SentinelOne Quick Integration Guide

for PacketFence version 7.4.0

SentinelOne Quick Integration Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

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 SentinelOne to provide information about device compliance before and during network access.

Assumptions

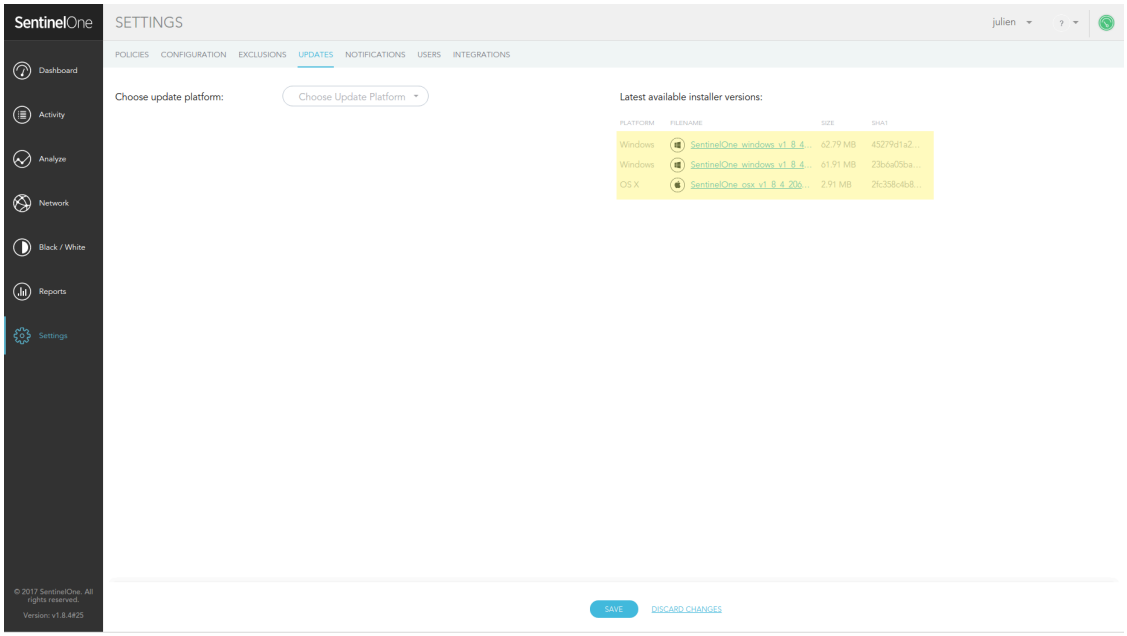
- You have a configured PacketFence environment with working test equipment;
- You have a SentinelOne instance available (this example uses `packetfence.sentinelone.net`)

Quick installation

Step 1: Download the agents

You will first need to download the SentinelOne agents in order to host them on the PacketFence server.

In order to do so, in your SentinelOne management console, go in *Settings→Updates*, then download the Windows and Mac OSX agents on your computer. Once they have been download transfer them on your PacketFence server using SCP. This example will use `/usr/local/pf/html/common/SentinelOne.exe` as the Windows agent path and `/usr/local/pf/html/common/SentinelOne.pkg` as the Mac OSX agent path.

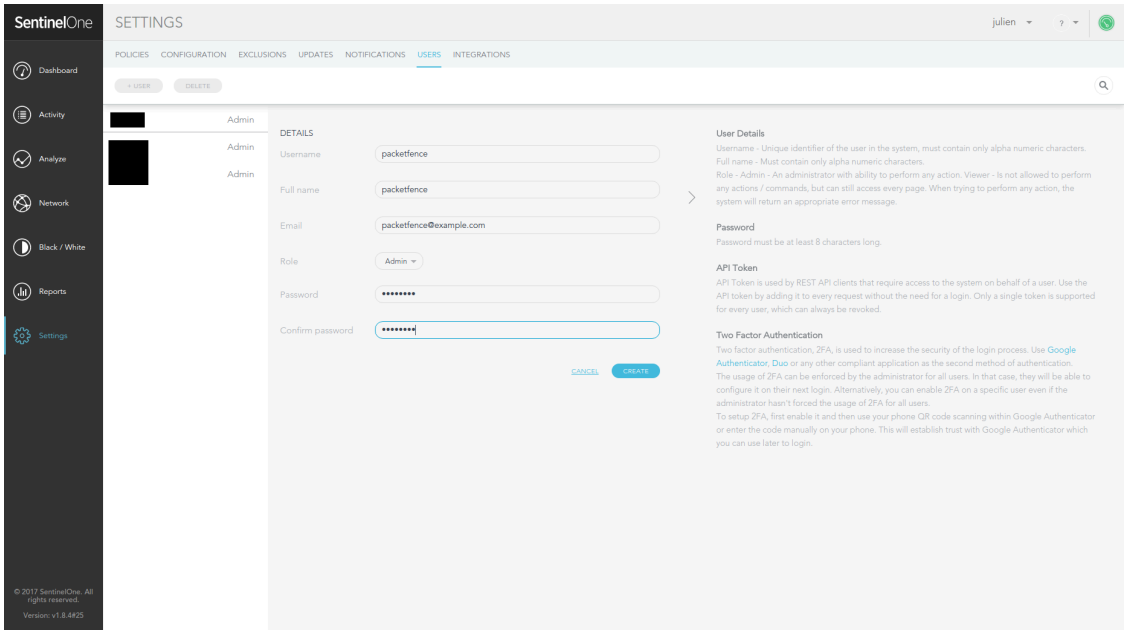


Note

All files in `/usr/local/pf/html/common/` are accessible to users that are on the captive portal. Make sure you put the agents file there or in another user-accessible location.

Step 2: Create an API user

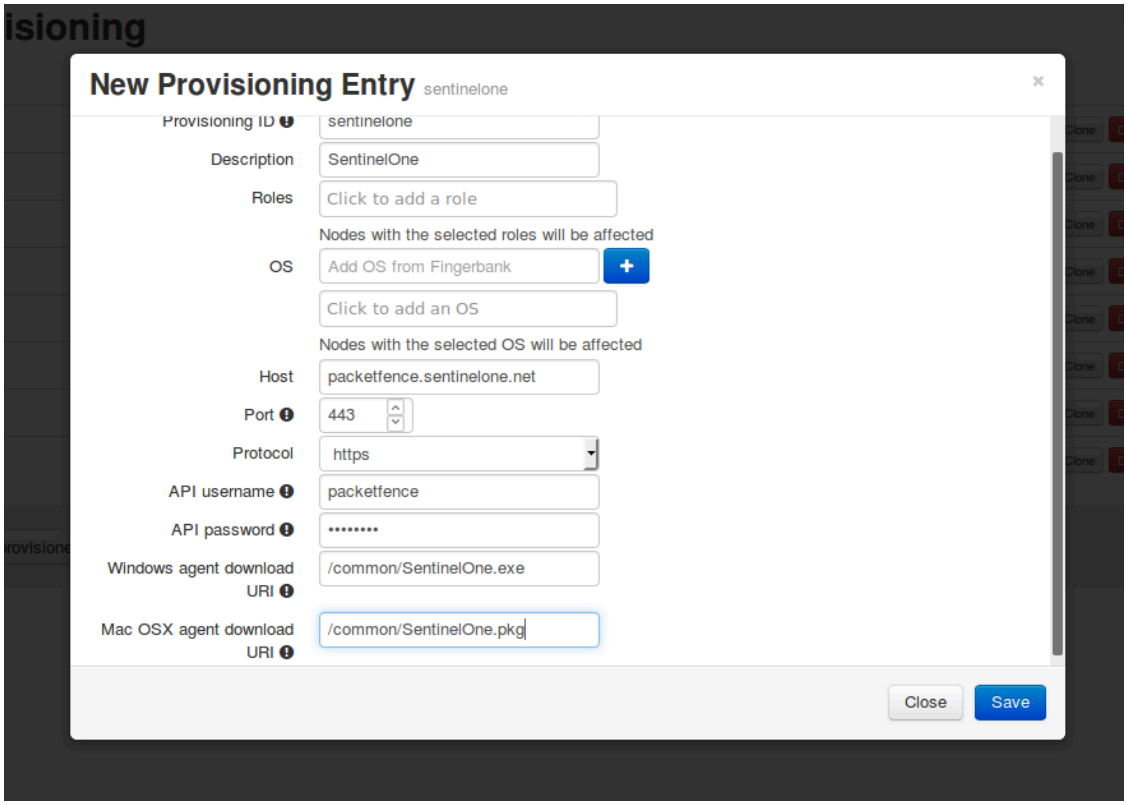
PacketFence will need a user on your SentinelOne instance in order to access the SentinelOne API. To create it, go in *Settings→Users* and create a new user. Make sure, you note the password you put here for configuration in PacketFence.



Step 3: 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 `SentinelOne`.



Where:

- *Provisioning ID* is the user-defined identifier of the provisioner.
- *Description* is a user friendly description of the provisioner.
- *Host* is the hostname of your SentinelOne instance.
- *Port* should be left to default unless your SentinelOne management console is on another port.
- *API username* is the username of the user you created above in SentinelOne.
- *API password* is the password of the API user.
- *Windows agent download URI* is the URI on which the users should download the Windows agent. If you followed the path in this guide, it should be `/common/SentinelOne.exe`.
- *Mac OSX agent download URI* is the URI on which the users should download the Mapf::errorc OSX agent. If you followed the path in this guide, it should be `/common/SentinelOne.pkg`.

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 connection profile. Click *Add Provisioner* and select the new SentinelOne that was created earlier.

Note

Make sure you have passthroughs enabled before proceeding further. Instructions on how to enable passthroughs can be found in the *Passthroughs* section of the Administration Guide.

Once you have completed the configuration, you need to restart pfdns in order for the SentinelOne specific passthroughs to be taken into consideration.

```
# /usr/local/pf/bin/pfcmd service pfdns restart
```

Step 4: Test

You can now test that the installation of the SentinelOne 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 SentinelOne client on your device. After you install the client click continue. If your access is enabled then this means the connectivity between PacketFence and SentinelOne is good.

PacketFence polls SentinelOne at a regular interval (30 seconds by default) to find devices that have uninstalled their agent. When it detects them as uninstalled, it automatically brings the device back to the portal so the agent is installed.

Everytime your device connects to PacketFence using RADIUS, it schedules a provisioning check to occur 2 minutes after the connection (controlled via violation 1300002). If the agent is inactive on the device or was uninstalled, PacketFence will bring the device back to the portal so the agent is installed again or brought back to an active state.