



Cisco MSE Quick Installation Guide

for PacketFence version 7.4.0

Cisco MSE Quick Installation Guide

by Inverse Inc.

Version 7.4.0 - Jan 2018

Copyright © 2018 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: <http://scripts.sil.org/OFL>

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

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

9279VnJ

Table of Contents

About this Guide	1
Assumptions	2
Portal based on localization	3
Step 1: Enable httpd.collector service on PacketFence	3
Step 2: Create a notification	3
Step 3: Configure a portal filter	4
MSE Tab	5

About this Guide

This guide has been created to give a quick start to configure the Cisco MSE with PacketFence 6.3+. In the first section we will explain how to use the Cisco MSE in order to present a captive portal based on the localization. Then in the second section we will integrate the device localization in the node view.

Assumptions

- You have at least one server with PacketFence 6.3 or later.
- The PacketFence management IP will be 192.168.1.5.
- An account has been created on the MSE in order to use RESTful API of the MSE. (Read only for localization , write to create notifications)
- The Cisco MSE IP will be 192.168.1.6.

Portal based on localization

Step 1: Enable httpd.collector service on PacketFence

This service is mandatory and will receive the mse notifications in json format. To enable this service go in **Configuration** -> **services** and tick `services.httpd_collector` and leave the default order.

`services.httpd_collector` Should httpd.collector be started ? Keep enabled unless you know what you're doing.

`services.httpd_collector_order` Order in which the service should be started.Lower order services start first and stop last.

Step 2: Create a notification

This part can be done directly on the MSE web admin GUI but we include a Perl script in `addons/mse-subscribe.pl` that will help you to create one using the RESTful API of the MSE.

So let say that you have a username with write permissions on the MSE (`mswrite/password`) now go in `/usr/local/pf/addons` then run:

```
./mse-subscribe.pl --username=msewrite --password=password --  
url=http://192.168.1.6:8083 --target-ip=192.168.1.5 --target-port=9292 --url-  
path=/mse/ --zone=Campus>Building>Level>Zone --notification-name=Zone1
```

This will create the notification and print out the notifications configured on the MSE. So now each time a device will enter or leave the specific zone PacketFence will be notified.

Step 3: Configure a portal filter

In Configuration Policies and Access Control -> Connection Profiles -> Add profile -> Advanced filter specify an advanced filter like that:

```
extended.mse_inout.locationMapHierarchy == "Campus>Building>Level>Zone"
```

The screenshot shows the PacketFence Configuration interface. The left sidebar contains a navigation menu with the following items: Advanced, OMAPI, Web Services, Monitoring, Clustering, Metadefender, Node MSE Tab, Portal Modules, Portal Profiles (highlighted), Admin Access, Filter engines, NETWORK, Interfaces and Networks, Switches, Floating Device, Firewall SSO, WRIX, USERS, Roles, Access Duration, Sources, Billing Tiers, Provisioners, PKI Providers, and RADIUS. The main content area is titled 'Configuration' and shows the 'Portal Profiles' configuration page. The 'Advanced filter' field is highlighted with a blue box and contains the text: `extended.mse_inout.locationMapHierarchy == "Campus>Building>Level>Zone"`. Other configuration options visible include 'Automatically register devices' (unchecked), 'Reuse dot1x credentials' (unchecked), and 'Dot1x recompute role from portal' (checked). The 'Filters' section shows a dropdown menu set to 'any' and a note: 'With no filter specified, an'. The PacketFence logo is visible in the top left corner of the interface.

And fill the other configuration needed to configure a connection profile then save it.

That's all, now when a device will hit the captive portal and will be in the specific zone then it will hit this connection profile.

MSE Tab

This configuration is really simple, you just have to enable and fill the URL, the username and password in **Configuration** -> **Integration** -> **Cisco Mobility Service Engine**. So in our example:

```
URL: http://192.168.1.6:8083
Username: mseread
Password: password
```

The screenshot shows the PacketFence web interface. The top navigation bar includes 'Status', 'Reports', 'Auditing', 'Nodes', 'Users', and 'Configuration'. The left sidebar lists various configuration options, with 'Node MSE Tab' highlighted. The main content area is titled 'MSE Lookup Service' and contains the following configuration fields:

- Enable MSE**: Enable MSE
- mse_tab.url**: URL of MSE service
- Username**: Username for MSE service
- Password**: Password for MSE service

At the bottom of the configuration area, there are two buttons: 'Save' and 'Reset'.

Now go in **Nodes** and click on a MAC address and you will see that a new tab appears, then if you click on it you will be able to retrieve the map and the localization of the device.

MAC 64:89:9a:8d:4d:7a

Info Fingerbank IP Address Location Violations MSE WMI Rules

Get Current Location Get History Location

MAC Address	64:89:9a:8d:4d:7a
AP MAC Address	dc:a5:f4:8d:4a:b0
Band	UNKNOWN
Currently Tracked	1
Dot11 Status	ASSOCIATED
IP Address	10.36.34.22
Is Guest User	0
SSID	[REDACTED]
First Located Time	2016-10-27T14:13:58.746-0400
Last Located Time	2016-10-27T14:20:20.627-0400
Map Hierarchy	[REDACTED]

Reevaluate access Close Save