# MobileIron Cloud and Common Platform Service



a Hewlett Packard Enterprise company

ClearPass

Integration Guide

## **Change Log**

Version	Date	Modified By	Comments	
0.1 / 0.2	Dec / Mar 2017	Danny Jump	Draft TechNote	
1.0	Nov 2018	Danny Jump	First Published Version	

## Copyright

© Copyright 2018 Hewlett Packard Enterprise Development LP.

## **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett- Packard Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett-Packard Company Attn: General Counsel 3000 Hanover Street Palo Alto, CA 94304 USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at <u>HPE-Aruba-gplquery@hpe.com</u>.

## Contents

Introduction	5
Introduction Software Requirements	6
Access to the Extension store	
Installation and Deployment Guide	7
Pictorial view of the Integration	8
New Extension support in ClearPass 6.7	8
Extensions and IP address configuration support	
Extensions and web proxy support	8
MobileIron Extension installation using GUI available in 6.7+	10
Configuring the MobileIron Extension	
GUI configuration for the Extension	13
MobileIron Configuration – Common Platform Services [CPS]	14
Account Creation	14
Enabling CPS framework	16
Manually triggering an event	
ClearPass Policy Manager Configuration	22
Appendix A – Additional Diagnostics & Support	24
The Extensions Service	24
Extension logs and debugging	24
Accessing Extension logs within ClearPass 'Collect Logs'	
Appendix B – MI Cloud Ingestion Performance Observations	27



www.arubanetworks.com 3333 Scott Blvd Santa Clara, CA 95054 Phone: 1-800-WIFI-LAN (+800-943-4526) Fax 408.227.4550

© 2017 Hewlett Packard Enterprise Development LP. All Rights Reserved.

# **Figures**

Figure 1: ClearPass MobileIron Extension feature matrix	5
Figure 2: Entering HP Passport credentials	7
Figure 3: Pictorial view of ClearPass Policy Manager integration with MobileIron Common Platform Se	ervice8
Figure 4: Extension Framework GUI	
Figure 5: Defining the base IP SUBNET and LOCALHOST for the Extensions Framework	9
Figure 6: Extensions Framework GUI	10
Figure 7: GUI Extension Installation	
Figure 8: GUI Extension Search	
Figure 9: GUI Extension Configuration at Install time	11
Figure 10: GUI Reviewing and Setting the Extension configuration	12
Figure 11: Adding a MobileIron account	
Figure 12: Checking the user has the correct roles assigned	
Figure 13: Adding a role to a user	
Figure 14: Adding the "Common Platform Services" role to the user	
Figure 15: Enable CPS Notifications framework [enableMqtt]	16
Figure 16: Add a new user for CPS Events [mqttUserName & mqttPassword]	
Figure 17: Assign a role to this new user - part1	
Figure 18: Assign the CPS role to this new user - part2	17
Figure 19: Assign the CPS role to this new user - part3	
Figure 20: Creating a Custom Compliance Policy – part1	
Figure 21: Creating a Custom Compliance Policy – part2	
Figure 22: Creating a Custom Compliance Policy – part3	
Figure 23: Creating a Custom Compliance Policy – part4	
Figure 24: Change an endpoint attribute to trigger an event notification – part1	
Figure 25: Change an endpoint attribute to trigger an event notification – part2	
Figure 26: Simple Enforcement Policies based upon endpoint attributes	
Figure 27: Device status set to RETIRED	
Figure 28: Checking on the Extensions service and how to start/stop the service	
Figure 29: Using the GUI to change the DEBUG level	
Figure 30: : Extension logs location in 'Collect Logs' diagnostic GZ file	26

## Introduction

This TechNote covers the setup, configuration, and monitoring of the ClearPass Extension for MobileIron Cloud and MobileIron Common Platform Services (CPS) and Event Notification Extension. This Extension provides two key features.

**The first** is adding support for MobileIron Cloud. MobileIron Cloud has not been previously supported, this Extension adds support for Cloud version R56 and above.

**The second** feature supported in this Extension, is the Common Platform Services Event Notifications. This provides for a near-real-time notification feed as discussed below, to allow ClearPass to maintain an up-to-date view of the managed devices, without the need to constantly poll. In this release we are supporting ClearPass in MobileIron Cloud starting in R56.

Note that ClearPass has supported MobileIron Core for several years, our support for this does not change. At this time this Extension could complement an existing MobileIron Core deployment but we have not verified interoperability with Core, we will complete this soon.

API Product	MI API's supported	Native ClearPass Polling	Native ClearPass Polling + Extension CPS API [Hybrid deployment]	MobileIron Extension CPS API
Pre-Core 9.5	V1	Yes	Yes*	No
Core 9.5 +	V1 + CPS	Yes	Yes	Yes
Cloud R56 +	CPS	No	No	Yes

Figure 1: ClearPas	s MobileIron Extensior	n feature matrix
--------------------	------------------------	------------------

\* For the Pre-Core 9.5 in Hybrid mode, only the Native ClearPass Polling API V1 are supported, the CPS API's are not available in the pre 9.5 Core so adding the Extension to add real-time updates is not supported.

As discussed, the Extension has the ability to ingest endpoint attributes (Core 9.5+ & Cloud R56+) and to receive a near real-time *[in testing about 5 seconds]* feed of endpoint changes within the customer's MobileIron tenant. ClearPass subscribes and receives real time event notifications for 5 distinct use-cases.

- 1. A New Device Added
- 2. A Device Retired/Deleted
- 3. A Device changes state to "out of Compliance"
- 4. A Device changes state to "in Compliance"
- 5. A Device is Wiped

When one of the above events occurs, the MobileIron EMM places the event notification into a message queue. All active ClearPass nodes that subscribe to that notification event queue, then can receive that message.

If no ClearPass nodes are active, then the message queue server retains that event notification for **maximum duration of up to 3 hours**, later when an active ClearPass node connects, it's able to consume this stored event message. Messages that exceed the maximum duration are purged.

In comparison, the legacy approach [still available] is to poll the tenant every hour and ingest all of the endpoint data, then update the delta changes into the EndpointDB. The obvious issues with the legacy approach is that if a device goes out of compliance, ClearPass won't know of the state change until the next poll. Similarly if a new device is added, typically the access-policy is that when a SmartDevice accesses the network, ClearPass checks to ensure it's a known managed device. In the legacy approach access would be denied until the next poll had completed. Utilizing the full polling capabilities in conjunction with the event notifications allows a near real-time local view of all of the managed Endpoints.

By comparison, the legacy approach [still available] requires polling the tenant every hour, ingesting all of the endpoint data, computing the delta changes for each endpoint and updating the EndpointDB. One issue with the legacy approach is that if a device goes "out of Compliance", ClearPass can't determine the state change until the next poll cycle. Another problem is that when a new device is added to the enterprise, the SmartDevice access-policy requires ClearPass to ensure that it's a known managed device, which can't be determined until the next poll cycle completes, thus the new device access is denied until then. By utilizing both polling with event notification, ClearPass is afforded a new real-time local view of all managed Endpoints. (latency is kept to a minimum).

Below, we cover installation and configuration of the Extension, configuration within MobileIron, and finally ClearPass configuration. Additionally, we document a solution which allows a device to be 'tagged' as in or out of compliance. This creates an event notification and allows for testing of the end-to-end workflow.

Installation of the MobileIron ClearPass Extension is performed either via the REST API interface, or the simplified GUI introduced in ClearPass Policy Manager v6.7, this is the preferred method. Access to the APIs is through the following URL **https://<ClearPass\_IP>/api-docs**.

# **Software Requirements**

The minimum software version required for CPPM is 6.7.2. At the time of writing, version 6.7.6 is available and the recommended release. CPPM runs on hardware appliances with pre-installed software or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 5.5, 6.0, 6.5 or higher
- Microsoft Hyper-V Server 2012 R2 or 2016 R2
- Hyper-V on Microsoft Windows Server 2012 R2 or 2016 R2
- KVM on CentOS 6.6, 6.7, or 6.8.

The versions of MobileIron supported with this Extension are

- MobileIron Cloud R56 or later
- MobileIron Core 9.5.0 or later

This is the first version which enables the installation, configuration and operation of the Extensions via the GUI. To use the simplified GUI Extension installation, details start on Page 11, else to use the legacy REST API approach, details start on Page 14.

## Access to the Extension store

Access to the Extension Store to download Extensions is simplified in ClearPass 6.7. The ability to download Extensions from the store and to validate support entitlement for access to the Software Updates Portal (e.g. Posture & Profile Data Updates, Software Updates, & Skins) now uses the HPE Passport account credentials that are associated with the customers' ClearPass licenses. This is configured where previously the subscription-id was defined, under **Administration -> Agents and Software Updates -> Software Updates** as shown below. Ensure you enter your HPE Passport credentials to enable Extension download capabilities.

aruba		Clea	arPass Policy Ma	anager		Support   <u>Help</u>   Logout admin (Super Administrator)
Dashboard	<ul> <li>Administration » Agents and Softwa</li> </ul>	re Updates » Softwa	are Updates			
Monitoring	<ul> <li>Software Updates</li> </ul>					Cluster Upgrade
Configuration	0					Cluster Update Check Status Now
🔐 Administration						
- JP ClearPass Portal	HPE Passport Credentials Username:		BTes col.			
🗈 🗣 Users and Privileges	Password:					
🖃 🕼 Server Manager	Passworu.					
- Jerver Configuration						Save
— Jog Configuration						
- Jocal Shared Folders	Desture & Drefile Date Hadate					
— 🧀 Licensing	Posture & Profile Data Updates		Bala Garatad	1 1 11 - d-1 -	1 1 - 1 - 1 - 1	
💽 🕼 External Servers	Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
🖃 🚔 Certificates	Posture Signature Updates*	-	-	-	-	Needs Update
— <i>P</i> Certificate Store	Windows Hotfixes Updates*	1.2173	2017/10/23 04:21:15	File	2017/11/21 11:12:44	Updated 4 days ago
- 🥜 Trust List	Endpoint Profile Fingerprints*	2.545	2017/10/23 22:45:29	File	2017/11/21 11:12:45	Updated 4 days ago
— A Revocation Lists						Import Updates
Dictionaries						
Agents and Software Updates	* Automatic download and install is disabled					
— A OnGuard Settings — Software Updates	To manually import Posture & Profile Data Upo	ates, refer to Help for this	s page.			
Support	Firmware & Patch Updates					

#### Figure 2: Entering HP Passport credentials

# **Installation and Deployment Guide**

The generic ClearPass installation and deployment guide is located here:

https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba\_DeployGd\_HTML/Default.htm#About%20Cl earPass/Intro\_ClearPass.htm

# **Pictorial view of the Integration**

The diagram below shows a pictorial overview of the components and how they interact with each other.

Figure 3: Pictorial view of ClearPass Policy Manager integration with MobileIron Common Platform Service



# New Extension support in ClearPass 6.7

With the release of 6.7, several new features enhance the functionality of the Extension framework. Previously, all Extension installation and operation tasks required use of the API Explorer to interoperate with the Extension and the underlying framework. This functionality has been exposed with a new GUI. The GUI is accessed from within the Guest UI and is shown below, **Administration -> Extensions**.

## **Extensions and IP address configuration support**

The 6.7 release provides the ability to define the extension framework base IP network and to define the static IP address of the individual extensions. Use the latter when deploying extensions into a cluster and for the ability to set a fixed IP address for the same extension across the cluster regardless of which ClearPass node(s) it was installed on.

## Extensions and web proxy support

Prior to 6.7 support for web proxy was limited to the installation of the Extensions. Starting in ClearPass 6.7, Extensions now support communications with 3<sup>rd</sup> parties via a web proxy. If a web proxy is defined in ClearPass Policy Manager, then an Extension use that configuration.



Note that the Policy Manger web proxy configuration is ONLY read at by the Extension at installation time. If the web proxy configuration is changed in Policy Manager, then the Extension must be re-installed, so the new settings are re-read and bonded to the Extension.

#### Figure 4: Extension Framework GUI

aruba	ClearPass Guest		
🗣 Guest 🛛 0	Home » Administration » Extensions		
📮 Onboard 🛛 🛛 💿	Manage Extensions		
Configuration O	The extensions currently installed on this system are listed below.		
— 🧼 Start Here	Filter:		
🖅 🔩 AirGroup Services	△ Name Version State Hostname IP Address		
API Services     Data Retention	1 There are no extensions installed. To find new extensions, use the 'Install extension' action to search the extension store.		
Extensions France Import Configuration	V Install extension		
🖅 🦣 Operator Logins	C Refresh No matching items		
- Q Plugin Manager			
	🚱 Back to administration		

Configuring the base Extension IP subnet, is defined within Policy Manager as shown below under **Administration -> Server Manager -> Server Configuration [chose your node] Service Parameters [ClearPass system service].** The default address 172.17.0.1/16, is the non-routed address of the ClearPass node itself. The IP addresses range for the extensions depends upon the network prefix used.



Note that the subnet defined here for the Extension framework must fall within the following subnet range 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 as defined by RFC1918.



aruba	ClearPass Policy I	Vlanager		apport   Help   Logo admin (Super Administrato
- Dashboard	• Administration » Server Manager » Server Configuration -			
Monitoring	<ul> <li>Server Configuration -</li> </ul>	LOPE COLUMN ADD		
Configuration				
Administration	System Services Control Service Parameters System Monitoring	Network FIPS		
P ClearPass Portal	Select Service: ClearPass system services \$			
Sers and Privileges	Parameter Name	Parameter Value	Default Value	Allowed Values
Server Manager	PHP System Configuration			
- Jog Configuration	Memory Limit	256 Megabytes	256	256-1024
- P Local Shared Folders	Form POST Size	15 Megabytes	15	1-256
Jucensing	File Upload Size	15 Megabytes	15	1-256
External Servers	Input Time	60 seconds	60	0-600
Certificates	Socket Timeout	60 seconds	60	5-600
- Dertificate Store	Enable zlib output compression	FALSE \$	FALSE	
- Just List - Just Revocation Lists	Include PHP header in web server response	TRUE \$	TRUE	
Dictionaries	TCP Keep Alive Configuration			
Agents and Software Updates	Keep Alive Time	7200 seconds	7200	10-86400
OnGuard Settings	Keep Alive Interval	75 seconds	75	1-3600
🥔 Software Updates	Keep Alive Probes	9	9	1-100
Support 🗧	Database Configurations			
	Maximum Connections	400	400	300-2000
	Extensions			
	Extensions Network Address	172.17.0.1/16	172.17.0.1/16	
	HTTP Proxy			
	Proxy Server			
	Port	3128	3128	1-65535
	Username			



Note when changing the Extension base IP address requires the Extension service to be restarted.

Changing the "Extensions Network Address" range becomes necessary when either the MGMT or DATA interface uses an address in the Extension default range of 172.17.x.x/12. Set the new network address range as needed then restart the Extension service for this change to take effect.

# MobileIron Extension installation using GUI available in 6.7+

Starting in ClearPass 6.7, a Graphical User Interface (GUI) was introduced to make the process of interacting with the Extension framework easier. To access the Extension GUI, from the **Guest System**, under **Administration** find the **Extension** User Interface as shown below.



aruba	ClearPass Guest			
😜 Guest 🛛 🛛 0	Home » Administration » Extensions			
📳 Onboard 🔹 💿	Manage Extensions			
Configuration	The extensions currently installed on this system are listed below.			
— 🛶 Start Here	Filter:			
🗄 💱 AirGroup Services	△ Name Version State Hostname IP Address			
API Services	<ul> <li>There are no extensions installed. To find new extensions, use the 'Install extension' action to search the extension store.</li> <li>Install extension</li> </ul>			
Operator Logins     Q Plugin Manager	C Refresh No matching items 20 rows per page \$			
🗄 🥳 Support	👰 Back to administration			
	🚱 Back to main			

From here, click on 'Install Extension', and the search box below appears.

Figure 7: GUI Extension Installation

Home » Adn	Home » Administration » Extensions				
Install E	Extension				
Use this form	Use this form to install a new extension.				
	Install Extension				
* Search:	Keywords or extension ID				
	Search				
* required fiel	f required field				

Enter either the Store-ID, or enter the name or partial name of the Extension, and click on 'Search'. See the example below:

#### Figure 8: GUI Extension Search

	Home » Administration » Extensions Install Extension				
Use this for	Use this form to install a new extension.				
	Install Extensior	1			
* Search: Mobile					
	Name	Version	State		
Results:	MobileIron MobileIron MQTT and MDM integration.	1.0.0	Stopped		
	Search				
* required fie	* required field				

Click on the Extension and then the "Install" option, and if necessary, set the IP address. Note it can be set later if required, e.g. you want to set a permanent static address for the extension.

Figure 9: GUI Extension Configuration at Install time

Home » Adm	Home » Administration » Extensions				
Install E	Install Extension				
Use this form	n to install a new extension.				
	Install Extension				
Extension:	MobileIron MobileIron MQTT and MDM integration.				
Extensio	Extension Settings				
Start:	□ Start the extension after installation				
IP Address:	17.17.0.55 Enter IPv4 address to allocate to this extension, from the network 172.17.0.1/16. Leave blank to automatically assign an IP address.				
	Install				

After the Extension has been installed, if the option to automatically start was not selected, review the Extension configuration and adjust as needed. Notice the options to Start, Delete, Reinstall or Show Logs and the option to review and set the Extension configuration.



Figure 10: GUI Reviewing and Setting the Extension configuration

A copy of the default MobileIron Extension is shown above, this will need to be modified for your deployment and the extension started/re-started as appropriate.

# **Configuring the MobileIron Extension**

## **GUI configuration for the Extension**

Regardless of whether the Extension was deployed with the GUI or with the legacy REST API's, a set of mandatory parameters must be collected to allow the default configuration {shown below} to be updated.

```
{
    "logLevel": "INFO",
    "verifySSLCerts": true,
    "cppmUser": "admin.user",
    "cppmPassword": "admin.password",
    "mobileIronUrl": "https://MI_URL",
    "mobileIronDserName": "user.name",
    "mobileIronPassword": "user.password",
    "enableMqtt": true,
    "mqttUrl": "ssl://MI_MQTT_URL:8883",
    "mqttUserName": "user.name",
    "mqttPassword": "user.password",
    "enableFullUpdate": false,
    "fullUpdateIntervalMinutes": 10080
}
```

The default configuration needs to be changed to match your environment. Each configuration option is described below.

- **logLevel:** Defines the logging level of the Extension. ("DEBUG", "INFO", "WARN", "ERROR")
- **verifySSLCerts:** Defines if the Extension verifies the presented certificate by MobileIron.
- **cppmUser:** A CPPM Admin account used to allow internal communications.
- **cppmPassword:** The password associated with the above Admin account.
- **mobileIronUrl:** The URL of the MobileIron tenant hostname/IP address.
- **mobileIronUserName:** The MobileIron username.
- **mobileIronPassword:** The MobileIron username's password.
- enableMqtt: Enables/Disables the Event Notification real-time update framework in the Extension.
- **mqttUrl:** The MQTT URL that the extension connects to receives event notifications.
- mqttUserName: The MQTT username.
- mqttPassword: The MQTT username's password.
- **enableFullUpdate:** If set to true, the Extension will ingest all of the endpoint information and populate the ClearPass EndpointDB. Default = false.
- **fullUpdateIntervalMinutes:** The frequency the full ingest service runs, in minutes. Default = 7 days.

Unless instructed by Aruba TAC, leave the logLevel at the default value.

NOTE

# **MobileIron Configuration – Common Platform Services [CPS]**

Below we cover the configuration required in the MobileIron environment. To properly configure the CPPM extension, first collect a number of items from the MobileIron tenant. Within the configuration, three username/password combinations required.

## **Account Creation**

**CPPM-Credentials.** The first pair [**cppmUser/cppmPassword**] is used by the Extension to call ClearPass API's that allow the creation/deletion/updating of endpoint data. You can use an existing CPPM Local Admin account or better, create a new dedicated read-only Admin account for this function.

**MobileIron-Tenant-Credentials.** The second pair **[mobileIronUserName/mobileIronPassword]** is used by the Extension to communicate with the MobileIron instance when calling MobileIron API's to retrieve all of the endpoint data which is then populated into the ClearPass EndpointDB. For the **MobileIron-Tenant-Credentials**, it is recommended that an account be created in MobileIron dedicated for this function. Although these credentials can be an Administrator account best practice recommends that a new account with the roles shone below in Figure12 be used. To create the account. **Users -> +Add** 

N > CLOUD	Dashboard	Users	Devices	Apps	Content	Configurations	Policies	Admin		L.	
	Users	User Groups	User Set	tings							
23 users	+ Add	Actions ~									*
Find users	DISPL	LAY NAME			Ŧ	USERNAME			EMAIL	INVITE STATUS	
	Dann	y Jump				djump@hpe.com			djump@hpe.com	Pending	:
Unmanaged Devices V	Josh	Santomieri				josh.santomieri@hpe	.com		josh.santomieri@hpe.com	Not Invited	÷
□ Yes (0)	Сррп	ı арі				cppm-api@cppmtes	t.org		cppm-api@cppmtest.org	Not Invited	:

Figure 11: Adding a MobileIron account

Then select the user and ensure that the user has 'System Read Only' & 'User Read Only' roles assigned.

Figure 12: Checking the user has the correct roles assigned.



**MobileIron-MQTT-Credentials.** The third pair **[mqttUserName/mqttPassword]** is used by the Extension to communicate with the MobileIron Event Notification Services. This service sends the real-time-notifications. It's possible to use the same account as above or a separate account. If using the same account, ensure that the **Common Platform Services** role has been added to the user account. In the Roles tab, click on **Actions -> Assign Roles** 



cppm api   Username: cpp	m-api@cppmtest.or	rg			
Actions ~					
Assign to Group Remove from Group Send Message Invite User to Register Assign Roles Delete Extend Password Expiration	Available Apps	Roles	Attributes		
				cppm api	
First Name				cppm	

Next add the CPS role to that user. Note, to add the role **Common Platform Services** scroll down as highlighted below to locate the role. Select the role, and confirm.

Figure 14: Adding the "Common Platform Services" role to the user

All (17)	Selected (0)
User Read Only   Global	
LDAP User Registration And Invite   Global	
Device Management   Space Bound	
Device Read Only   Space Bound	
App & Content Management   Space Bound	
App & Content Read Only   Space Bound	
Device Actions   Space Bound	$\frown$
Cisco ISE Operations   Global	(~)
Scheduled Task Management   Global	
Common Platform Services (CPS)   Global	

## **Enabling CPS framework**

After creating the accounts, to use the *near-real-time* event notification service, additional configuration steps are required. Navigate to the *Admin* tab on MI Cloud portal, click on *CPS Notifications* sub-tab and select enable the service. (see below)

Figure 15: Enable CPS Notifications framework [enableMqtt]

N > CLOUD	Dashboard	Users Devices	Apps	Content	Configurations	Policies	Admin	L <sup>0</sup> ()
Admin	Common	Platform Ser	vices N	otificatio	ons			
SYSTEM Attributes		orm Services enable te					stomers. With Common Platfor	m Services, partners no longer have to poll for sed notification system
Common Platform Services Notifications		oint management dates	a time by on					
Notification Emails Spaces System Use Notification INFRASTRUCTURE App Lists App Reputation	S. One time inte		K Constant of the second secon	Services	Subscribes to Events	ch integration Partners		
Certificate Authority Connector Help@Work Identity	Settings	rm Services Notificati	ons					

If the CPS role has not been added to an existing user, then create a new CPS user: Create a user by navigating to **Users** tab on the admin portal.

Figure 16: Add a new user for CPS Events [mqttUserName & mqttPassword]

Northeast CLOUD	Dashboard Use					Ļ	
	Users User Gr	Add Single Use	er	X			
2 users	+ Add Actions						*•
Find users	DISPLAY NAME	Email Address	testusercps@mi.com			INVITE STATUS	
	nobody-1148002	Username	testusercps@mi.com		2000@auto0001.mobileiron.com	Not Invited	:
Unmanaged Devices V	miadmin@auto0	First Name	Test		mobileiron.com	Not Invited	:
Yes (0)		Last Name	User				
Account Source V LDAP (0) AAD (0)		Display Name	Test User (Edit)				
Roster (0) Salesforce (0) Local (2)		Password					
Invite Status			If password is left blank the user will be sent a one-time use PIN and then be prompted to set a password.				
Completed (0)		Confirm Password					
Not Invited (2) Pending (0)		Locale	English \$				
Google Status	Showing 1 to 2 of 2	Assign (optional):	+ Add New User Group	Ļ		Export to I	CSV [ai],

Select the user created and assign "Common Platform Services" role to the user.

	Dashboar	d Users Devices	Apps	Content	Configurations	Policies	Adm	in	<u> P</u>	
	Users	User Groups User S	ettings Use	er Branding						
3 users	+ Add	Actions ~								*•
Find users	DISP		-	USERNA	ME			EMAIL	INVITE STATUS	
	🛛 Test	Remove from Group Send Message		testuserc	ps@mi.com			testusercps@mi.com	Pending	
Unmanaged Devices 🗸	nobe		obileiron.com	nobody-1	1480022-42000@aut	o0001.mobileiror	n.com	nobody-11480022-42000@auto0001.mobileiron.com	Not Invited	÷
Yes (0)	🗆 miac	Assign Custom Attributes Remove Custom Attributes		miadmin@	@auto0001.mobileiror	i.com		miadmin@auto0001.mobileiron.com	Not Invited	÷
Account Source V		Delete								
LDAP (0) AAD (0) Roster (0) Salesforce (0) Local (3)		Append Roles Extend Password Expiration								
Invite Status										

Figure 17: Assign a role to this new user - part1

*Figure 18:* Assign the CPS role to this new user - part2

N > CLOUD	Dashboard Users Devices Apps Content Configurations Policies Admin	
	Users User Groups User Settings User Branding	
Append Roles Cancel	Append Roles	
1 Select Roles	Select Roles	
2 Summary	Search User Roles Q	
	All (17) Selected (1)	
	User Read Only   Global	
	LDAP User Registration And Invite   Global	
	Device Management   Space Bound	
	Device Read Only   Space Bound	
	App & Content Management   Space Bound	
	App & Content Read Only   Space Bound	
	Device Actions   Space Bound	
	Cisco ISE Operations   Global	
	Scheduled Task Management   Global	
	Common Platform Services (CPS)   Global	
		Next →

Figure 19: Assign the CPS role to this new user - part3

🔨 > CLOUD	Dashboard Users Devices Apps Content Configurations Policies Admin				
	Users User Groups User Settings User Branding				
Append Roles Cancel	Append Roles				
Select Roles	Summary				
2 Summary	Global Roles (1)				
	ROLE NAME				
Append Roles Cancel Append Roles Select Roles Summary Global Roles (1) RoLE NAME Common Platform Services (CPS) Space Bound Roles RoLE NAME There is no information to display.	Common Platform Services (CPS)				
	Cancel Append Roles Summary Global Roles (1) RoLE NAME Common Platform Services (CPS) Space Bound Roles				
	Users       User Groups       User Stitlings       User Branding         pend Roles       Cancel       Append Roles         Select Roles       Summary       Global Roles (1)         ROLE NAME       Common Platform Services (CPS)         Space Bound Roles       ROLE NAME         There is no information to display.				
	Dashboard       Users       Davices       Apps       Content       Configurations       Policies       Admin       C         Users       User Groups       User Settings       User Branding       User Settings       User Branding         Cancel       Append Roles       Summary       Global Roles (1)       Image: Common Platform Services (CPS)       Image: Common Platform Services (CPS)         Space Bound Roles       SPACES       Image: Common Platform Services (CPS)       Image: Common Platform Services (CPS)         There is no information to display.       Image: Common Platform Services (CPS)       Image: Common Platform Services (CPS)				
Users User Groups User Settings User Branding     Append Roles     Select Roles   Summary Global Roles (1)   ROLE NAME   Common Platform Services (CPS)   Space Bound Roles   ROLE NAME   Proces There is no information to display.					
		Done			

## Manually triggering an event

As an example of how you could use custom attributes to simulate a compliance policy to force devices in and out of non-compliant state: This section allows for the creation of an event to test the end-to-end workflow of the system.

A good use case would be to toggle a value of a custom attribute (say, nacCompliant) for devices which have moved out of compliance from **true** to **false** and then, use the attribute to take actions on the device. There are multiple ways to force compliance actions on the device to render it non-compliant. Please refer the below steps:

#1: Create a compliance action policy: Navigate to Policies on the admin portal menu bar and click on Add

N > CLOUD	Dashboard	Users	Devices	Apps	Content	Configurations	Policies	Admir			<u> </u>	
	+ Add											*
Policies	NAME			TYPE			DISTRIB	UTION		COMPLIANCE ACTION	ACTIONS	
Vhat are Policies?	Compromised E	Devices		_ c	ompromised De	evices	0		0	Monitor only	$   \bigcirc $	:
blicies define the security iteria for deciding when evices are not compliant and e action(s) to be taken for olating devices. Violating avices will be marked as non- mpliant and the compliance	Data Protection/Encryption Disabled			≡à ¤	ata Protection/E	Encryption Disabled	0	0 0 Monitor, Quarantine		Monitor, Quarantine	$\bigcirc$	:
	International Roaming Devices			😽 In	ternational Roa	ming	0	0 0 Monitor only		Monitor only	$\bigcirc$	:
	MDM / Device Administration Disabled			NEW M	MDM / Device Administration Disabled		0		0	Monitor only	$\bigcirc$	:
ompliant and the compliance ction(s) associated with the olicy will be taken against the	Out of Contact			@ 0	ut of Contact		0		0	Monitor only	$\bigcirc$	:
levice.												
preating Policies lew policies can be chosen om a list of policy types with re-defined security criteria or "Custom Policy" can be reated where the security riteria can be defined. In both asses, compliance actions are et for violating devices.												

Figure 20: Creating a Custom Compliance Policy – part1

**#2**: Add policy rule/definition to determine the criteria for a device going non-compliant: Click on "**Custom Policy**" option to create a custom compliance action policy.

Figure 21: Creating a Custom Compliance Policy – part2

CLOUD Dashboard (	Jsers Devices Apps Content Configurations Policies Admin	4
Choose Policy Type Cancel		
Choose the actions to take if a compromised (ex: jallbroken) device is detected.	Data Protection/Encryption Disabled Choose the actions to take if a device does not have a passcode or encryption enabled.     International Roaming Choose the actions to take if a device is outside its home country	
MDM / Device Administration Disabled Choose the actions to take if the MDM relationship is severed	Out of Contact Choose the actions to take if a device has not checked in for a specified number of hours or days Custom Policy Create a custom policy. Set conditions and specify related actions.	
Allowed Apps Create a list of allowed/disallowed and/or required apps. Choose the actions to take if a device's installed apps do not meet these requirements.		?
	Copyright © 2013-2017 Mobileiron, Inc. All rights reserved. About Mobileiron   Terms of I	Use   Privacy Policy

Choose a custom policy rule: Enter a **policy name** and create a criteria query to specify policy rule, E.g. If the device ownership is 'User Owned' or the device OS is type 'Android' mark it as non-compliant and click **Next**.

Figure 22: Creating a Custom Compliance Policy – part3

N CLOUD	Dashboard Users Devices Apps Content Configurations Policies Admin	Ŀ	
Add Policy Cancel	Create a custom policy. Set conditions and specify related actions.		
2 Distribute	Policies and Compliance Setup Name Device_Not_Compliant_Policy + Add Description		
	Define Conditions     Learn more about Custom Policies ?       Set policy conditions that trigger actions when conditions are met.     Reset All		
	ANY ALL of the following rules are true:		
	Ownership is equal to User Owned Choose Actions		
	Of Monitor Note: Sentry version 9.0.0 or later is required to utilize the tiered compliance actions.		?)
	Image: Do Nothing     Image: Do Nothing       Image: Do Nothing		×t →

#### #3: Distribute the policy to all devices and click Done



#4: Perform state changes on the device to match the criteria, this would mark the device non-compliant, in which case, **device\_not\_compliant** events would be triggered e.g. Changing device ownership to 'User Owned' and initiate force check-in and device sync.

	Dashboard Users	Devices Apps Co	ntent Configu	rations Policies	s Admin			٤.	3 (
	Devices Device Group	DS Unmanaged Connect	ons App Inve	ntory					
3 devices	Actions ~								*
Find devices	Assign to user	ADDRESS	PHONE #	os	DEVICE TYPE	STATUS	LAST CHECK-IN	VIOLATION COUNT	
	Force Check-in	1@aries.mobileiron.net		Android 5.0.1	GT-19500	Active	1 day 3 hours ago	1	
Carrier V	Unlock	1@aries.mobileiron.net		iOS 10.3.1	iPad6,3	Active	10 days 8 hours ago	1	
	AppConnect Unlock Send Message	arcps@aries.mobileiron.net		iOS 9.3.2	iPad6,3	Active	31 days 20 hours ago	1	
Supervised V	Retire								
Yes (0)	Wipe Set Ownership								
Secure Apps Status 🗸	Enter Kiosk Mode								
Transitional (0)	Exit Kiosk Mode								
Enabled (0) Disabled (1)	Add To Group								
N/A (0)	Restart/Shutdown device								
Unsupported (0)	Assign Custom Attributes								
Android Work 🗸 🗸	Remove Custom Attributes								
No (3)									
Yes (0)									
Device Type 🗸 🗸									
iPad6,3 (2) GT-19500 (1)									
Iser Group ? 🗸 🗸	Showing 1 to 3 of 3								ort to CS\
All Users (3)	Showing 1 to 3 of 3							Expo	IT to CSV

Figure 24: Change an endpoint attribute to trigger an event notification - part1

← Back

!

	Dashboard Users	Devices Apps Content Config	urations Policies Admin	4 Q
	Devices Device Gr	Set Device Ownership	×	
3 devices	Actions ~	The ownership of this device is currently "use	er owned". Choose a new ownership attribute below:	<b>茶</b> ~
Find devices				LAST CHECK-IN + VIOLATION COUNT
	Z tes	Company Owned	User Owned	1 day 3 hours ago 1
Carrier V	🖸 tes			10 days 9 hours ago 1
	Test CPS test			31 days 20 hours ago 1
Supervised ~ No (3) Yes (0)		These devices are owned by your company and used by employees for work.	These devices are owned by your employees and used for work.	
Secure Apps Status 🗸				
Transitional (0) Enabled (0) Disabled (1)			Cancel Set Ownership	
N/A (0) Unsupported (0)				
Android Work 🗸 🗸 Managed D				
□ No (3) □ Yes (0)				
Device Type ~ iPad6,3 (2) GT-19500 (1)				
User Group (?) V	Showing 1 to 3 of 3			Export to CSV
			Copyright © 2013-2017 Mobileiron, In	nc. All rights reserved. About MobileIron   Terms of Use   Privacy Policy

*Figure 25:* Change an endpoint attribute to trigger an event notification – part2

Certain policy rules can affect a large set of devices at one time; these aren't generally recommended.

- OS is iOS
- Last check-in is 10 hrs ago
- Ownership Type is 'User Owned'

**#5**: To bring the device back to compliance, either perform reverse device state changes or delete the compliance action policy and initiate force-sync on devices.

# **ClearPass Policy Manager Configuration**

The final part is the configuration on ClearPass Policy Manager. Depending on how you use the integration will ultimately define how you configure the interaction between MobileIron Cloud/Core and the ClearPass Extension and Policy Manager.

If you plan on using the Extension to interface with MobileIron Cloud then configure the Extension and its associated polling. Following this, configuring ClearPass Policy Manager configuration is no different in how you'd authenticate and authorize any other device, it's really about how you use the endpoint database attributes in your authorization policy checks for role-mapping or your enforcement policy.

If you plan on using the Extension to complement the existing MobileIron polling, then overall this is a hybrid deployment. Using the built-in polling to ingest the endpoint details once per day in addition to using the Extension to 'trickle-feed' changes into the endpoint-database as they happen. This hybrid deployment can remove the need for the lengthy and regular polling, carefully consider your polling strategy and how often you poll.

Regardless of which deployment you configure, as noted above the power of the integration is how you use the endpoint data base attributes. As an example here are a few simple examples.

Inforcement P	cement » Policies » Edit - MobileIron Enforcement Policy Policies - MobileIron Enforcement Policy	
Summary Enforcement:	orcement Rules	
Name:	MobileIron Enforcement Policy	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	[Allow Access Profile]	
Rules:		
Rules Evaluation Alg	gorithm: First applicable	
Conditions		Actions
1. (Endpo	int:Status EQUALS RETIRED)	[Deny Access Profile]
2. (Endpo	int:Compliant EQUALS true)	Quarantine Role, Create SNOW incident tickets, Send Quarantined Device Notification (SMS)
	vint:OS EQUALS IOS) t:OS Version NOT_CONTAINS 11)	Old-OS-ArubaRole, BlackBerry endpoint out_of_Compliance, Create SNOW incident tickets
4. (Endpo	int:Compromised EQUALS true)	Quarantine Role, Send Quarantined Device Notification (SMS)
5. (Endpo	int:Quarantined EQUALS true)	Email Security Response Team, Create SNOW incident tickets, [Deny Access Profile]

#### Figure 26: Simple Enforcement Policies based upon endpoint attributes

To add, a little more clarity, if a device is retired from within MobileIron then the endpoint status flag is set accordingly. Within your enforcement policy you need to add a rule {#1} as shown above, where, when the **status** of the endpoint is set as **RETIRED**, the enforcement action would be to Deny Access. This can be adjusted to fit your own needs, as an example if you detected a device trying to access the network which has been deleted/retired from the system, you may want to have a work flow that drops the device into a captive portal role which directs the user to contact the helpdesk for assistance.

Figure 27: Device status set to RETIRED

	Attribute		Value
1.	Compliant	=	true
2.	Compromised	=	false
3.	Last Check In	=	2018-02-14 23:10:13
4.	Manufacturer	=	Apple Inc.
5.	OS	=	IOS
6.	OS Version	=	9.3
7.	Quarantined	=	false
8.	Registration Date	=	2018-02-09 15:54:47
9.	Serial Number	=	ee5c69f0bf31
10.	Source	=	MobileIron
11.	Status	=	RETIRED
12.	UDID	=	6xLyq8QzRgiKuFADeUTKqWgrsrwNrzVBpyL7jlQP
13.	User ID	=	oscarjimenez@auto0001.mobileiron.com

# **Appendix A – Additional Diagnostics & Support**

## **The Extensions Service**

The ClearPass Extension is supported by a new system service that was initially added in 6.6. This service should be running. Note that restarting this service will affect **all** deployed and running Extensions. To check on the state and to restart the service, go to **Administration > Server Manager > Server Configuration** [select a cppm node] > Service Control. From here start/stop the Extension service. By default, this service is automatically started.

Figure 28: Checking on the Extensions service and how to start/stop the service

	on » Server Manager » Server Configuration - cppm6dot6-160 Configuration - cppm6dot6-160 (10.2.100.160)		
System	Services Control Service Parameters System Monitoring Network FIPS		
	Service Name	Status	Action
1.	AirGroup notification service	Running	Stop
2.	Async DB write service	Running	Stop
3.	Async network services	Running	Stop
4.	ClearPass IPsec service	Running	Stop
5.	DB change notification server	Running	Stop
6.	DB replication service	Running	Stop
7.	Extensions service	Running	Stop

## **Extension logs and debugging**

If there is a need to access the logs from inside the Extension, turn on log collection from the API Explorer. Referencing the configuration previously used, adjust the "**logLevel**" to "**DEBUG**". In the new 6.7 GUI change the config and restart the Extension as shown below. Logs can then be viewed from the '**Show Logs**'.

Figure 29: Using the GUI to change the DEBUG level

integrati	on MQTT and MDM	
	Extension Configuration	
* Configuration:	<pre>{     "logLevel": "DEBUG"     "verifySSLCerts": false,     "cppmUser": "admin",     "cppmPassword": "***********************************</pre>	
Restart:	Restart extension after updating configuration	
	Save Changes	

Here are a few examples of 'normal' logs

[2017-12-05T10:44:37.651] [INF0] MobileIron - Client reconnecting to ssl://ppp1234.auto.mobileiron.com:8883. [2017-12-05T10:44:37.783] [DEBUG] MobileIron - Got a MQTT packet. [2017-12-05T10:44:37.784] [INF0] MobileIron - Connected to server ssl://ppp1234.auto.mobileiron.com:8883. [2017-12-05T10:44:37.784] [INF0] MobileIron - Querying for MQTT topics... [2017-12-05T10:44:37.814] [INF0] MobileIron - Subscribing to da5d1822-5cda-41c0-9507dda52597a312/device/compliant, da5d1822-5cda-41c0-9507-dda52597a312/device/wiped, da5d1822-5cda-41c0-9507-dda52597a312/device/not\_compliant, da5d1822-5cda-41c0-9507dda52597a312/device/enrolled, da5d1822-5cda-41c0-9507-dda52597a312/device/retired topic(s).

Here are a few logs showing failures.

```
[2017-12-05T10:46:37.897] [DEBUG] MobileIron - Got a MQTT packet.
[2017-12-05T10:47:37.949] [DEBUG] MobileIron - Got a MQTT packet.
[2017-12-05T10:38:00.866] [WARN] MobileIron - MQTT Connection closed.
[2017-12-05T10:38:01.867] [INFO] MobileIron - Client reconnecting to
ssl://ppp1234.auto.mobileiron.com:8883.
[2017-12-05T10:38:01.999] [DEBUG] MobileIron - Got a MQTT packet.
[2017-12-05T10:38:02.000] [ERROR] MobileIron - Connection error!
[2017-12-05T10:38:02.001] [ERROR] MobileIron - { Error: Connection refused: Not author-
ized
```

## Accessing Extension logs within ClearPass 'Collect Logs'

In addition to the logging of messages that be examined in the Extension as shown above, it's possible to configure the Extension to log messages so that they can be collected and examined via the Policy Manager **'Collect Logs'** system function. This is extremely useful for Aruba TAC.

If there is a requirement for Aruba TAC to investigate a system issue, one of the items they regularly ask for is the system logs to aid with their diagnostic investigation. The ClearPass Extension can write its logs such that they are available and can be collected with all other system diagnostics information when the **'Collect Logs'** function is run. Remember that by default, the logLevel is set to INFO but TRACE, DEBUG, INFO, WARN, ERROR, FATAL can also be set. Any of the levels will display the information for the selected state and lower. For example, if INFO is selected, it will show messages for INFO, WARN, ERROR, FATAL.

After the Logs have been collected and exported from the system, expand the GZ file and locate the Extension logs in the following location '**PolicyManagerLogs->Extension'** as shown below.



Figure 30: : Extension logs location in 'Collect Logs' diagnostic GZ file

# **Appendix B – MI Cloud Ingestion Performance Observations**

During our testing of the integration we performed extensive testing, as part of this process we recorded timing related to the performance of ingesting endpoints from a Cloud tenant. In our testing we had circ 5,000 endpoints.

Your performance for ingesting your tenant data will be dependent on a number of factors which are beyond the scope of this document, but we wanted to provide our experience and observations.

During a new ingest, i.e. a first time sync we recorded over a number of iterations a rate of approximately 1,000 endpoints per 10 minutes. When running a compare, i.e. get all endpoints but update only the ClearPass EndpointDB with new endpoints, changed attributes i.e. very minimal changes the ingest rate was 1,000 endpoints processed in approximately 6 minutes.