mobileiron

Device Posture Integration MobileIron and ForgeRock

July 2020
Version 1.0

Initial Version 1.0	July 2020

www.mobileiron.com

Copyright Notice

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

Contents

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.

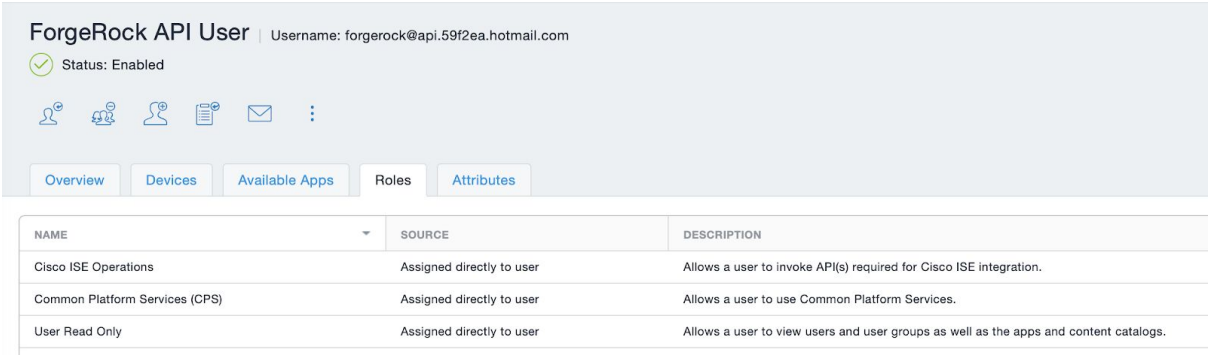
The solution involves MobileIron pushing identity (x509) certificates to managed devices containing a unique device identifier (populated in the 'CN' field of the x509 certificate). Mutual Transport Layer Security (mTLS) is configured on ForgeRock AM and each time a device interfaces with ForgeRock, it is requested and required to present it's 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.



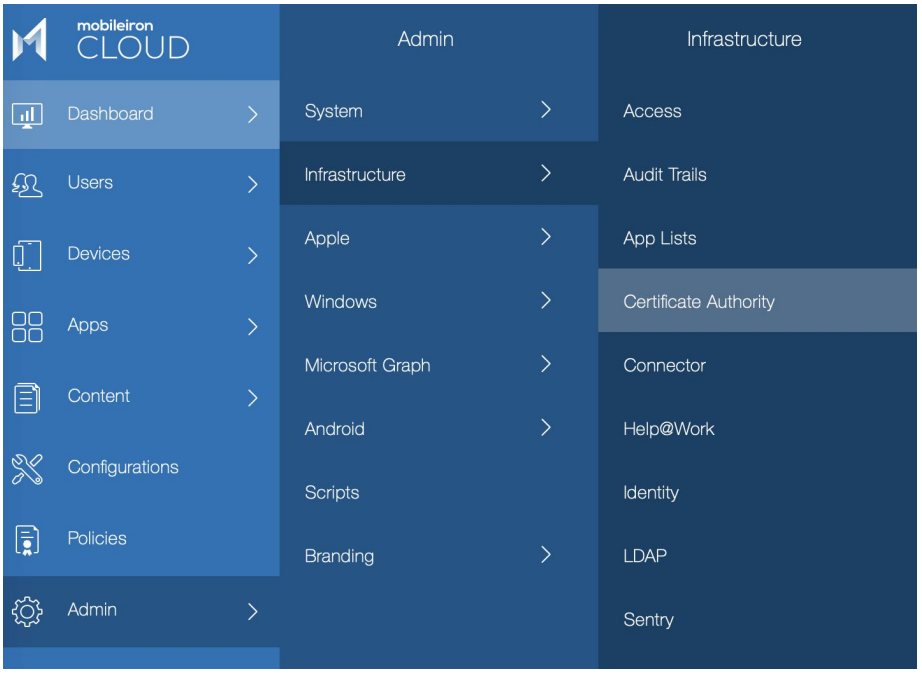
- MobileIron Authentication Node and ForgeRock configured with mTLS:
  - https://backstage.forgerock.com/marketplace/api/catalog/entries/AXJn29ysTBzErls7wY9e

Integration Workflow

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

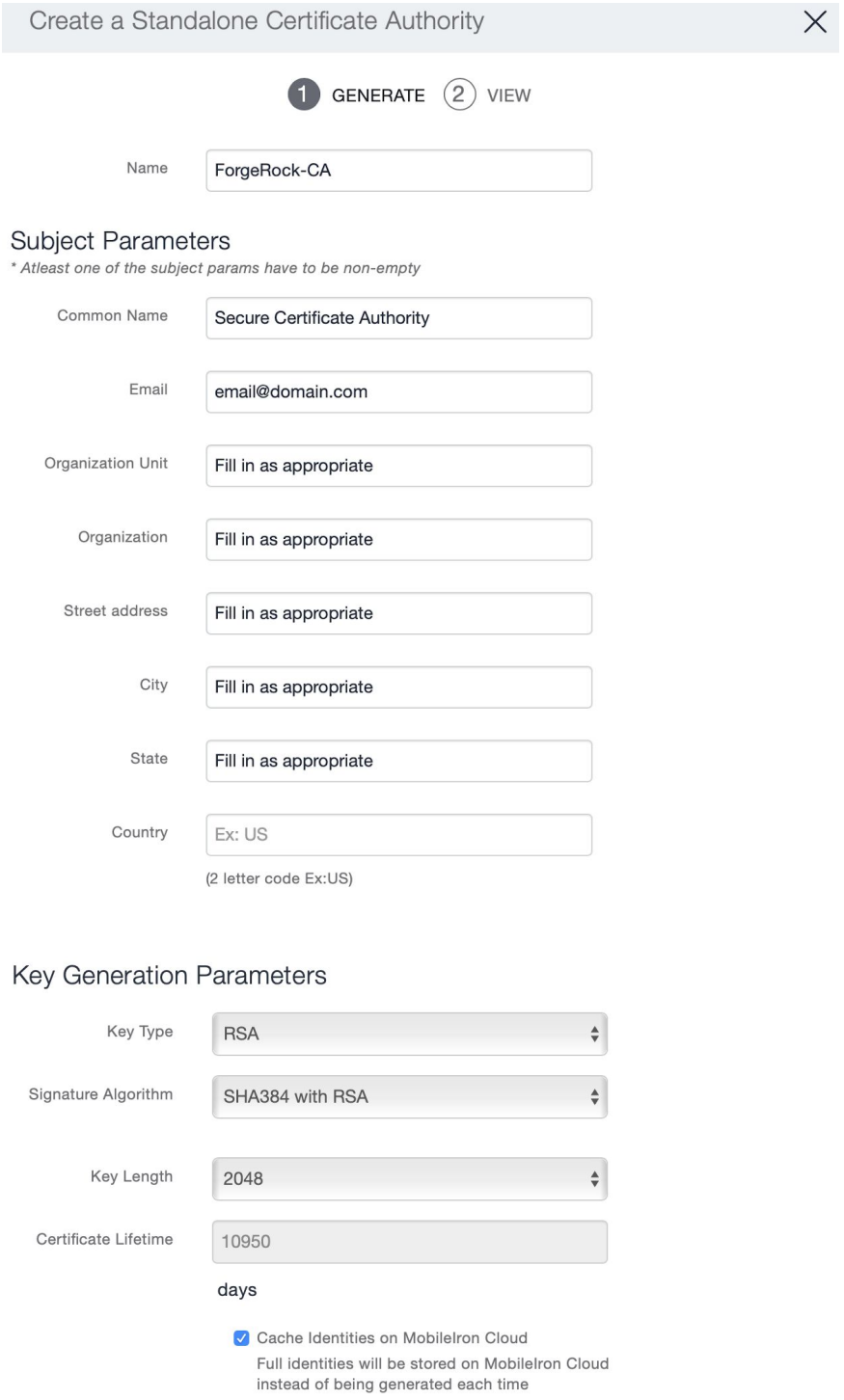
Settings and Configuration

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



   b. Click +Add > Create Standalone Certificate Authority

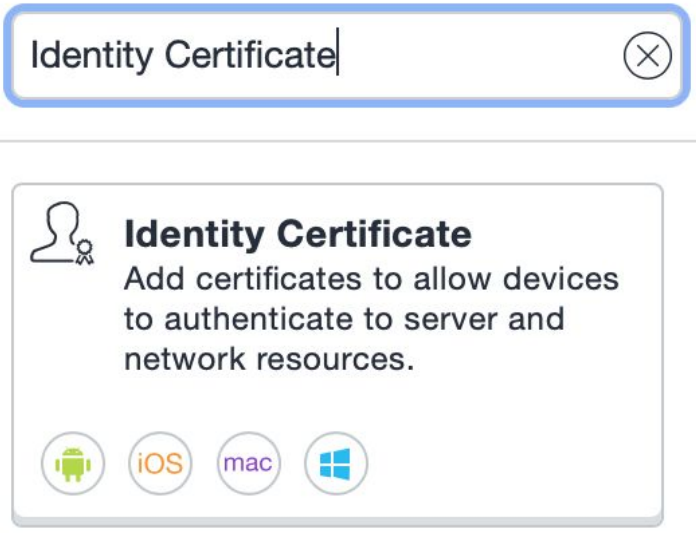
c. Fill in the details accordingly and click Generate



2. Create Certificate Enrollment Configuration and Deploy to Devices

a. MobileIron Cloud Admin: Configurations > +Add

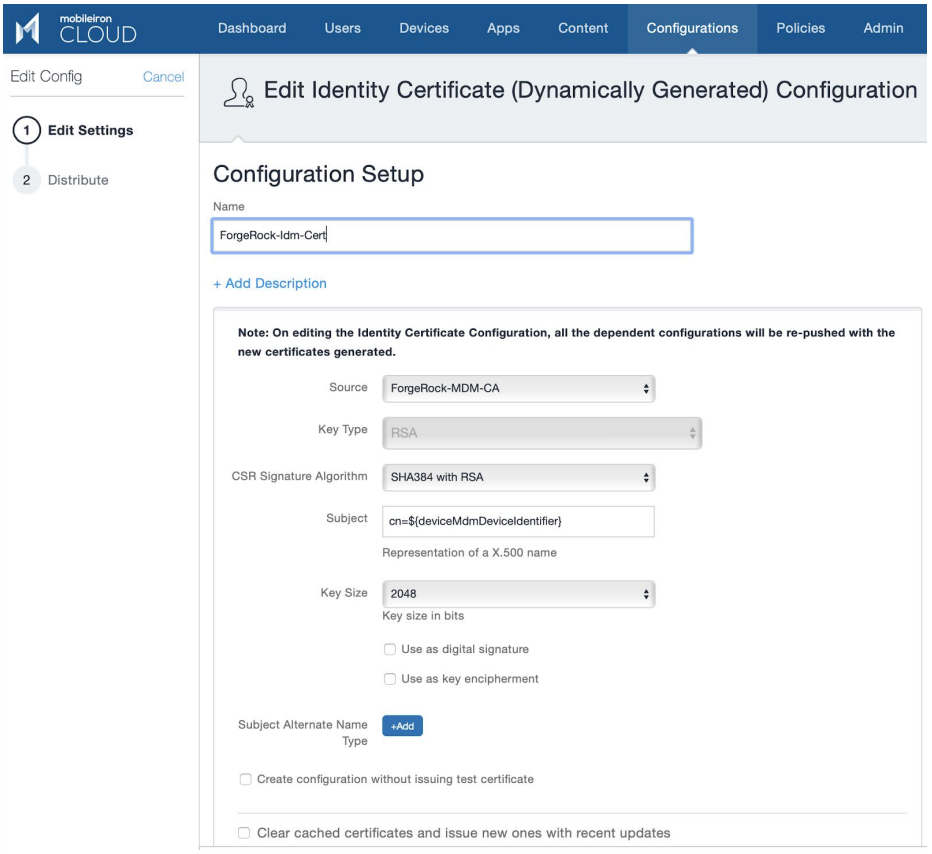
b. Search for ‘Identity Certificate’ > Select it



c.

d. Fill in details appropriately and click Test Configuration and Continue

   i. **Set subject as cn=${deviceMdmDeviceIdentifier}**



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.

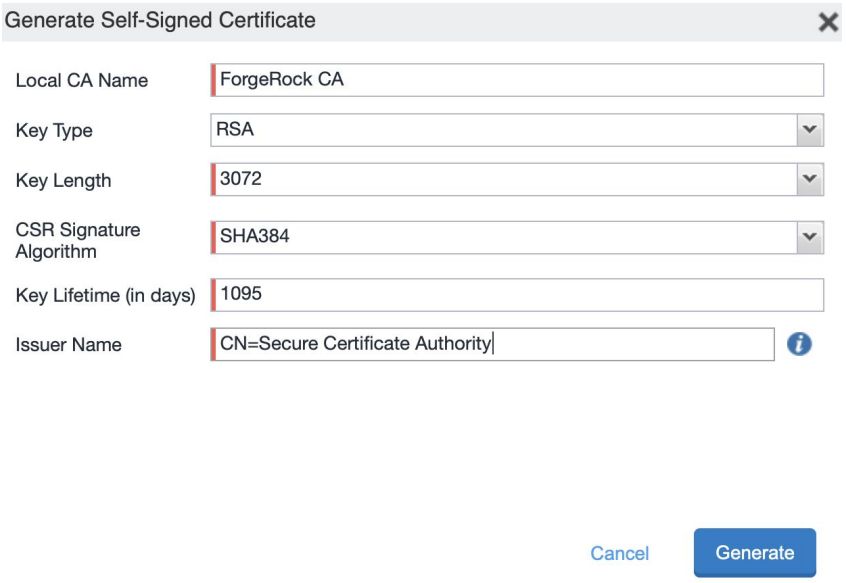
- ForgeRock Authentication Node and configured with mTLS
    - https://backstage.forgerock.com/marketplace/api/catalog/entries/AXJn29ysTBzErls7wY9e

Integration Workflow

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

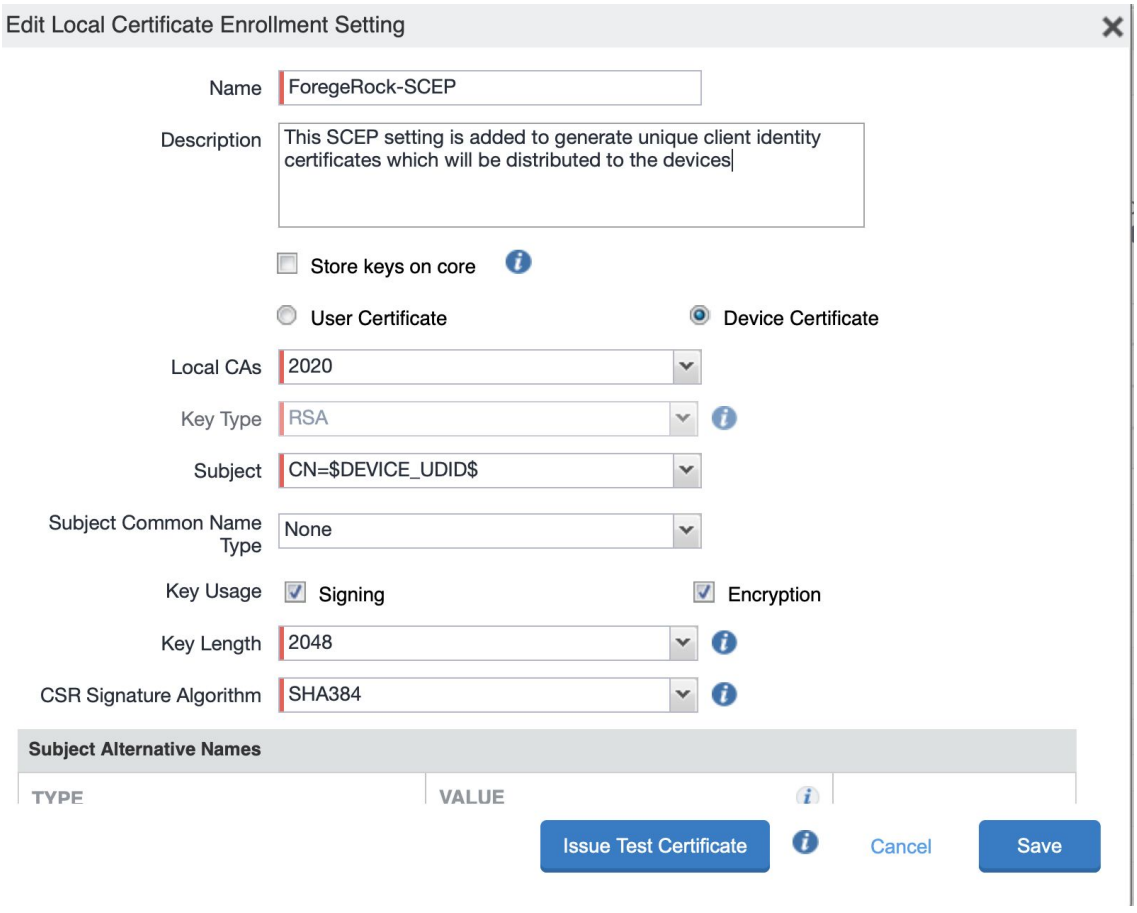
Settings and Configuration

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



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=$DEVICE_UDID$



    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.