be found at http://www.opswatgears.com/integration/secure-access.

End Point Control

A Dell SonicWALL Aventail® Secure Remote Access (SRA) appliance can be configured to utilize OPSWAT GEARS for advanced threat detection and compliance enforcement for remote users. These checks will ensure that endpoint devices connecting to the network are meeting all compliance requirements established by the organization.

The policies can be easily configured via the GEARS Dashboard, and will enable an administrator to ensure that the security and compliance requirements of an organization are met on a continuous basis.

Device Profile Definition

In order to configure the End Point Control function, you first need to establish the Device Profiles. Navigate to *End Point Control* under *User Access*, and then select the *Device Profiles* tab.

Step 1:

Click on *New* and select *Microsoft Windows* from the drop-down list. This will open the *Device Profile Definition* window, where you can create your device profiles. We will be creating 3 device profiles: Windows 32-bit, Windows 64-bit, and Mac OSX.

Within the *Device Profile Definition* page specify the following attributes:

- Name: "GEARS-RegistryCheck-32bit"
- Description: "Compliance check of 32bit Windows endpoints for GEARS registry"

Add Attribute(s)

If you are using the persistent, installed GEARS client:

The first of 2 attributes:

- Type: Application
- Application: "GearsAgentService.exe"

Click *Add to Current Attributes*.

- Type: Windows registry entry
- Key Name: "HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Config"
- Value name: "Policy"
- Registry entry: "="
- Data: "1"

If you are using the on demand, portable GEARS client:

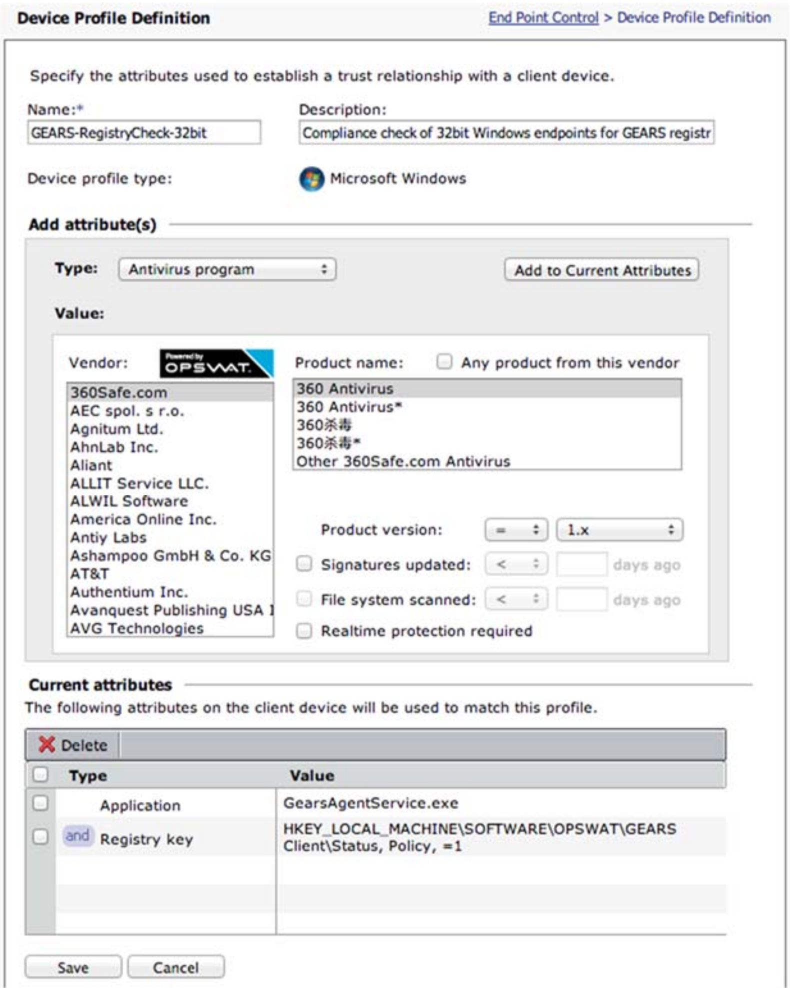
The first of 2 attributes:

- Type: Application
- Application: "opswat-gears-od.exe"

Click *Add to Current Attributes*.

- Type: Windows registry entry
- Key Name: "HKEY_CURRENT_USER\SOFTWARE\OPSWAT\GEARS OnDemand\Config"
- Value name: "Policy"
- Registry entry: "="
- Data: "1"

Click *Add to Current Attributes* and then click *Save and Add Another.*



Device Profile Definition

End Point Control > Device Profile Definition

Specify the attributes used to establish a trust relationship with a client device.

Name:* GEARS-RegistryCheck-32bit

Description: Compliance check of 32bit Windows endpoints for GEARS registr

Device profile type: Microsoft Windows

Add attribute(s)

Type: Antivirus program

Value:

Vendor: 360Safe.com

Product name: 360 Antivirus

Product version: = 1.x

Current attributes

The following attributes on the client device will be used to match this profile.

Type	Value
Application	GearsAgentService.exe
and Registry key	HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Status, Policy, =1

Step 2:

For the second *Device Profile Definition* page specify the following attributes:

- Name: "GEARS-RegistryCheck-64bit"
- Description: "Compliance check of 64bit Windows endpoints for GEARS registry"

If you are using the persistent, installed GEARS client:

Add Attribute(s)

The first of 2 attributes:

- Type: Application
- Application: "GearsAgentService.exe"

Click *Add to Current Attributes*.

- Type: Windows registry entry
- Key Name: "HKEY Local Machine\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status"
- Value name: "Policy"
- Registry entry: "="
- Data: "1"

If you are using the on demand, portable GEARS client:

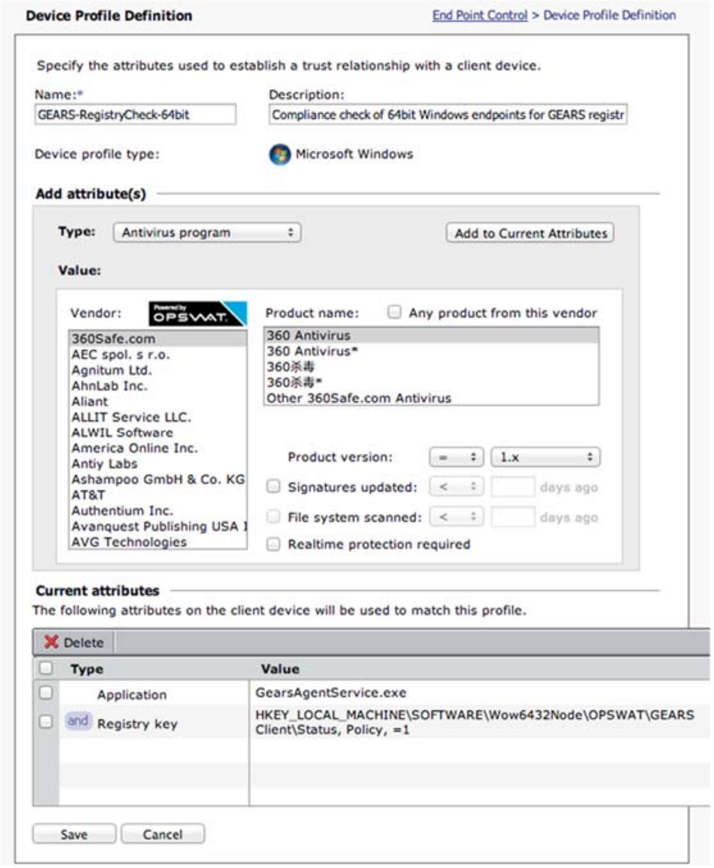
The first of 2 attributes:

- Type: Application
- Application: "opswat-gears-od.exe"

Click *Add to Current Attributes*.

- Type: Windows registry entry
- Key Name: "HKEY_CURRENT_USER\SOFTWARE\OPSWAT\GEARS OnDemand\Config"
- Value name: "Policy"
- Registry entry: "="
- Data: "1"

Click *Add to Current Attributes* and then click *Save and Add Another.*



Device Profile Definition

End Point Control > Device Profile Definition

Specify the attributes used to establish a trust relationship with a client device.

Name:* GEARS-RegistryCheck-64bit

Description: Compliance check of 64bit Windows endpoints for GEARS registr

Device profile type: Microsoft Windows

Add attribute(s)

Type: Antivirus program

Value:

Vendor: Powered by OPSWAT

360Safe.com
AEC spol. s r.o.
Agnitum Ltd.
AhnLab Inc.
Aliant
ALLIT Service LLC.
ALWIL Software
America Online Inc.
Antiy Labs
Ashampoo GmbH & Co. KG
AT&T
Authentium Inc.
Avanquest Publishing USA I
AVG Technologies

Product name: □ Any product from this vendor

360 Antivirus
360 Antivirus*
360杀毒
360杀毒*
Other 360Safe.com Antivirus

Product version: = 1.x

□ Signatures updated: < days ago

□ File system scanned: < days ago

□ Realtime protection required

Current attributes

The following attributes on the client device will be used to match this profile.

□	Type	Value
□	Application	GearsAgentService.exe
□	and Registry key	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status, Policy, =1

Step 3:

For the final *Device Profile Definition* page specify the following attributes:

- Name: "GEARS-Check-Mac"
- Description: "Compliance check of Mac endpoints for GEARS"

If you are using the persistent, installed GEARS client:

Add Attribute(s)

- Type: File name
- Value:
  - File name: "***Applications/OPSWAT GEARS Client/Policies/ GEARS_<gears license key>_1.txt"***

If you are using the on demand, portable GEARS client:

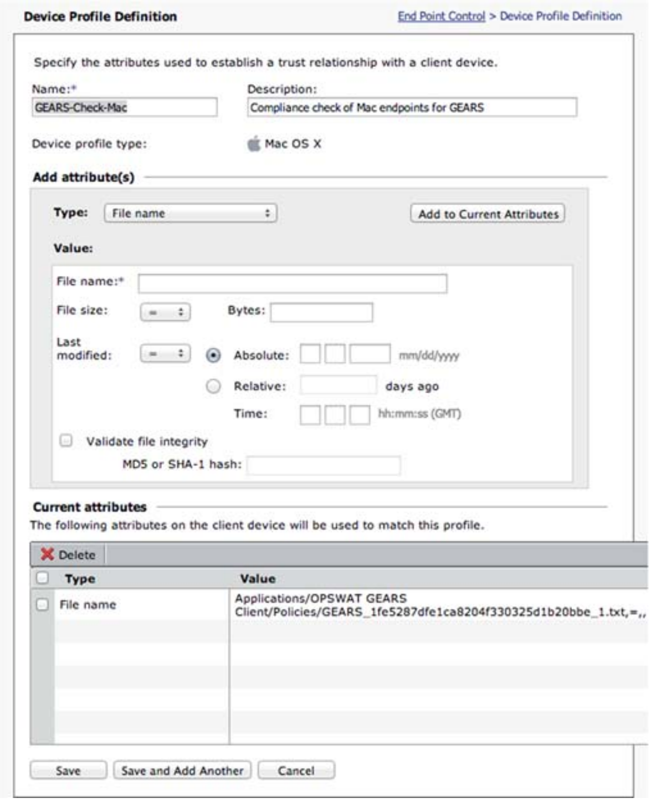
Add Attribute(s)

- Type: File name
- Value:
  - File name: "*/Users/Documents/OPSWAT/GEARS OnDemand/GEARS_<license_key>_<0 or 1>*"

Click *Add to Current Attributes*, and then click *Save.*

The file referenced, ***Applications/OPSWAT GEARS Client/Policies/ GEARS_<gears license key>_1.txt,* or */Users/Documents/OPSWAT/GEARS OnDemand/ GEARS_<license_key>_<0 or 1>*,** includes the variable *gears license key.* This value will be **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.



Device Profile Definition

End Point Control > Device Profile Definition

Specify the attributes used to establish a trust relationship with a client device.

Name:* GEARS-Check-Mac

Description: Compliance check of Mac endpoints for GEARS

Device profile type: Mac OS X

Add attribute(s)

Type: File name

Value:

File name:*

File size: = Bytes:

Last modified: = ● Absolute: mm/dd/yyyy

○ Relative: days ago

Time: hh:mm:ss (GMT)

□ Validate file integrity

MD5 or SHA-1 hash:

Current attributes

The following attributes on the client device will be used to match this profile.

□ Type	Value
□ File name	Applications/OPSWAT GEARS Client/Policies/GEARS_1fe5287dfe1ca8204f330325d1b20bbe_1.txt,=,,

Your *Device Profiles* should now include your 3 new profiles. You can now navigate to End Point Control Zones, to establish how you wish to manage the devices with these policies. Depending on your preference you can create a Standard Zone, Deny Zone, or Quarantine Zone. Within these zones you are able to define the action the network should take when the devices pass the established policies or fail the established polices. The checks can be a one-time check when the endpoint logs in, or it can be a continuous check that validates the compliance state of the endpoint throughout the time within the network.

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.