



mobileiron

Device Posture Integration MobileIron and ForgeRock

July 2020
Version 1.0

Initial Version 1.0	July 2020
---------------------	-----------

www.mobileiron.com

Copyright Notice

© 2020 MobileIron, Inc. All rights reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication.

"MobileIron," the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

MobileIron, Inc.
490 East Middlefield Road
Mountain View, CA 94043

Contents

Device Posture Integration - MobileIron and ForgeRock	4
Overview	4
Configurations on MobileIron Cloud	4
Pre-Requisites	4
Integration Workflow	5
Settings and Configuration	5
Configurations on MobileIron Core	8
Pre-Requisites	8
Integration Workflow	8
Settings and Configuration	8
Contact Information	10

Device Posture Integration - MobileIron and ForgeRock

Overview

The following guide walks you through the steps involved in configuring device posture integration between MobileIron UEM (Core or MI Cloud) and ForgeRock Access Manager (AM). The ForgeRock Authentication Node configured as part of the integration in ForgeRock AM queries MobileIron UEM via a ReST API to see whether or not the end-user's device has been deemed compliant (ie, checks the "Device Posture") before they are allowed to access a protected resource. The APIs leveraged by ForgeRock AM are MobileIron's Common Platform Services (CPS) API - which is a common API URI scheme between MobileIron Core & MobileIron Cloud.

The solution involves MobileIron pushing identity (x509) certificates to managed devices containing a unique device identifier (populated in the 'CN' field of the x509 certificate). Mutual Transport Layer Security (mTLS) is configured on ForgeRock AM and each time a device interfaces with ForgeRock, it is requested and required to present its client certificate. The authentication tree in ForgeRock is configured to extract the device's unique identifier from the CN field in the presented certificate; with that in hand, the authentication tree next makes a ReST query to the MobileIron UEM for Device Posture information.

Configurations on MobileIron Cloud

Pre-Requisites

- MobileIron Cloud with Common Platform Services enabled
 - Latest CPS documentation is available here.
<https://help.mobileiron.com/s/mil-productdoclistpage?Id=a1s3400000240gyAAA&Name=Common+Platform+Services+API>
 - Refer above document to enable CPS - you do not need to do any configurations or settings concerning event notifications.

- Make sure you follow the guide to also create an API user and assign CPS roles. You will need this while configuring the authentication node later in Forgerock.

ForgeRock API User | Username: forgerock@api.59f2ea.hotmail.com

✓ Status: Enabled

Overview | Devices | Available Apps | Roles | **Attributes**

NAME	SOURCE	DESCRIPTION
Cisco ISE Operations	Assigned directly to user	Allows a user to invoke API(s) required for Cisco ISE integration.
Common Platform Services (CPS)	Assigned directly to user	Allows a user to use Common Platform Services.
User Read Only	Assigned directly to user	Allows a user to view users and user groups as well as the apps and content catalogs.

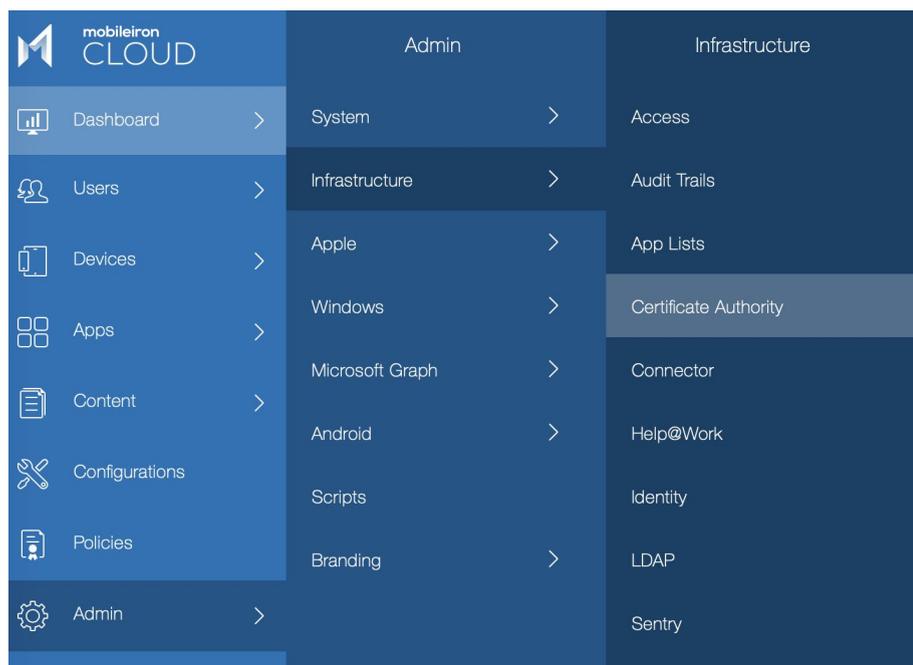
- MobileIron Authentication Node and ForgeRock configured with mTLS:
 - <https://backstage.forgerock.com/marketplace/api/catalog/entries/AXJn29ysTBzErls7wY9e>

Integration Workflow

1. Create local CA
2. Create Certificate Enrollment Configuration and Deploy to Devices
3. Configure ForgeRock AM

Settings and Configuration

1. Create local CA
 - a. MobileIron Cloud Admin Portal : Admin > Infrastructure > Certificate Authority



- b. Click +Add > Create Standalone Certificate Authority

c. Fill in the details accordingly and click Generate

Create a Standalone Certificate Authority✕

1 GENERATE 2 VIEW

Name

Subject Parameters

** Atleast one of the subject params have to be non-empty*

Common Name

Email

Organization Unit

Organization

Street address

City

State

Country

(2 letter code Ex:US)

Key Generation Parameters

Key Type

Signature Algorithm

Key Length

Certificate Lifetime

days

Cache Identities on MobileIron Cloud
Full identities will be stored on MobileIron Cloud instead of being generated each time

2. Create Certificate Enrollment Configuration and Deploy to Devices

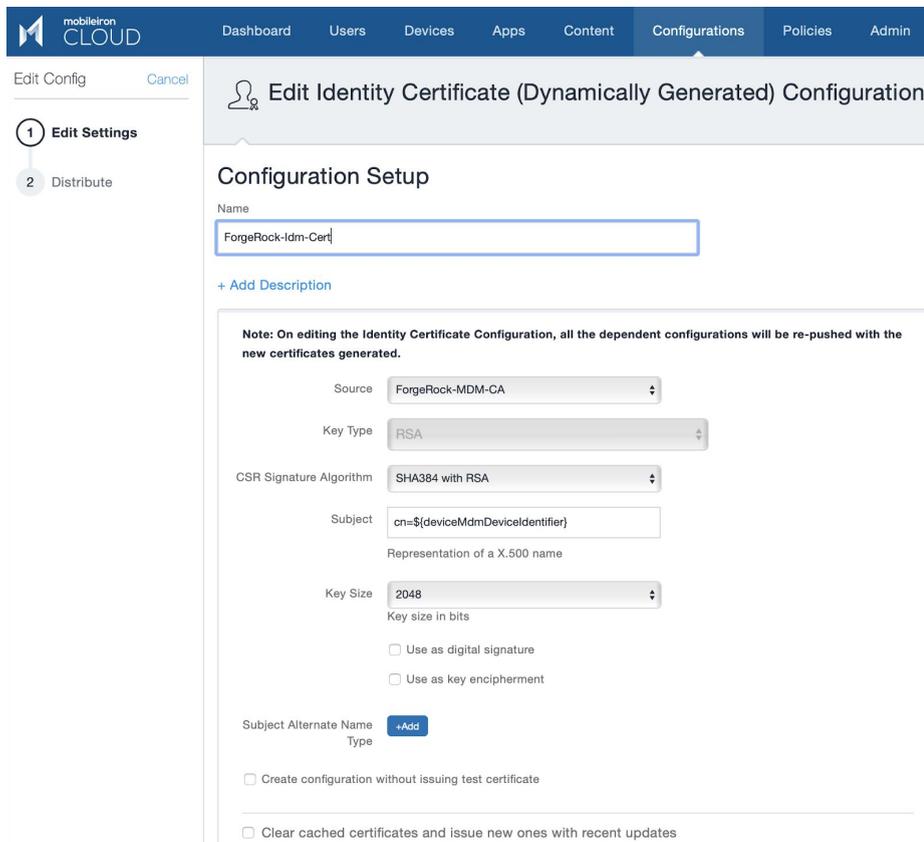
a. MobileIron Cloud Admin: Configurations > +Add

- b. Search for 'Identity Certificate' > Select it

 **Identity Certificate**
Add certificates to allow devices to authenticate to server and network resources.

- c.
- d. Fill in details appropriately and click Test Configuration and Continue
- i. **Set subject as `cn=${deviceMdmDeviceIdentifier}`**



The screenshot shows the 'Edit Identity Certificate (Dynamically Generated) Configuration' page in the MobileIron Cloud interface. The page has a navigation bar with 'mobileiron CLOUD' and tabs for 'Dashboard', 'Users', 'Devices', 'Apps', 'Content', 'Configurations', 'Policies', and 'Admin'. Below the navigation bar, there are two steps: '1 Edit Settings' and '2 Distribute'. The main content area is titled 'Configuration Setup' and contains the following fields:

- Name: ForgeRock-Idm-Cert
- + Add Description
- Note: On editing the Identity Certificate Configuration, all the dependent configurations will be re-pushed with the new certificates generated.
- Source: ForgeRock-MDM-CA
- Key Type: RSA
- CSR Signature Algorithm: SHA384 with RSA
- Subject: `cn=${deviceMdmDeviceIdentifier}`
Representation of a X.500 name
- Key Size: 2048
Key size in bits
- Use as digital signature
- Use as key encipherment
- Subject Alternate Name Type: +Add
- Create configuration without issuing test certificate
- Clear cached certificates and issue new ones with recent updates

- e. Define device group to which the certificate enrollment settings are to be distributed and save the configuration

3. Configure ForgeRock AM

- a. Please refer this article to know more about the configuration for ForgeRock
<https://backstage.forgerock.com/marketplace/api/catalog/entries/AXJn29ysTBzErls7wY9e>

Configurations on MobileIron Core

Pre-Requisites

- MobileIron Core with Common Platform Services enabled
 - Latest CPS documentation is available here.
<https://help.mobileiron.com/s/mil-productdoclistpage?Id=a1s3400000240gyAAA&Name=Common+Platform+Services+API>
 - Refer above document to enable CPS - you do not need to do any configurations or settings concerning event notifications
 - Make sure you follow the guide to also create an API user and assign CPS roles. You will need this while configuring the authentication node later in Forgerock screen.
- ForgeRock Authentication Node and configured with mTLS
 - <https://backstage.forgerock.com/marketplace/api/catalog/entries/AXJn29ysTBzErls7wY9e>

Integration Workflow

1. Create local CA
2. Create SCEP Configuration and Deploy to Devices
3. Configure ForgeRock AM

Settings and Configuration

1. Create Local CA
 - a. MobileIron Core Admin: Services > Local CA > Add New > Fill in Details
 - b. Click Generate and Click Save
 - c. **Note:** Set Key Lifetime no more than 3 years

Generate Self-Signed Certificate
✕

Local CA Name

Key Type

Key Length

CSR Signature Algorithm

Key Lifetime (in days)

Issuer Name

Cancel
Generate

2. Create SCEP configurations and deploy to devices

- a. MobileIron Core Admin: Policies and Configs > Certificate Enrollment > Local
- b. Fill in information and click Issue Test Certificate
- c. Click Save

Note: Set the subject to CN=\$DEVICE_UDID\$

Edit Local Certificate Enrollment Setting
✕

Name

Description

Store keys on core ❗

User Certificate Device Certificate

Local CAs

Key Type ❗

Subject

Subject Common Name Type

Key Usage Signing Encryption

Key Length ❗

CSR Signature Algorithm ❗

Subject Alternative Names

TYPE	VALUE

Issue Test Certificate ❗
Cancel
Save

- d. MobileIron Core Admin Portal > Policies and Configs > Search or select the recently created Certificate Enrollment Setting > Click Actions > Apply to Labels and select appropriate labels to push this app to required audience
3. Configure ForgeRock AM
 - a. Please refer this article to know more about the configurations on ForgeRock <https://backstage.forgerock.com/marketplace/api/catalog/entries/AXJn29ysTBzErls7wY9e>

Contact Information

Please contact MobileIron Technology Ecosystem team at ecosystem@mobileiron.com with any questions.