OPSWAT Quick Integration Guide

for PacketFence version 7.4.0

OPSWAT Quick Integration Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

Table of Contents

Chapter 1

About this Guide

This guide has been created in order to help sales engineers, product managers, or network specialists demonstrate the PacketFence capabilities on-site with an existing or potential customer. It can also provide guidelines to setup a proof of concept for a potential PacketFence deployment using OPSWAT Metadefender Endpoint to provide information about device compliance before and during network access.

Assumptions

- You have a configured PacketFence environment with working test equipment;
- You have, or will create, an OPSWAT Metadefender Endpoint account at https://www.opswat.com/products/metadefender/endpoint/management/.
- You are aware of the licensing options available at https://www.metadefender.com/licensing

Quick installation

Step 1: Configure OPSWAT Metadefender Endpoint

You will first need to create an OPSWAT Metadefender Endpoint account at https://www.opswat.com/products/metadefender/endpoint/management/ and configure your account according to OPSWAT's documentation.

Step 2: Developer account

Now that you have basic functionality for your OPSWAT Metadefender Endpoint account, you will need to create a Metadefender Endpoint developer account so PacketFence can access the OPSWAT Metadefender Endpoint API. You can do this here https://gears.opswat.com/developers.

Creating the application

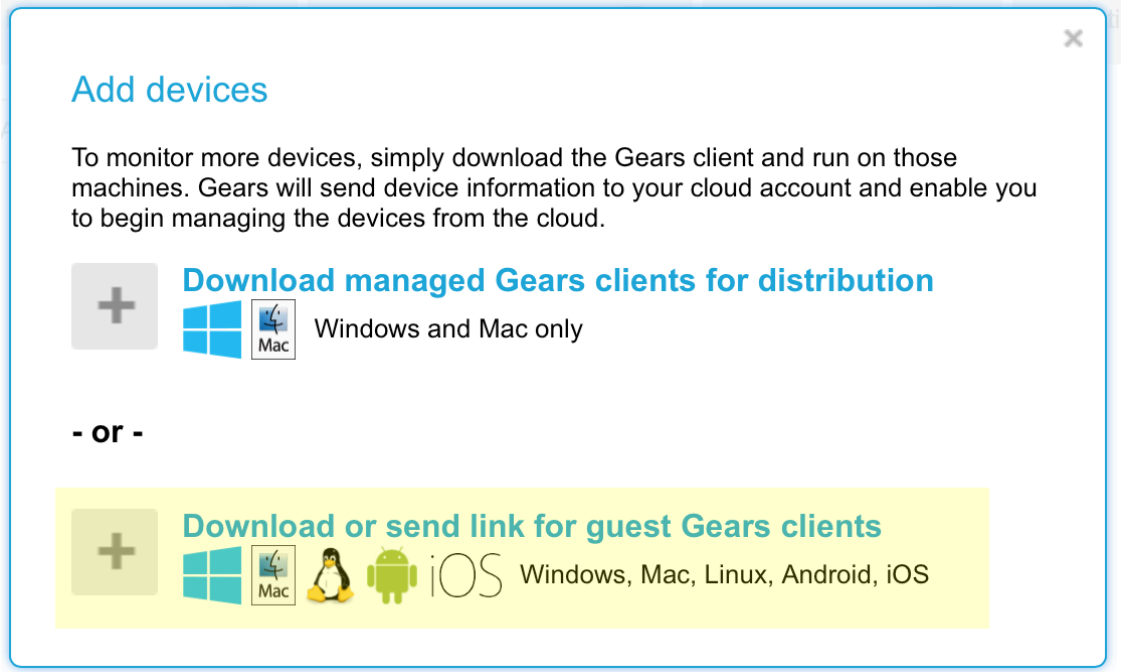
Once this is done, click *Register a new application*. The only thing important here is to set the callback URL to http://127.0.0.1/opswat.

Once you created the application, note the client key and client secret for usage below.

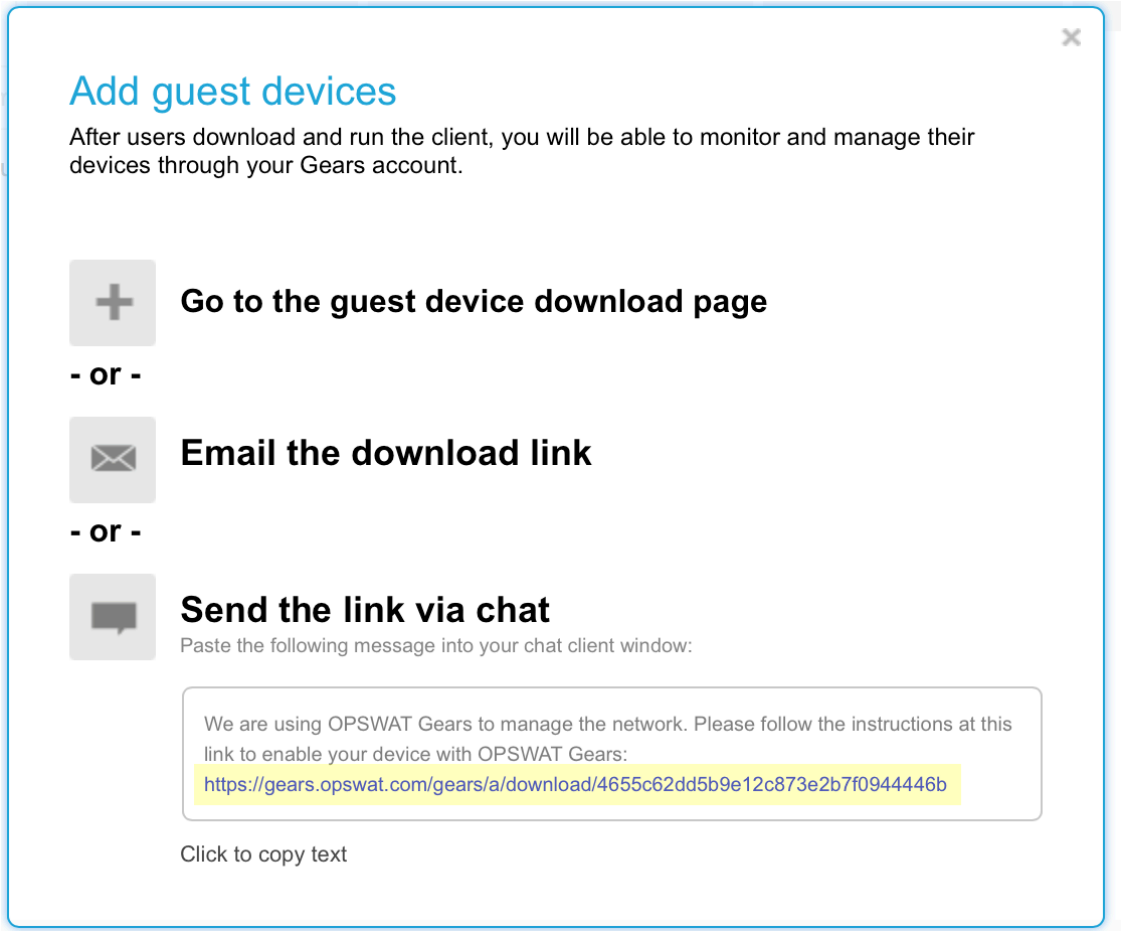
Step 3: Gathering the install URL

From your OPSWAT Metadefender Endpoint console, click *+Devices* at the top. Then click on Enable *Metadefender Endpoint client on another device*.

Then click *Download or send link for guest Metadefender Endpoint clients*



Then note the URL at the bottom of the screen.



Step 4: API access

In order to configure OPSWAT Metadefender Endpoint in PacketFence you will need to generate an OAuth2 access and refresh token so PacketFence can access the OPSWAT Metadefender Endpoint API.

Generate the authorization code

First you will access this page using your browser (replace `-clientid-` by your client ID that you got when creating the application):

```
https://gears.opswat.com/o/oauth/authorize?client_id=-clientid-
&response_type=code&redirect_uri=http://127.0.0.1/opswat
```

Authorize the application and you will then be redirected to an unavailable page but the URL will contain the code in it's parameters (ex: `http://127.0.0.1/opswat?code=wJ2RTE`).

Generate the access and refresh token

We will now use the code at the end to generate the access and refresh token using another HTTP request that will be done in your browser. Replace `-clientid-` and `-clientsecret-` by the client id and secret of your application. Then add the code you got above at the end of this URL.

```
https://gears.opswat.com/o/oauth/token?client_id=-clientid-&client_secret=-
clientsecret-&grant_type=authorization_code&redirect_uri=http://127.0.0.1/
opswat&code=
```

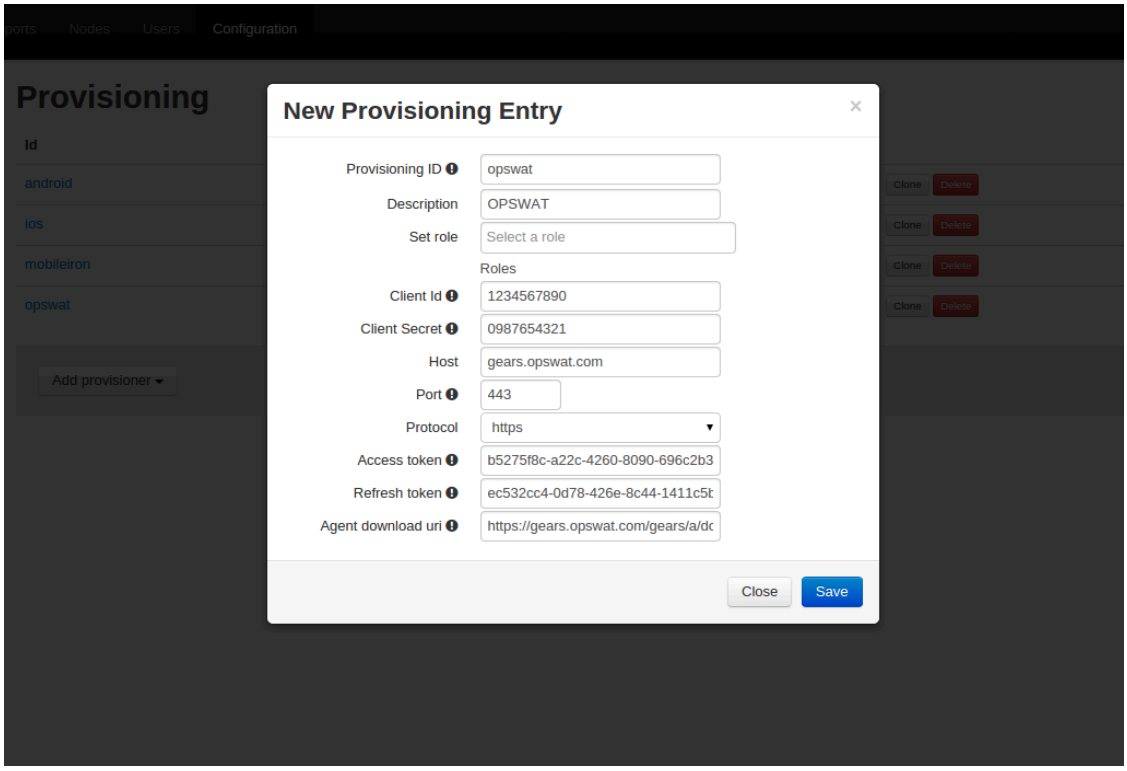
You should now be presented with a JSON response that contains the access and refresh token. Take note of both of these values for the PacketFence configuration. Example:


```
{"access_token":"ab3aec71-fa6a-4752-8804-00c37f934059","token_type":"bearer",
 "refresh_token":"f9e7c698-4d88-42cb-b9ae-c067557e8385","expires_in":43199,
 "scope":"read","client_id":"1234567890"}
```


Step 5: Configure PacketFence

Create a new provisioner

Login in the PacketFence administration interface, then go in the *Configuration* tab, then in *Provisioners*. Click *Add provisioner* then select opswat.

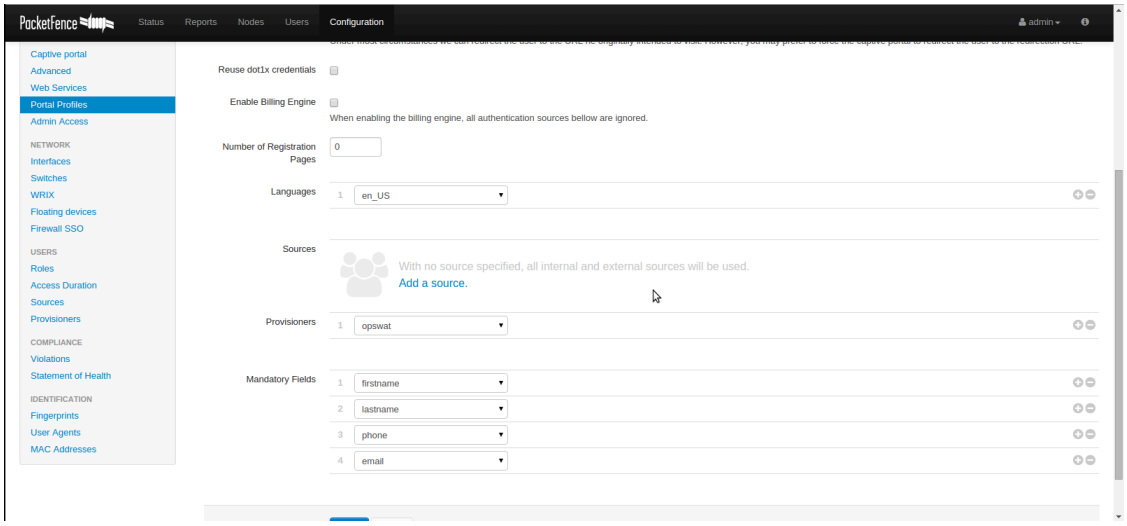


Now configure this new provisioner with the information you got above.

- The Provisioning ID is the friendly name of the provisioner.
- The Client Id is the ID of the application you created in the developer account.
- The Client Secret is the secret of the application you created in the developer account.
- The default host should work if you have a cloud account, if not adapt it to your local instance.
- The port and protocol should be left to default.
- The access and refresh token are the tokens you got at the end of step 4.
- The *Agent download uri* is the one you got in step 3.

Add the provisioner to the profile

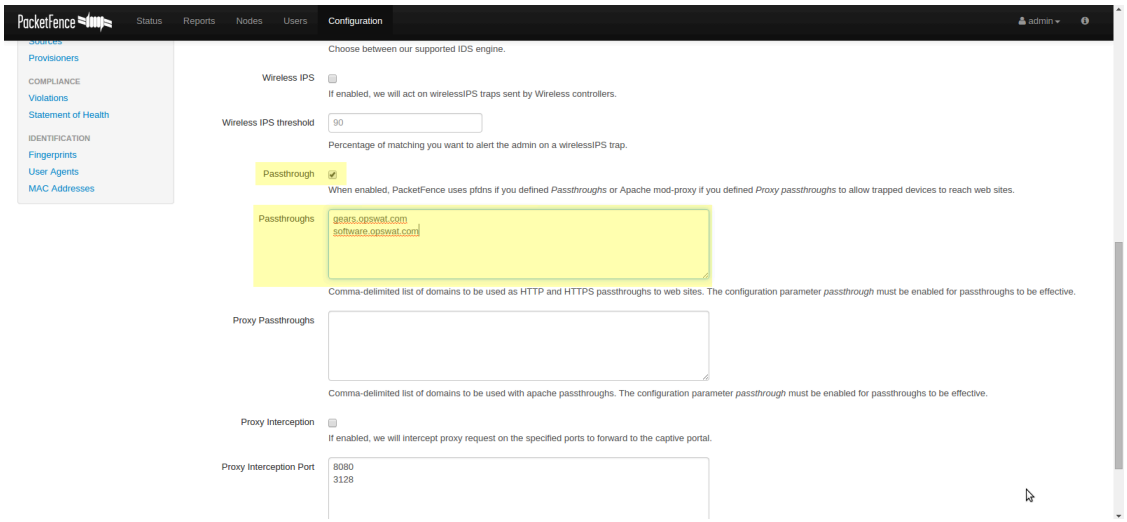
Now that you have created the provisioner, go in the *Connection Profiles* menu on the left and select the default portal. Click *Add Provisioner* and select the new OPSWAT Metadefender Endpoint provisioner that was created earlier.



Step 6: Add the necessary passthroughs

Next, still in the PacketFence administration console, go in *Fencing* in the left menu, then scroll then to *Passthroughs*. Check the *Passthrough* box above the field and add the following domains to the passthrough list.

- gears.opswat.com
- software.opswat.com
- opswat-gears-cloud-clients.s3.amazonaws.com



Step 7: Test

You can now test that the installation of the OPSWAT Metadefender Endpoint client is mandatory after the device registration. Connect a device to your test network and register like you normally would. At the end of the registration process you will be presented a page asking you to install the OPSWAT Metadefender Endpoint client on your device. After you install the client click continue. If your access is enabled than this means the connectivity between PacketFence and OPSWAT Metadefender Endpoint is good.

Compliance enforcement

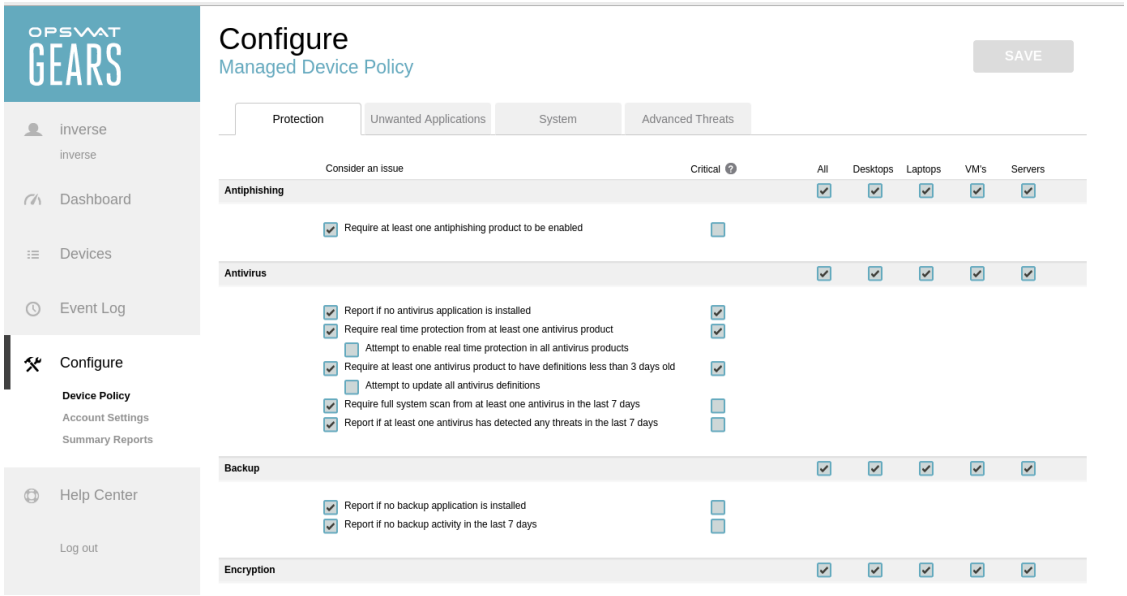
PacketFence polls the OPSWAT Metadefender Endpoint API in order to trigger violations on noncompliant devices.

PacketFence uses the number of critical issues the device has to determine whether or not it needs to isolate it.

Step 1: Configure OPSWAT Metadefender Endpoint

First you need to configure what you consider as a critical issue in your OPSWAT Metadefender Endpoint console.

You will do that through the *Configure* menu. Then you'll see a column that allows you to flag what is considered as a critical issue.



Step 2: Configure PacketFence

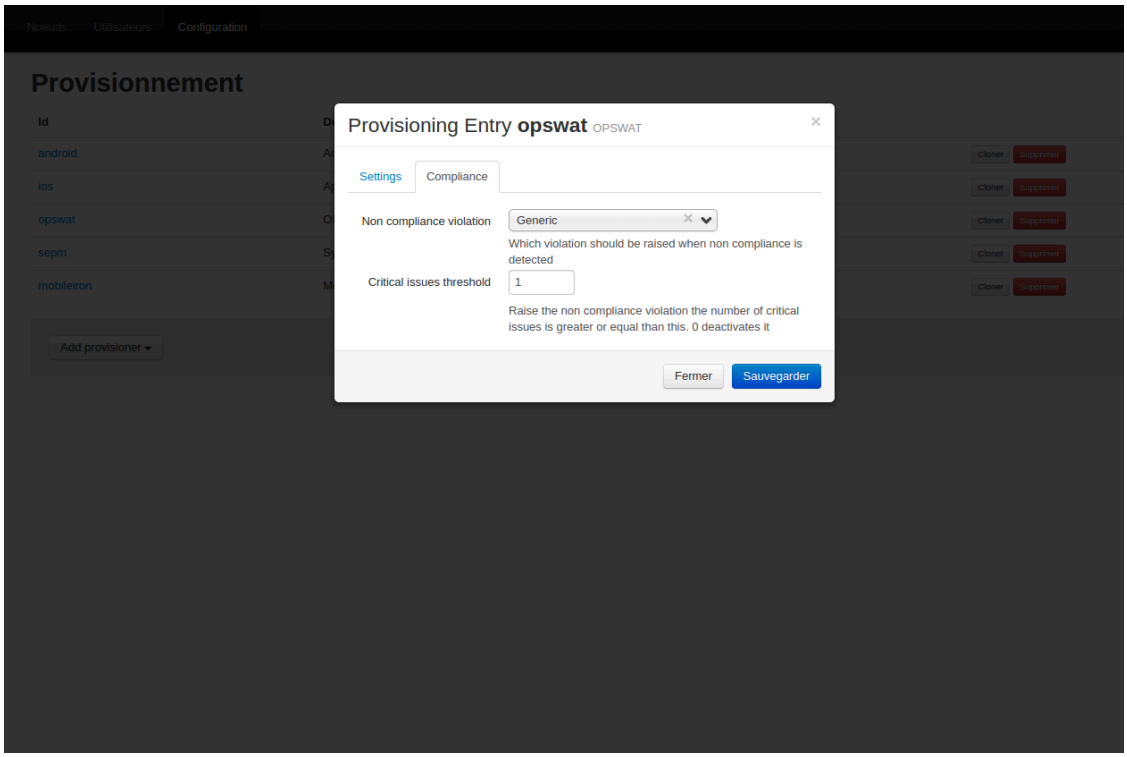
Now in order to enforce the compliance of the devices using the flagged critical issues above, you will need to configure the provisioner you created above to activate the enforcement.

Back in the provisioner configuration, go in the *Compliance* tab.

You now have to configure the violation that is raised when a device is noncompliant. Using the violation *Generic* should fit your needs for now, and you can modify the template after.

Then configure the *Critical issues threshold* and put it at the minimum critical issues a device needs to have before it gets isolated.

Putting 1 into that field will isolate the device whenever there is at least one critical issue with the device.



You can then hit *Save* and now the device will get isolated whenever it's found as noncompliant.

Step 3: Customize the template

You can now customize the template the violation is using in the *Connection Profile* section. Simply select your connection profile and then go in the *Files* tab.

You can then modify the template violations/generic.html so it displays additional information.

You can also customize this violation in the *Violations* section of the administration interface. Refer to the PacketFence Administration Guide for additional information about this.