

Symantec Endpoint Protection Manager Quick Integration Guide

for PacketFence version 7.4.0

Symantec Endpoint Protection Manager Quick Integration Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018 Copyright © 2014 Inverse inc.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The fonts used in this guide are licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <u>http://</u><u>scripts.sil.org/OFL</u>

Copyright © Łukasz Dziedzic, http://www.latofonts.com, with Reserved Font Name: "Lato".

Copyright © Raph Levien, <u>http://levien.com/</u>, with Reserved Font Name: "Inconsolata".

inverse

Table of Contents

About this Guide	1
Assumptions	2
Quick installation	3
Step 1: Configure the SEPM	3
Step 2: Create the install package	3
Step 3: API access	5
Step 4: Configure PacketFence	7
Step 5: Test	8

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 brevity and better visibility, the Symantec Endpoint Protection Manager will be referred 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*.

🔘 Syr	nantec™ Endpoint Protectio	n Manager	Refr	esh Help Log Off
	Clients	Default Group	Policy serial number: DF02-0	5/23/2014 15:52:30 690
	L 🕞 Default Group	Clients Policies Details Install Packages	All users and computers	Filter
Monitors			yn us denni, Poirty Seri Last Scan Anus	<u>nus 3 ri ewai 3(a</u>
Clients				
Admin	Tasks Add a cleft Add colort Add colort Import Active Directory or LDAP I Import Active Directory or LDAP I Run a command on the group Search clients Set display filter			
		4	II X	► 1 of 1 ► FI

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*.

🛡 Symanteo	: En	🔘 Client Deployment W	lizard	×	
🔘 Sym	an	Select Group an	d Install Feature Sets	Symantec.	elp Log Off
Home	Clie =-	Install Packages:	Mindows - Symantec Endpoint Protection version 12.1.4013.4013 - English		<mark>4 15:52:30 690</mark>
 Monitors			This selection includes: WIN32BIT: Windows - Symantec Endpoint Protection version 12.1.4013.4013 - English (2014-05-23) WIN64BIT: Windows - Symantec Endpoint Protection version 12.1.4013.4013 - English (2014-05-23)		Filter
		Group:	My Company/Default Group	Browse	
Reports		Install Feature Sets	Full Protection for Clients Recommended for laptops and desktops - Includes all protection technologies.		
Policies		Install Settings:	Default Client Installation Settings	Options	
Qlents		Content Options:	 All content (Recommended) This option provides maximum security immediately following client installation. All content is contained in the prive time of deployment. Basic content This option provides basic protection and creates a smaller client deployment package. Virus definitions and care downloaded via LiveUpdate after client installation. C Computer mode C User mode 	eackage at	
	•		< Back Next >	Cancel	

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*.

関 Symantec	En 🔍 Client Deployment Wizard	× • • ×
🔘 Syma	an Specify the folder where you want to save the package:	ec. elp Log Off
Home C	C.ttemp Browse	4 15:52:30 690
Monitors	 Single .exe file (default) Separate files (required for .MSI) 	Filter
Peports		
Policies		
Clients	as	
<u>A</u> cimin		
	< Back Neitz Cam	

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.

\bigtriangledown	

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 <u>https://192.168.1.100:8446/sepm</u>.

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

🔶 🥑 🏉 https://localhosta	8446/sepm/oauth/viewCliv	O → 😵 Erreur de c 🗟 🖒 🗙 🍊	Web Service Application F	2 ×	☆ 🔅
Symantec™ Endpoint	Protection Manage	r			Log Out
	-				
Tasks	Web Service	e Application Regis	stration		
Add an application	Application Name	Created By	Enable Access	Client ID	Client Secret
Delete application	packetdance	admin	~	cdfadaaf-0945-1971-b af0500dfdcec	ond854cm14e0=4937-8550 9937582de49d
Chable access					
Oisable access					

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.

	Provisionnemen	New Provisionin	ng Entry	×		
	ld					
	android	Provisioning ID 9	sepm			
	las	Description	Symantec Endpoint Protection			
	105	Assigner un rôle	Select a role		Apprimer	
	mobileiron		Roles		supprimer	
	opswat	Client Id 9	1234567890-0987654321-1234567			
		Client Secret 9	0987654321-1234567890-0987654:			
		Hôte 9	192.168.1.100			
	Add provisioner 👻	Port Ø	8446			
		Protocol	https			
		Access token U	4e3ab3ab-7b1e-4d24-9f5e-c347599			
		Refresh token 0	e03fd915-e9dd-45a6-a05a-e5a1c53			
		Agent download uri	http://192.168.1.5/content/sep.exe			
		Alt agent download uri 🛛	http://192.168.1.5/content/sep64.exr			
			Fermer	Sauvegorder		
UTILISATEURS						

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 *Connection Profiles* menu on the left and select the default portal. Click *Add Provisioner* and select the new SEPM provisioner that was created earlier.

PacketFence 🕬 Status		Configuration	🛓 admin 👻 🤨
Portal Profiles	Enable Billing Engine		
Admin Access		When enabling the billing engine, all authentication sources bellow are ignored.	
NETWORK	Number of Registration		
Interfaces	Pages	0	
Switches			
WRIX	Languages	1 en_US •	00
Floating devices			
Firewall SSO			
LISEDS	Sources		
Roles		With no source specified, all internal and external sources will be used.	
Access Duration		Add a source.	
Sources			
Provisioners	Provisioners	1 sepm •	00
COMPLIANCE			
Violations			
Statement of Health	Mandatory Fields	1 firstname •	00
IDENTIFICATION			0.0
Fingerprints		A Resultance	
User Agents		3 phone •	00
MAC Addresses		4 email •	00
		Control Double	
		Sav Reset	

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.