

# **MobileIron Quick Integration Guide**

for PacketFence version 5.0.0

#### MobileIron Quick Integration Guide

by Inverse Inc.

Version 5.0.0 - Mar 2015 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 MobileIron	
Step 2: Create an API user	4
Step 3: Gather the boarding host	6
Step 4: Configure PacketFence	6
Step 5: Add the necessary passthroughs	8
Step 6: Test	9

## 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 **MobileIron mobile device manager**.

# Assumptions

- You have a configured PacketFence environment with working test equipment;
- You have access to a MobileIron cloud account.

# **Quick installation**

### Step 1: Configure MobileIron

First of all you will need to configure the basic functionality of MobileIron using their documentation.

### MDM profile

One important step is to enable the MDM profile like in this screenshot. Note that this will require you to create an MDM certificate with Apple. Refer to the MobileIron documentation for specifics about this step.

	DASHBOARD	USERS & DEVICE	s admin	APPS	POLICIE	S & CONFIGS	SETTINGS	LOGS & EVENTS
	Preferences	Sentry Conn	ector LDA	AP Op	erators	Local CA	Service Diagnos	tics Templates •
The management of the second s								
Remove Wi-Fi settings for cellul	lar-enabled devices							
Remove Wi-Fi settings for cellul	lar-enabled and Wi-	Fi only devices						
Clear passcode								
APNs Preferences								
Use Enterprise Issued APNs certi	ificate 🕕							
View Certificate								
MDM Preferences								
Enable MDM Profile								
View MDM Alerts								
Enable Profile Encryption								
Permit expired client certificates	MDM Certific Report	ate						
Enable MDM for iOS 4.1 and grea	ater 🕕							
Install MDM Certificate	View Certific	cate						
Save User Password Preferences								
Save User Password: O Yes ()	No							
Registration PIN code Preferences								
Passcode Length: 6	(6-1	2)						
Save								

## Step 2: Create an API user

Next, we will need a user that has the rights to access the MobileIron API in order to verify the state of the devices directly from PacketFence.

First go in the USERS & DEVICES tab and then in Users and click Add local user.

Mobile Iron	DASHBOARD	USERS & DEVICES	ADMIN APPS	POLICIES & CONFIGS	SETTINGS LOGS & EVENTS
	Devices	ActiveSync Associations	Labels User	s	
Actions - Add - Resync W	ith LDAP				
EDIT Add Local User		USER ID	EMAIL		CREATION DATE
admin		admin	address@	domain.com	2014-07-31 5:17:39 PM
🔲 🖉 julien semaan		julien	jsemaan@	)inverse.ca	2014-08-06 1:28:26 PM
zammit	zammit zammit@zammit.com 2014-08-15 11:16/4			2014-08-15 11:16:40 AM	
https://m.mobileiron.net/inverseca/a	admin/vsp.html#				

Now enter the information about your user and note the user ID and password for usage in the PacketFence configuration, then hit *Save*.

ARD	USERS & DEVICES	ADMIN APPS	POLICIES & CO	ONFIGS SETTINGS	LOGS & EVENTS			
s	ActiveSync Associations	Labels Us	ers					
	USER ID admin julien pfapi zammit	Add New User First Last Displ Pass Confi Emai	v User ID Vame Vame ay Name ( vord mr Password	pfapi pf api ······· pfapi@example.com	Save	X s	To Authorized 1 OURCE  Docal   Cocal  Cocal	User Portal User Portal User Portal User Portal User Portal
-	✓ per page							

Now go in the ADMIN tab, check the box next to your newly created user and then in Actions select Assign to Space.

ADMIN: Actions  Edit Roles US Assign to Space adr julien semaan juli g pf api pfa zammit zam	IS DEVICE SPACES	EMAIL address@domain.cor jsemaan@inverse.ca pfapi@inverse.ca zammit@zammit.com	n	SOURCE Local Local Local	ROLES API, Add de
Actions - Edit Roles US Assign to Space adr julien semaan juli 7 pf api pfa zammit zar	SER ID Imin ien api immit	EMAIL address@domain.cor jsemaan@inverse.ca pfapi@inverse.ca zammit@zammit.com	n 	SOURCE Local Local Local Local	ROLES API, Add de
Edit Roles     US       Assign to Space     adr       julien semaan     julie       Ø     pf api       pf api     pfa       zammit     zar	SER ID Imin Ien api Immit	EMAIL address@domain.cor jsemaan@inverse.ca pfapi@inverse.ca zammit@zammit.com	n 	SOURCE Local Local Local Local	ROLES API, Add de
Assign to Space     adr       julien semaan     julien       grapi     pfa       zammit     zar	Imin ien api mmit	address@domain.cor jsemaan@inverse.ca pfapi@inverse.ca zammit@zammit.com	n	Local Local Local Local	API, Add de
julien semaan     julien       v     pf api     pf avi       zammit     zam	ien api ımmit	jsemaan@inverse.ca pfapi@inverse.ca zammit@zammit.com	1	Local Local Local	
Image: provide state stat	api mmit	pfapi@inverse.ca zammit@zammit.com	1	Local	
zammit zar	ımmit	zammit@zammit.com	1	Local	

Select the Global space at the top and then check API at the bottom. You should now see API in the roles list of your newly created user when viewing the users list.

## Step 3: Gather the boarding host

To find the boarding host, add a fake device to MobileIron and at the end of the process you will see the registration instructions.

In it you will find the boarding host and port for the PacketFence configuration. In this case, the boarding host is **m.mobileiron.net** and the boarding port is **50291**.



### Step 4: Configure PacketFence

In PacketFence, MDM are refered to as provisioners. This will walk you through adding MobileIron as a provisioner.

#### Create the provisioner

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

PocketFence <b>&gt;/////&gt;</b> statu	us Reports Nodes Users <b>Config</b>	uration				🛔 admin + 🛛 🛈
	Provisioning	New Provisionir	ng Entry	×		
	ld	Provisioning ID 9	mobileiron			
		Description	Mobile Iron		Clone Délete	
		Set role	Select a role		Clone Delete	
			Roles		Clone Delete	
		Username	admin		Clone Delete	
		Password 9				
	Add provisioner +	Android download uri	https://m.mobileiron.pat/inverseca/ci			
		los download uri 9	https://m.mobileiron.net/inverseca/ci			
		Windows phone download	https://m.mobileiron.net/inverseca/E			
		uri 🛛				
		Boarding host O	m.mobileiron.net			
		Boarding port 🛛	50291			
				Close Save		
				Jave Jave		

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

- The Provisioning ID is the friendly name of the provisioner.
- The Username is the user you created with API access above.
- The password is the password of the API user.
- The host is the domain name of the instance + your account name if you have a cloud account (ex: m.mobileiron.net/accountName)
- Now add the download URI for the agent. See below for more details.
- The Boarding host is the host that you got in step 3.
- The Boarding port is the port that you got in step 3.

Here are the URIs that should work by default. Replace **accountName** by your real account/instance name at MobileIron.

- Android: https://m.mobileiron.net/accountName/c/d/android.html
- IOS devices: https://m.mobileiron.net/accountName/c/d/ios.html
- Windows: https://m.mobileiron.net/accountName/EnrollmentServer/Discovery.svc

#### Add the provisioner to the portal profile

In order for the provisionner to be used by your captive portal you need to add it in its configuration. Go in *Portal Profiles*, then select the portal you want to modify and add *mobileiron* as a provisioner.

PocketFence 🕬 Status	Reports Nodes Users	Contiguration & admin + O
Registration Self Registration	Profile Name O	default
Billing Alerting	Profile Description	Default Profile
Scan Maintenance	Logo 0	/commontpacket/ence-cp.png
Expiration Services	Redirection URL 0	http://www.packetlence.org/
SNMP	Course and counting (10)	Default URL to redirect to on registration/miligation release. This is only used if a per-violation redirect URL is not defined.
Service watch Captive portal	Porce redirection ORL	Under most circumstances we can redirect the user to the URL he originally intended to visit. However, you may prefer to force the captive portal to redirect the user to the redirection URL.
Advanced	Reuse dot1x credentials	8
Web Services	Enable Billing Engine	When expline the billion engine. all authentication sources below are innored.
Admin Access	Number of Registration	
NETWORK	Pages	
Switches	Languages	1 en_US •
Floating devices		
USERS	Sources	1 nuli •
Roles		
Access Duration Sources	Provisioners	1 mobileron •

### Step 5: Add the necessary passthroughs

Next, still in the PacketFence administration console, go in *Trapping* 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.

- m.mobileiron.net
- \*.itunes.apple.com
- itunes.apple.com
- play.google.com
- \*.play.google.com

PacketFence Status Rep	oorts Nodes Users	Configuration & admin + 0
Provisioners	Wireless IPS	Choose between our supported IDS engine.
Violations Statement of Health IDENTIFICATION	Wireless IPS threshold	If enabled, we will act on wirelessIPS traps sent by Wireless controllers.  So Percentage of matching you want to alert the admin on a wirelessIPS trap.
Fingerprints User Agents MAC Addresses	Passthrough	When enabled, PacketFence uses pldns If you defined Passthroughs or Apache mod-proxy if you defined Proxy passthroughs to allow trapped devices to reach web sites.
	Passthroughs	In mobilizion nat * Amesa apple.com Marka apple.com play apple.com - play apple.com
	Proxy Passthroughs	Comma-delimited list of domains to be used as HTTP and HTTPS passthroughs to web sites. The configuration parameter passthrough must be enabled for passtbroughs to be effective.
	Proxy Interception	Comma-delimited list of domains to be used with apache passtbroughs. The configuration parameter passtbrough must be enabled for passtbroughs to be effective.
	Proxy Interception Port	If enabled, we will intercept proxy request on the specified ports to forward to the captive portal.

#### **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 6: Test

You can now test that MobileIron 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 MobileIron on your device. After you install the agent click *Continue*. If your access is enabled than this means the connectivity between PacketFence and MobileIron is good.