Symantec Endpoint Protection Manager Quick Integration Guide

for PacketFence version 5.0.0

Symantec Endpoint Protection Manager Quick Integration Guide

by Inverse Inc.

Version 5.0.0 - Mar 2015

Table of Contents

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 the Symantec Endpoint Protection Manager to provide information about device compliance before and during network access.

For brievity and better lisibility, the Symantec Endpoint Protection Manager will be refered as *SEPM* in the rest of this document.

Assumptions

- You have a configured PacketFence environment with working test equipment
- You have a working Symantec Endpoint Protection Manager server

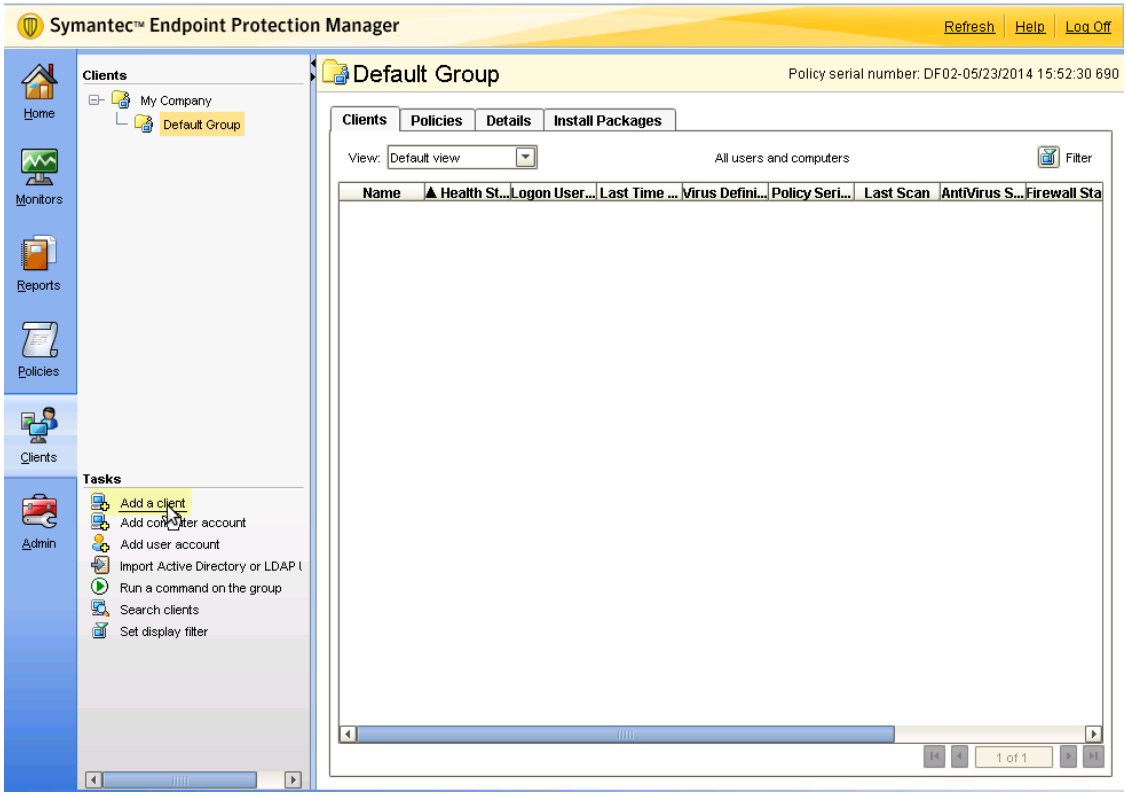
Quick installation

Step 1: Configure the SEPM

Configure the necessary policies in your SEPM before the creation of the install package. This document does not cover the policy and group configuration. Please refer to Symantec's documentation for more information. This document will use the default policies and the default group for the package creation.

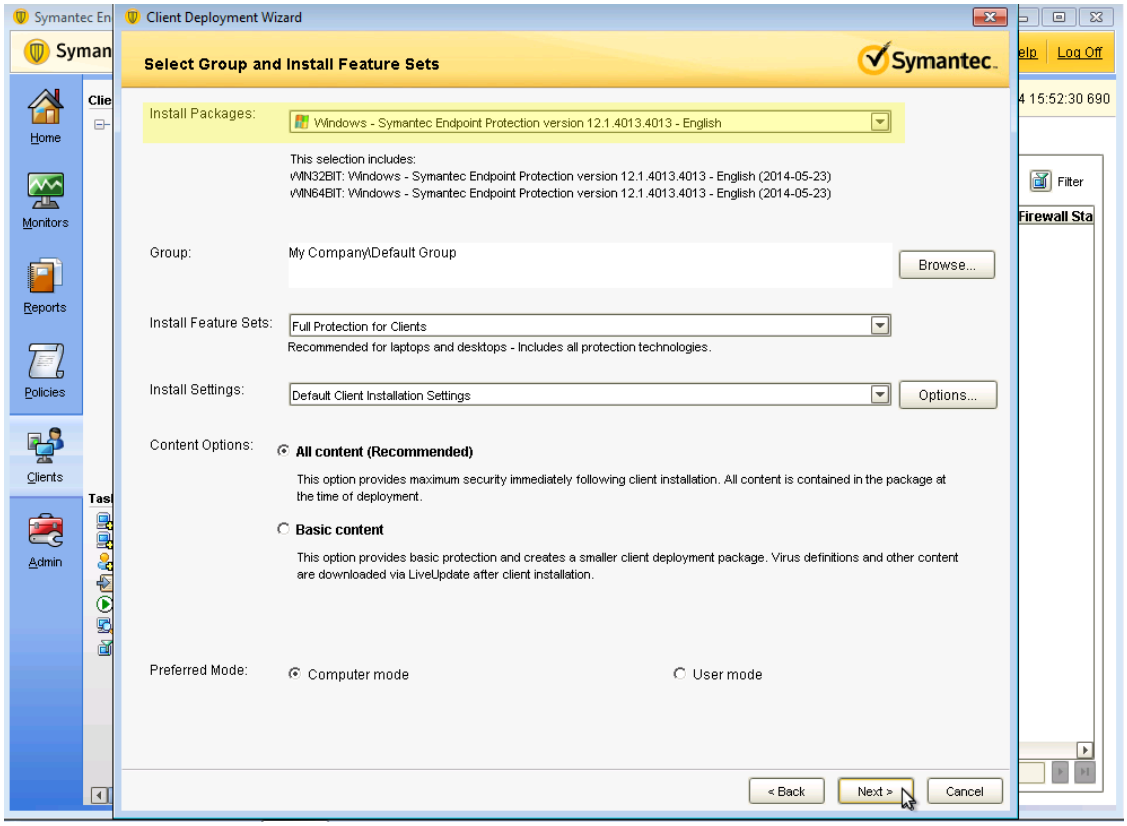
Step 2: Create the install package

Login in your SEPM console and then go in the *Clients* tab on the left. Select the group your clients should belong and then click *Add a client*.



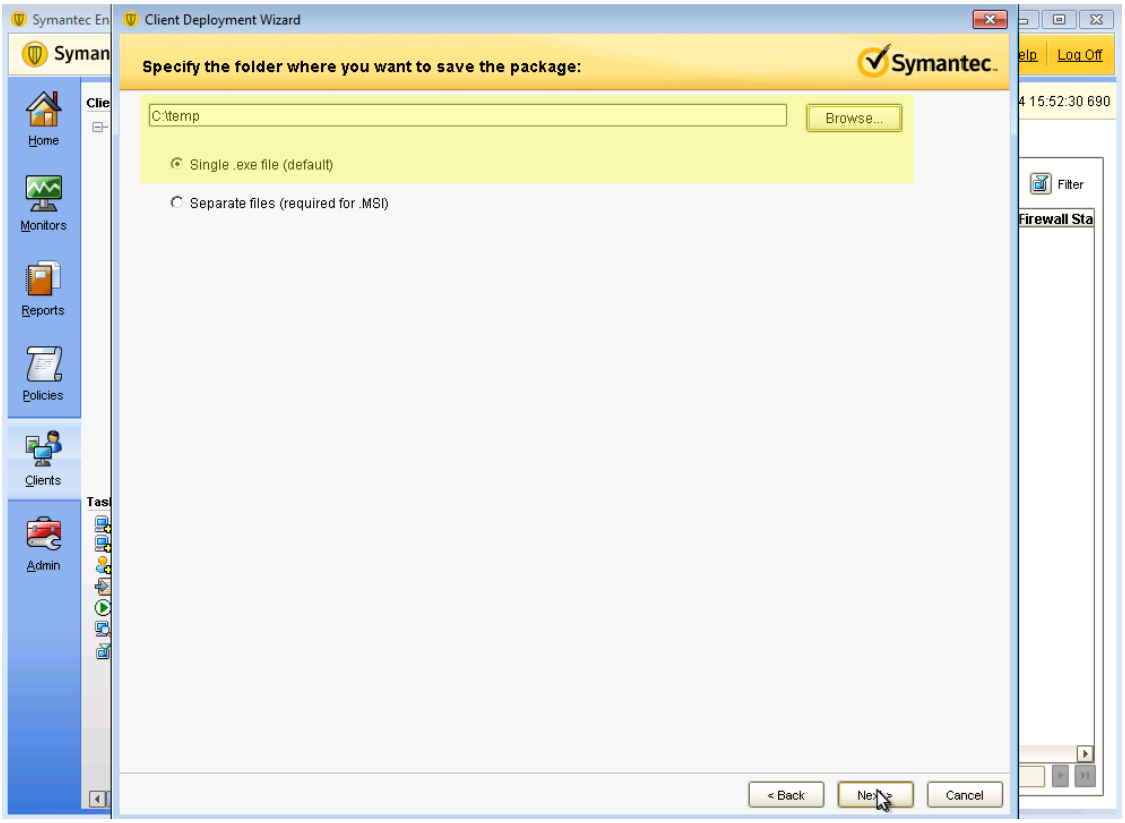
The wizard for the package creation will open. On the first page, make sure *New Package Deployment* is selected and click *Next*.

Now on this page, make sure you are creating the package for Windows. Then select the content options you prefer and click *Next*.



Now on this page, select *Save Package* and click *Next*.

Now you will need to select the export location of your new packages. Select any location you prefer. This guide will use `C:\temp\`. Once you are done, click *Next*.



On the next page, confirm the settings and click *Next*.

Once the package is created go in the directory where you created the package and navigate your way to the 32 bit package. Then using an SCP or any other method, upload this file to `/usr/local/pf/html/captive-portal/content/sep.exe` on your PacketFence server. Do the same thing for the 64 bit package by uploading it to `/usr/local/pf/html/captive-portal/content/sep64.exe`.

Step 3: API access

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

Note

The next steps use `192.168.1.100` as the SEPM address. Adapt the URLs to your own SEPM address.

Create an application

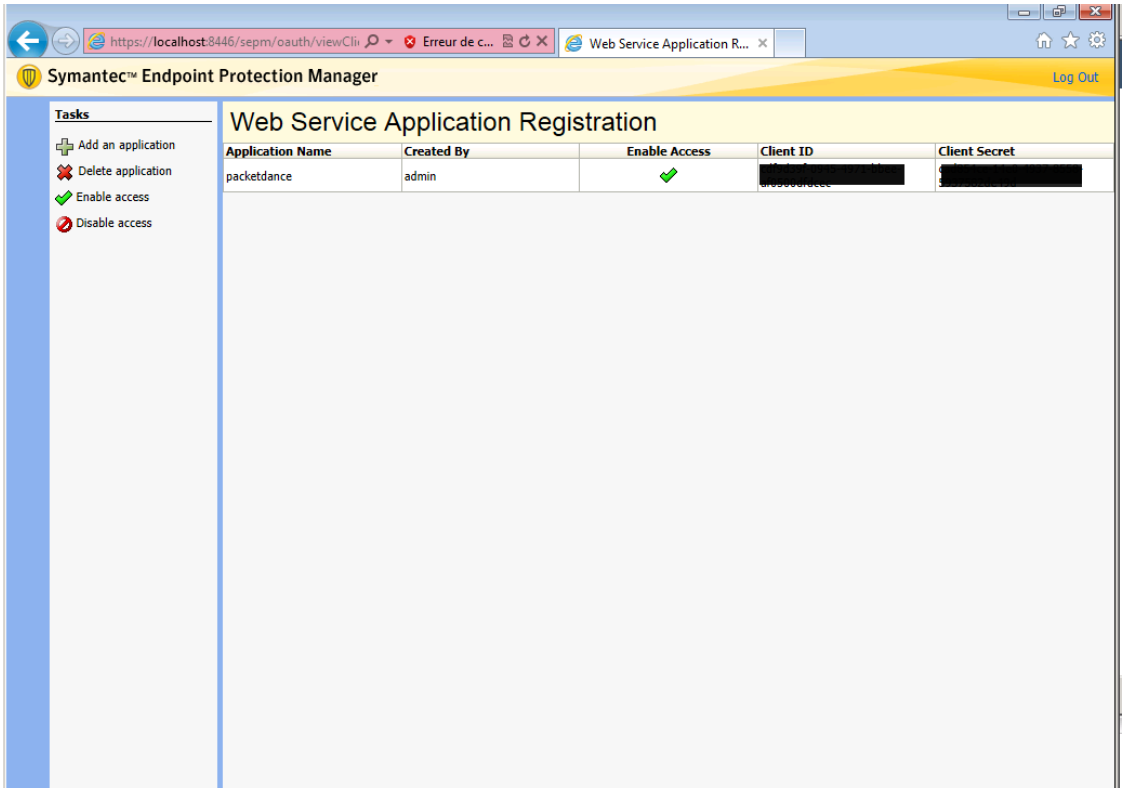
On your computer open a browser and access https://192.168.1.100:8446/sepm.

Accept any certificate error and login with your SEPM credentials.

On the left of the screen, click *Add an application* and give it a name.

You should now see your application in the list on the right.

Take note of the *Client ID* and *Client Secret* of your application



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://192.168.1.100:8446/sepm/oauth/authorize?response_type=code&client_id=-clientid-&redirect_uri=http://localhost/
```

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/?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://172.21.2.186:8446/sepm/oauth/token?grant_type=authorization_code&client_id=-clientid-&client_secret=-clientsecret-&redirect_uri=http://localhost/&code=
```

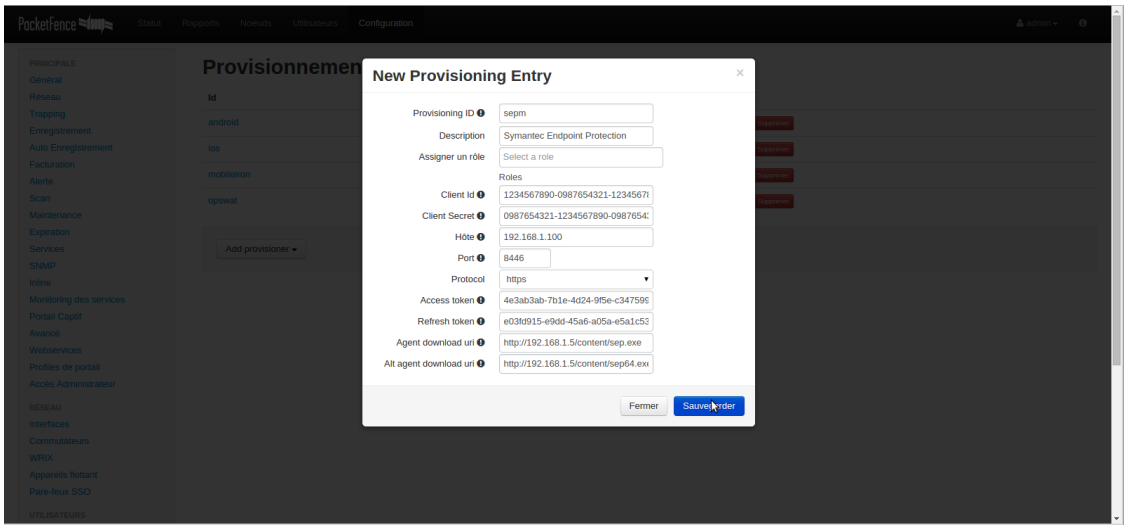
You should now be presented with a JSON response that contains the access and refresh token. Take note of both of these values for the PacketFence configuration. Example:

```
{"access_token":"4e3ab3ab-7b1e-4d24-9f5e-c347599a8a72","token_type":"bearer",
 "refresh_token":"e03fd915-e9dd-45a6-a05a-e5a1c53c1ccd","expires_in":43199}
```

Step 4: 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 sepm.

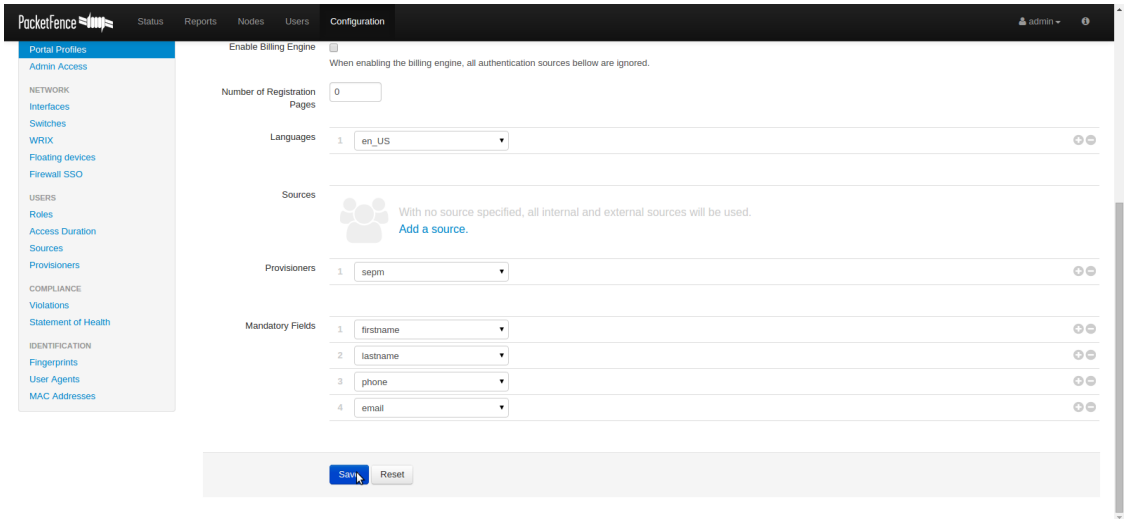


Now configure this new provisioner with the information you got above.

- The Provisioning ID is the friendly name of the provisioner.
- The Client Id is the ID of the application you created in above.
- The Client Secret is the secret of the application you created above.
- The host is the IP address of your SEPM.
- The port and protocol should be left to default.
- The access and refresh token are the tokens you got at the end of step 3.
- The *Agent download uri* is the HTTP path where we placed the 32 bit package on step 2. In this example it should be `http://packet.fence/content/sep.exe` where `packet.fence` is the domain name of the registration website of your PacketFence server.
- The *Alt agent download URI* is the HTTP path where we placed the 64 bit package on step 2. In this example it should be `http://packet.fence/content/sep64.exe` where `packet.fence` is the domain name of the registration website of your PacketFence server.

Add the provisioner to the profile

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



Restart PacketFence

In order to enable the boarding passthrough for the device enrollment, you will need to restart the iptables service of PacketFence.

You can do this using the command line by doing `/usr/local/pf/bin/pfcmd service iptables restart` or in the administration interface under *Status / Services*.

Step 5: Test

You can now test that the installation of the Symantec Endpoint Protection 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 Symantec Endpoint Protection client on your device.

After you install the client click *Continue*. If your access is enabled than this means the connectivity between PacketFence and the Symantec Endpoint Protection Manager is working.