

# Securing access to OneLogin with certificates deployed from MobileIron UEM

April 2020  
Version 1.0

Initial Version 1.0	April 2020
---------------------	------------

[www.mobileiron.com](http://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

<b>Securing access to OneLogin with Certificates deployed from MobileIron UEM</b>	<b>4</b>
Overview	4
Create LocalCA	5
Create Certificate Enrollment / Identity Certificate Configuration and deploy to devices	8
Extracting Root Certificate from MobileIron	11
Device Trust Configuration in OneLogin	11
Contact Information	15

# Securing access to OneLogin with Certificates deployed from MobileIron UEM

## Overview

OneLogin (IdP) provides SSO into an array of enterprise applications based on the user's role and MobileIron manages and secures the endpoint including distribution of sanctioned apps along with their managed configurations.

OneLogin hosts an IdP portal which can be accessed by a browser on a mobile or desktop. When the user attempts to login on a mobile app, where authentication is federated with OneLogin it prompts the user to enter their username, password and select the x509 client identity certificate that is deployed from UEM. The identity certificate is procured by MobileIron UEM from its LocalCA and issued to a managed device which will be leveraged at the time of authentication. The LocalCA's root certificate is uploaded into OneLogin tenant to ensure a secure trust is established between the user on the device and OneLogin. If the device falls out of compliance, MobileIron UEM removes the identity certificate thus denying access to login to OneLogin portal consequently denying access to enterprise apps.

In short, the integration ensures that sign-in to OneLogin is restricted to users who have a certificate that MobileIron creates/deploy on devices thus creating an *equivalent* of device trust solution

There is however a caveat though, for applications that use their own mobile browser such as O365, this solution is not applicable. OneLogin therefore provides App Policies which can be configured to be applied to specific applications that mandates a certificate at the time of sign-on. While the user policies apply during login to OneLogin - in terms of hierarchy, the user logs in to OneLogin before they log in to the app, so the app policy is something that would only be used in a "hybrid" rollout

## Create LocalCA

### Core:

1. MobileIron Core Admin: Services > Local CA > Add New > Fill in Details
2. Click Generate and Click Save

**Note:** Set Key Lifetime no more than 3 years.

Generate Self-Signed Certificate

Local CA Name

OneLogin-CA

Key Type

RSA

Key Length

3072

CSR Signature Algorithm

SHA384

Key Lifetime (in days)

1095

Issuer Name

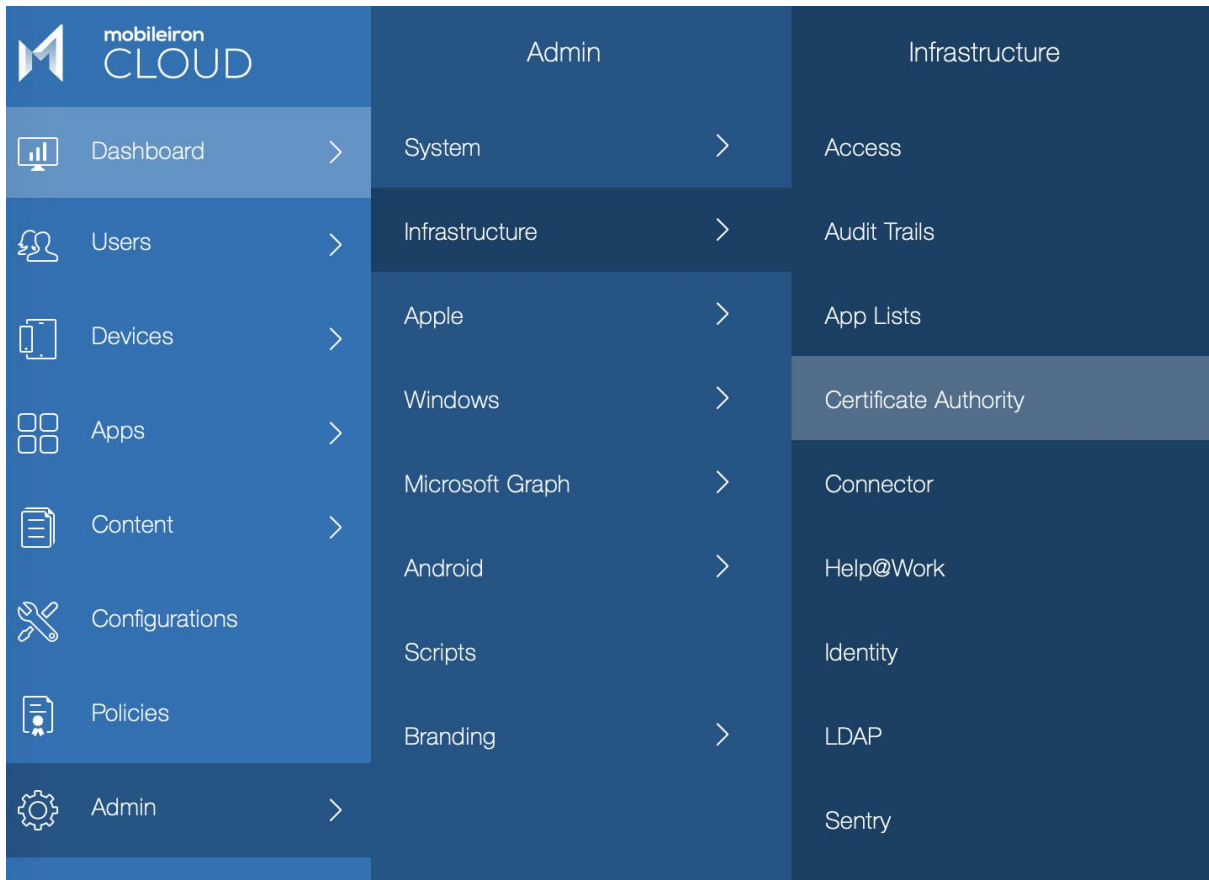
CN=Secure Certificate Authority

Cancel

Generate

## MI Cloud:

1. MobileIron Cloud Admin Portal : Admin > Infrastructure > Certificate Authority



2. Click +Add > Create Standalone Certificate Authority
3. Fill in the details accordingly and click Generate

! Create a Standalone Certificate Authority



1 GENERATE 2 VIEW

Name

OneLogin-LocalCA

### Subject Parameters

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

Common Name

Secure Certificate Authority

Email

email@domain.com

Organization Unit

Fill in as appropriate

Organization

Fill in as appropriate

Street address

Fill in as appropriate

City

Fill in as appropriate

State

Fill in as appropriate

Country

CA

(2 letter code Ex:US)

### Key Generation Parameters

Key Type	<div>RSA</div>
Signature Algorithm	<div>SHA384 with RSA</div>
Key Length	<div>2048</div>
Certificate Lifetime	<div>10950</div>

days

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

## Create Certificate Enrollment / Identity Certificate Configuration and deploy to devices

### Core:

1. MobileIron Core Admin: Policies and Configs > Certificate Enrollment > Local
2. Fill in information and click Issue Test Certificate
3. Click Save



New Local Certificate Enrollment Setting

Name
OneLogin-SCEP

Description
This SCEP setting is added to generate unique client identity certificates which will be distributed to the devices to be used by OneLogin

☐ Store keys on core

☐ User Certificate
☒ Device Certificate

Local CAs
OneLogin-CA

Key Type
RSA

Subject
CN=\$EMAIL\$

Subject Common Name Type
None

Key Usage
☒ Signing
☒ Encryption

Key Length
2048

CSR Signature Algorithm
SHA384

Subject Alternative Names

TYPE	VALUE

Issue Test Certificate
Cancel
Save

- 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

### MI Cloud:

- MobileIron Cloud Admin: Configurations > +Add
- Search for 'Identity Certificate' > Select it

Identity Certificate



## Identity Certificate

Add certificates to allow devices to authenticate to server and network resources.



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

mobileiron CLOUD

Configurations / Details

Add Config Cancel

1 Create Settings

2 Distribute

Create Identity Certificate Configuration

User-, device-, or group-based certificates can be used to authenticate access to resources such as websites, email servers, and network components like VPN or Wi-Fi. After manually uploading a certificate, you can set your email, Wi-Fi, or VPN configurations to use the identity cert [More...](#)

Name

OneLogin Identity Certificate Configuration

+ Add Description

Configuration Setup

Certificate Distribution

Dynamically Generated

Source OneLoginLocalCA

Key Type RSA

CSR Signature Algorithm SHA256 with RSA

Subject \$[userEmailAddress]

Representation of a X.509 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

Back Test Configuration and Continue

4. Define device group to which the certificate enrollment settings are to be distributed.

## Extracting Root Certificate from MobileIron

## Core:

1. MobileIron Core Admin: Services > Local CA > Select the OneLogin CA you created > Click View Certificate

OneLogin-CA		Active	1	0	<a href="#">View Certificate</a>
Name	Value				
Name	OneLogin-CA				
CA Created	04-17-2020 05:52:19				
CA Modified	04-17-2020 05:53:11				
CA Signature Algorithm	SHA384withRSA				

2. Copy the contents of the screen and share it with your OneLogin contact

## MI Cloud:

1. MobileIron Cloud Admin Portal : Admin > Infrastructure > Certificate Authority
2. Select Actions > Download Certificate

<input checked="" type="checkbox"/>	OneLogin-LocalCA	Local	April 16, 2020	April 9, 2050	No	<a href="#">Actions</a>
Showing 1 to 6 of 6						
						<a href="#">Edit</a>
						<a href="#">View Issued Certificates</a>
						<a href="#">Download Certificate</a>

3. Share the certificate with your OneLogin contact

# Device Trust Configuration in OneLogin

## Creating or Modifying a OneLogin Policy

1. After the certificate is loaded in to your OneLogin account, navigate to your OneLogin account and log in as an Administrator
2. Navigate to Administration → Security → Policies
3. Create or modify an existing policy. For testing, OneLogin recommends creating a new policy
4. In the policy, navigate to MFA → Require trusted device

Policies / Certificate Policy [More Actions](#) [Save](#)

Sign In	<b>Require trusted device</b>
Password Update	<input type="checkbox"/> Enabled ⓘ
Session	<input type="checkbox"/> Allow self-installation
<b>MFA</b>	ⓘ PKI certificates are installed in the user's browser and can be used as a second authentication factor. Once installed, the user can only sign in using a browser that has the certificate. Read more about <a href="#">PKI Certificates</a>
IP Addresses	Certificate expires in
Customization	1 Year

5. Check the box to enable trusted device

Policies / Certificate Policy More Actions Save

Sign In	<b>Require trusted device</b> <input checked="" type="checkbox"/> Enabled ⓘ <input type="checkbox"/> 3rd Party Certificates Enabled <input type="checkbox"/> Allow self-installation <div>             ⓘ PKI certificates are installed in the user's browser and can be used as a second authentication factor. Once installed, the user can only sign in using a browser that has the certificate. Read more about <a href="#">PKI Certificates</a> </div>
Password Update	
Session	
<b>MFA</b>	
IP Addresses	
Customization	Certificate expires in 1 Year

## 6. Check the box to enable 3rd Party Certificates

Policies / Certificate Policy More Actions Save

Sign In	<b>Require trusted device</b> <input checked="" type="checkbox"/> Enabled ⓘ <input checked="" type="checkbox"/> 3rd Party Certificates Enabled Select Certificates for Validation <input type="text"/> <input type="checkbox"/> Allow self-installation <div>             ⓘ PKI certificates are installed in the user's browser and can be used as a second authentication factor. Once installed, the user can only sign in using a browser that has the certificate. Read more about <a href="#">PKI Certificates</a> </div>
Password Update	
Session	
<b>MFA</b>	
IP Addresses	
Customization	Certificate expires in 1 Year

## 7. Select the certificate(s) for validation under this policy

Policies / Certificate Policy More Actions Save

Sign In	<b>Require trusted device</b> <input checked="" type="checkbox"/> Enabled ⓘ <input checked="" type="checkbox"/> 3rd Party Certificates Enabled Select Certificates for Validation <div>jeff intermediate ca1 ✕</div> <input type="text"/> <input type="checkbox"/> Allow self-installation <div>             ⓘ PKI certificates are installed in the user's browser and can be used as a second authentication factor. Once installed, the user can only sign in using a browser that has the certificate. Read more about <a href="#">PKI Certificates</a> </div>
Password Update	
Session	
<b>MFA</b>	
IP Addresses	
Customization	Certificate expires in 1 Year

## Assigning a Policy to a User

1. As a OneLogin administrator, navigate to Users → Users
2. Select a user and navigate to the Authentication tab
3. Under the User security policy section, select the policy where trusted device is enabled

Users / cert-fn cert-ln More Actions Save User

User Info
Authentication
Applications
Devices
Activity

**Authentication**

Group: None

Trusted IDP: -- NONE --

Authenticated by: OneLogin

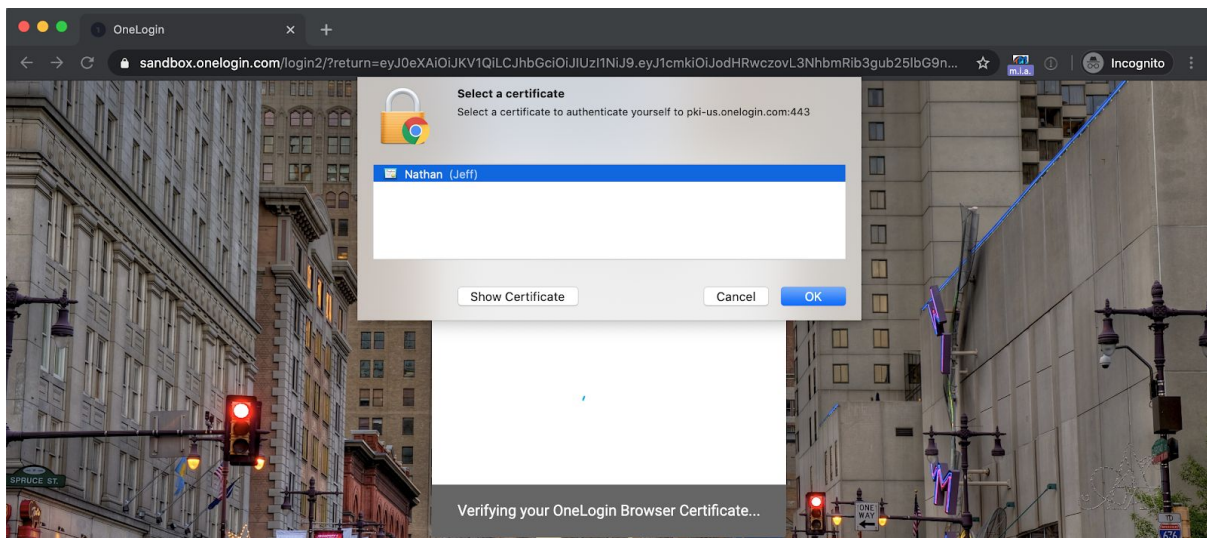
User security policy: Certificate Policy

Multi-factor methods

Search: |

- default is Default policy --
- AAA
- PKI Certificate Policy
- Certificate Policy
- Sandbox User Policy

4. Test the certificate policy by logging in as the user. OneLogin will prompt the user for the certificate on log in



## Application Policy Configuration

Note: This is an optional configuration. Certificates are typically required on login to OneLogin, but for a “hybrid” rollout, they can be required only for login to specific applications

1. As a OneLogin Administrator, navigate to Administration → Security → Policies
2. Create or modify an existing App Policy
3. In the policy, navigate to Require trusted device
4. Check the box to enable trusted device

### Require trusted device

☐ Enabled ⓘ

5. Check the box to enable 3rd Party Certificates

### Require trusted device

☒ Enabled ⓘ

☐ 3rd Party Certificates Enabled

6. Select the certificate(s) for validation under this policy

### Require trusted device

☒ Enabled ⓘ

☒ 3rd Party Certificates Enabled

Select Certificates for Validation

jeff intermediate ca1 ✕

### Applying an App Policy to an App

1. As a OneLogin Administrator, navigate to Administration → Applications → Applications
2. Select an application
3. In the application configuration settings, navigate to Access
4. Set up the policy as either a policy for all users or for a specific role

Applications /  
Box

More Actions Save

Info

Configuration

Parameters

Rules

SSO

Access

Provisioning

Users

Policy

By default all your users will be using this policy to log into this app

App Policy: Certificates

Role-based policy

Make exception for the users in a role and select a policy for them. Make sure the roles are enabled from the ROLE ACCESS SECTION below

Business Development

will use

App Policy: Certificates

Remove

Note: Choose a policy for all users if the policy should apply to all users who sign in to the application. Choose a role-based policy if the policy should apply to only specific users who sign in to the application

## Contact Information

Please contact the Mobileiron Technology Ecosystem team at [ecosystem@mobileiron.com](mailto:ecosystem@mobileiron.com) with any questions or [partners@onelogin.com](mailto:partners@onelogin.com)