Securing access to OneLogin with certificates deployed from MobileIron UEM

April 2020
Version 1.0

Initial Version 1.0	April 2020

www.mobileiron.com

Copyright Notice

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

Contents

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/deploys on devices thus creating an *equivalent* of device trust solution

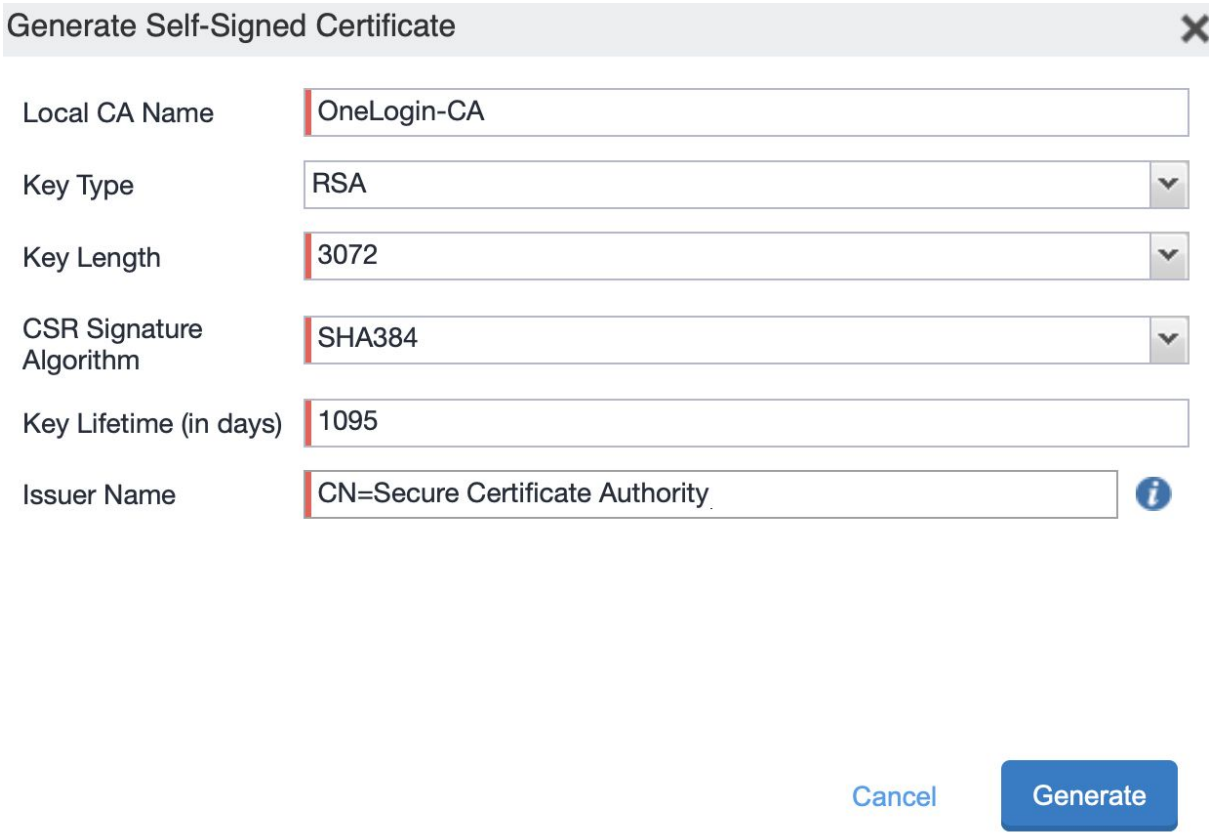
There is however a caveat though, for applications that use their own mobile browser such as O365, this solution is not applicable. OneLogin therefore provides App Policies which can be configured to be applied to specific applications that mandates a certificate at the time of sign-on. While the user 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:

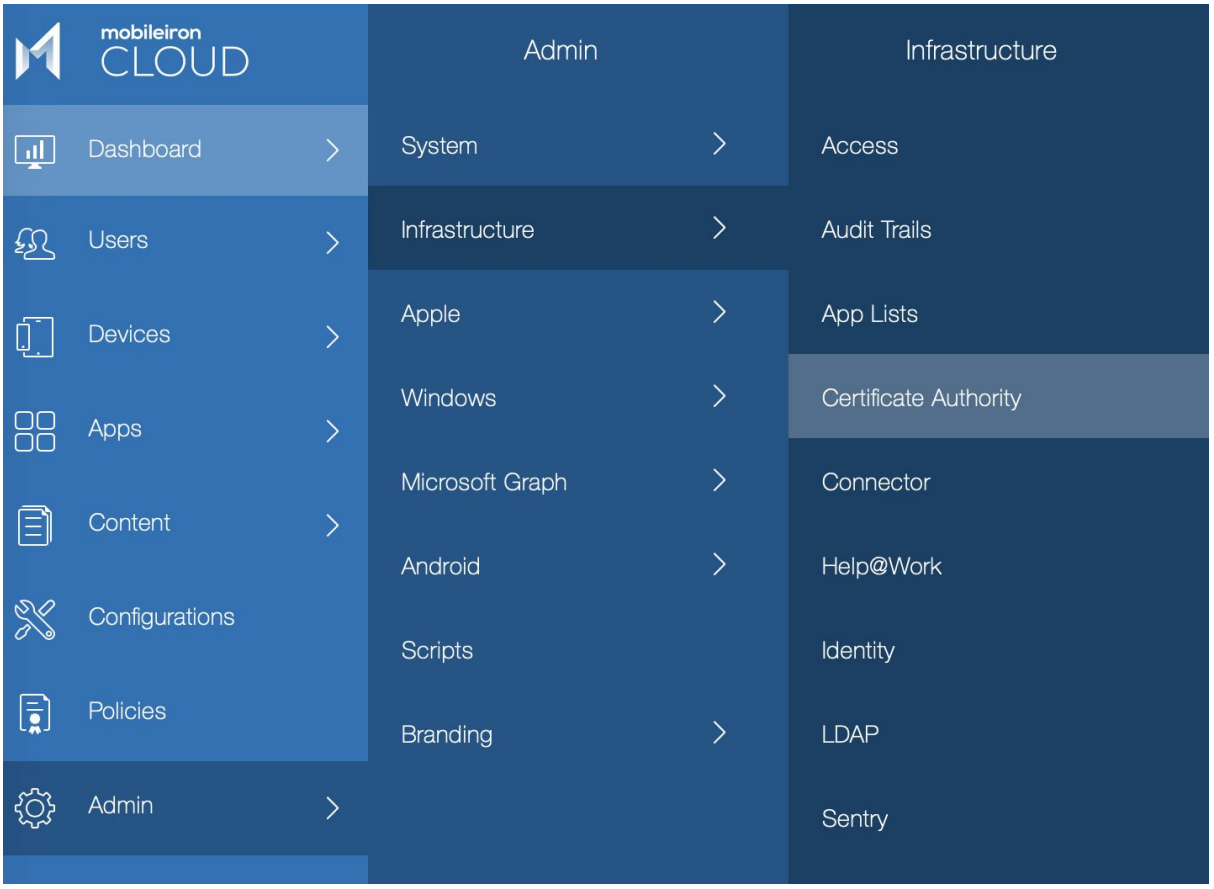
1. MobileIron Core Admin: Services > Local CA > Add New > Fill in Details
2. Click Generate and Click Save

Note: Set Key Lifetime no more than 3 years.

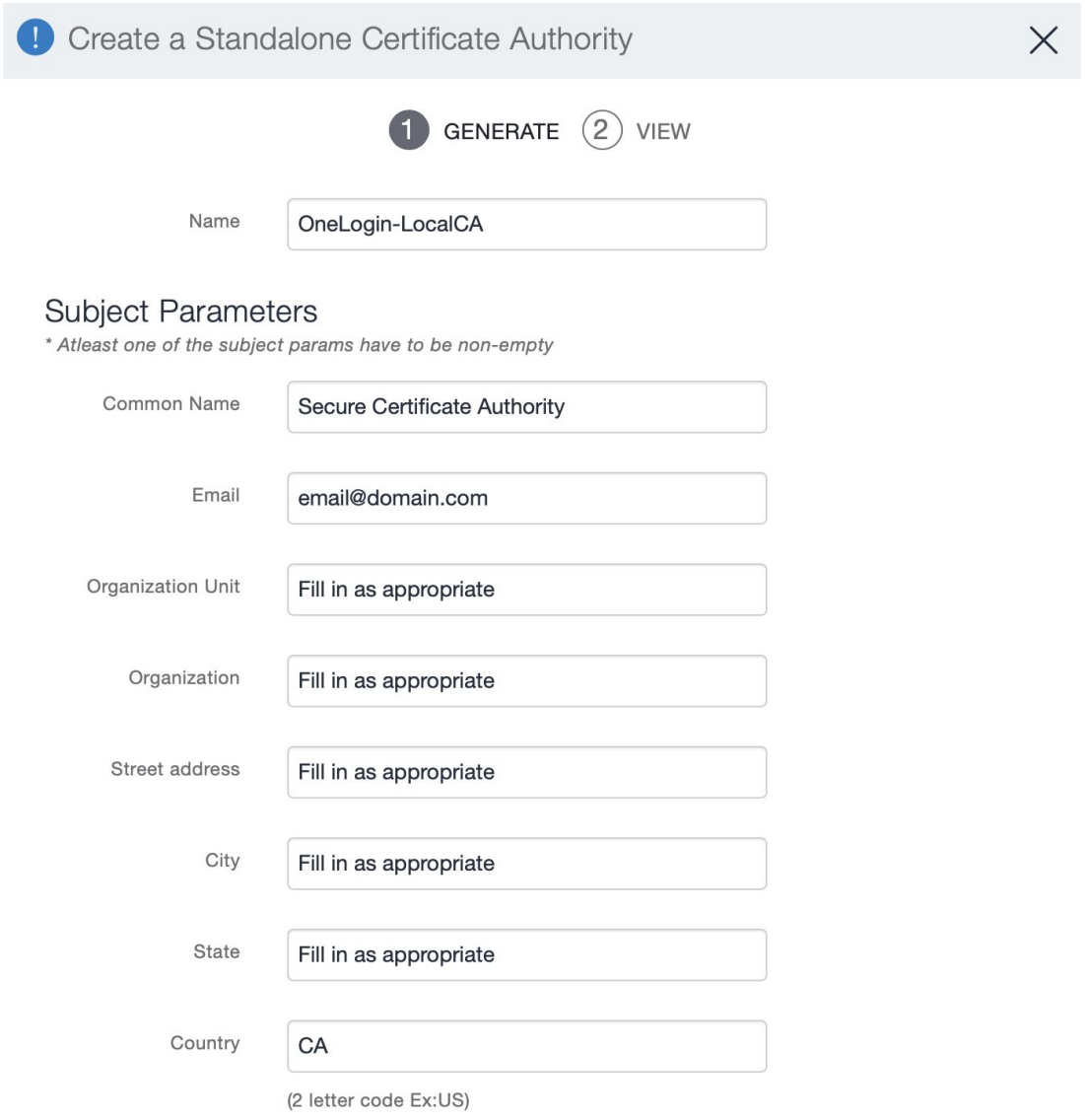


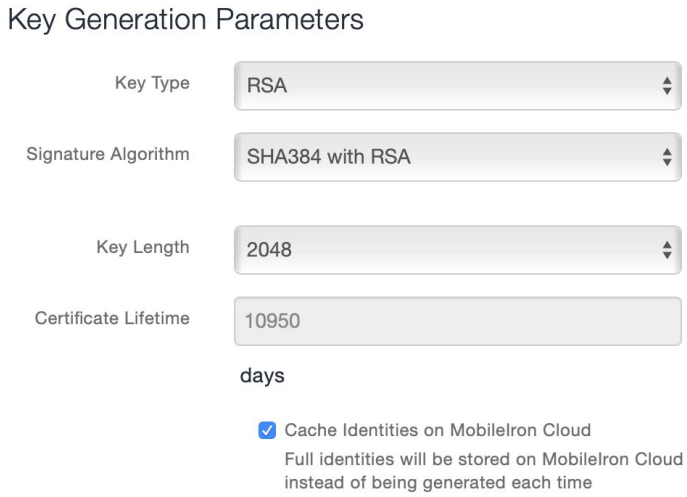
MI Cloud:

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

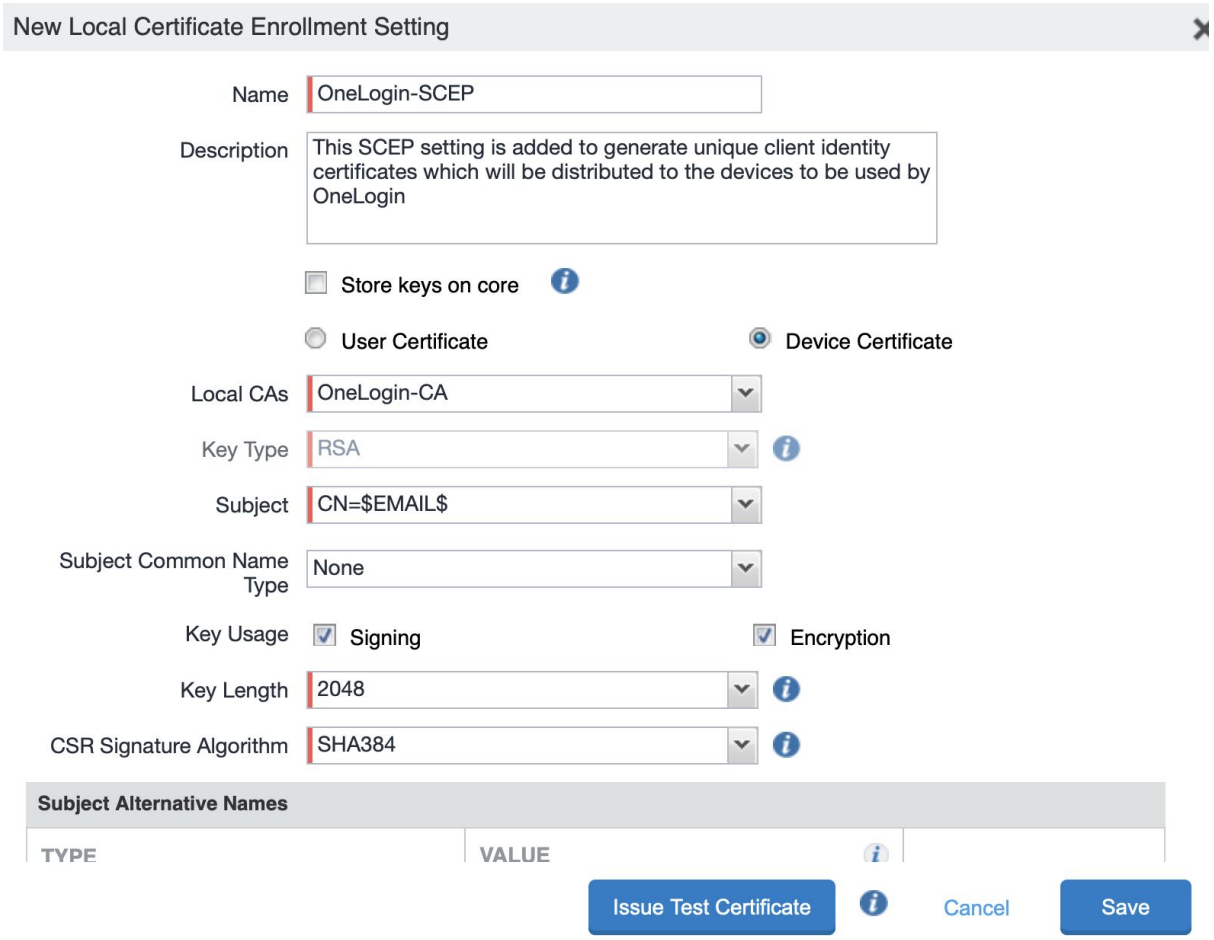

Create a Standalone Certificate Authority
1 GENERATE
2 VIEW
Name
OneLogin-LocalCA
Subject Parameters
* Atleast one of the subject params have to be non-empty
Common Name
Secure Certificate Authority
Email
email@domain.com
Organization Unit
Fill in as appropriate
Organization
Fill in as appropriate
Street address
Fill in as appropriate
City
Fill in as appropriate
State
Fill in as appropriate
Country
CA
(2 letter code Ex:US)



Create Certificate Enrollment / Identity Certificate Configuration and deploy to devices

Core:

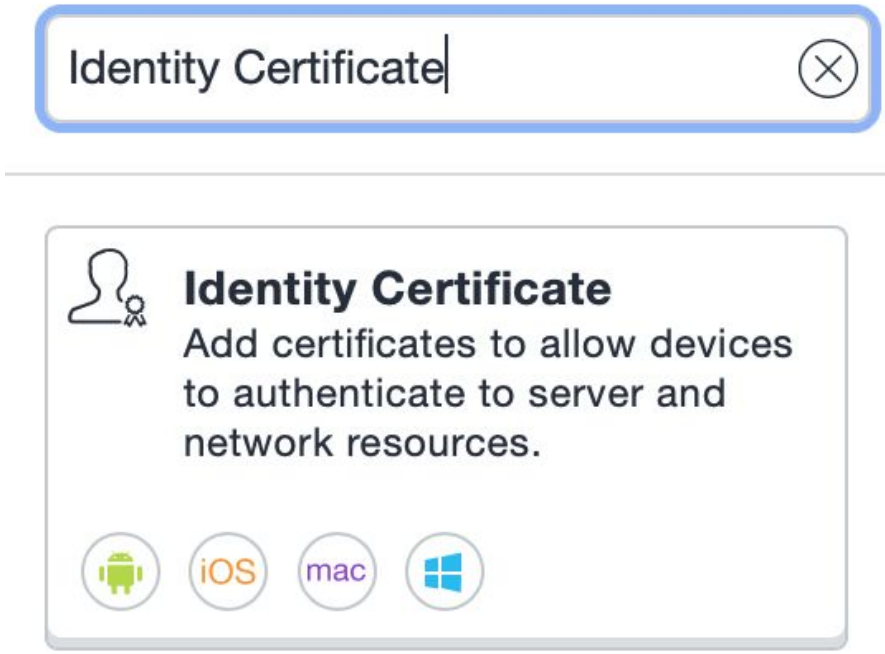
1. MobileIron Core Admin: Policies and Configs > Certificate Enrollment > Local
2. Fill in information and click Issue Test Certificate
3. Click Save



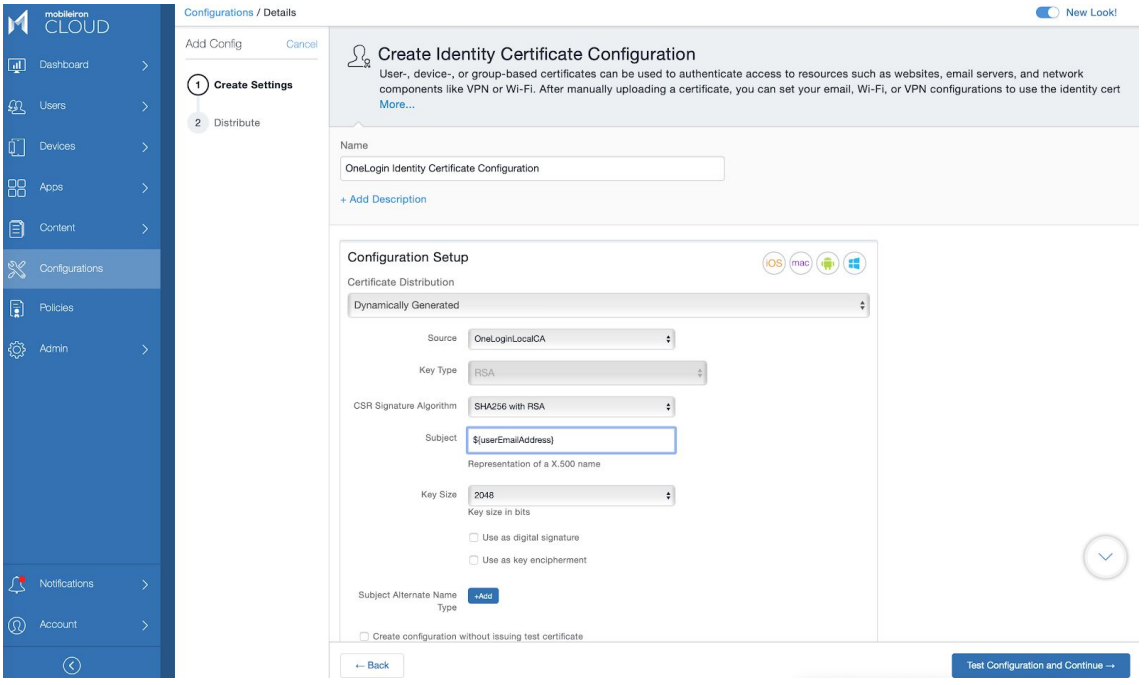
4. MobileIron Core Admin Portal > Policies and Configs > Search or select the recently created Certificate Enrollment Setting > Click Actions > Apply to Labels and select appropriate labels to push this app to required audience

MI Cloud:

1. MobileIron Cloud Admin: Configurations > +Add
2. Search for ‘Identity Certificate’ > Select it



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

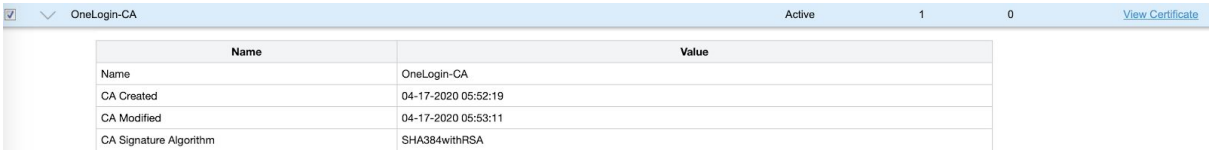


4. Define device group to which the certificate enrollment settings are to be distributed.

Extracting Root Certificate from MobileIron

Core:

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



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

MI Cloud:

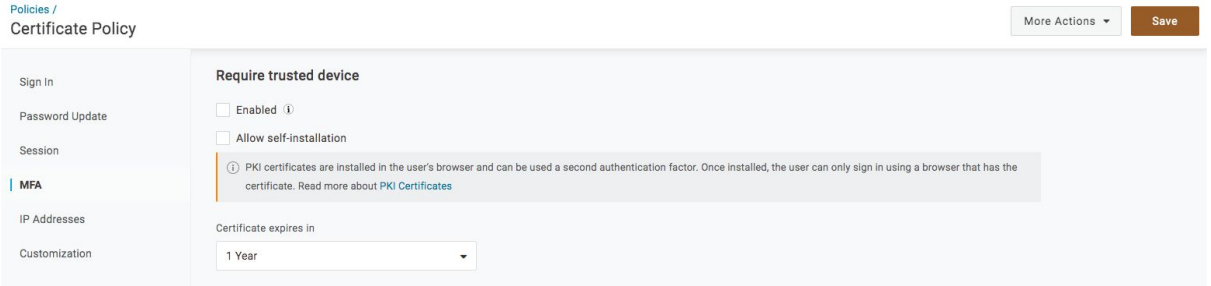
1. MobileIron Cloud Admin Portal : Admin > Infrastructure > Certificate Authority
2. Select Actions > Download Certificate

3. Share the certificate with your OneLogin contact

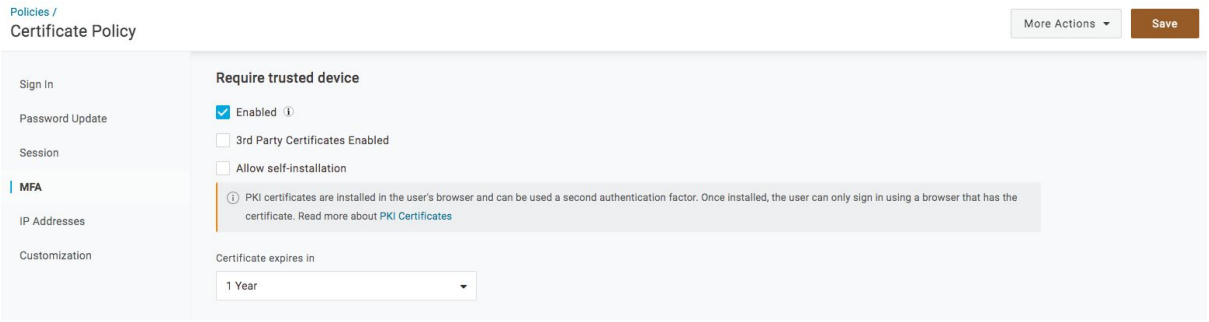
Device Trust Configuration in OneLogin

Creating or Modifying a OneLogin Policy

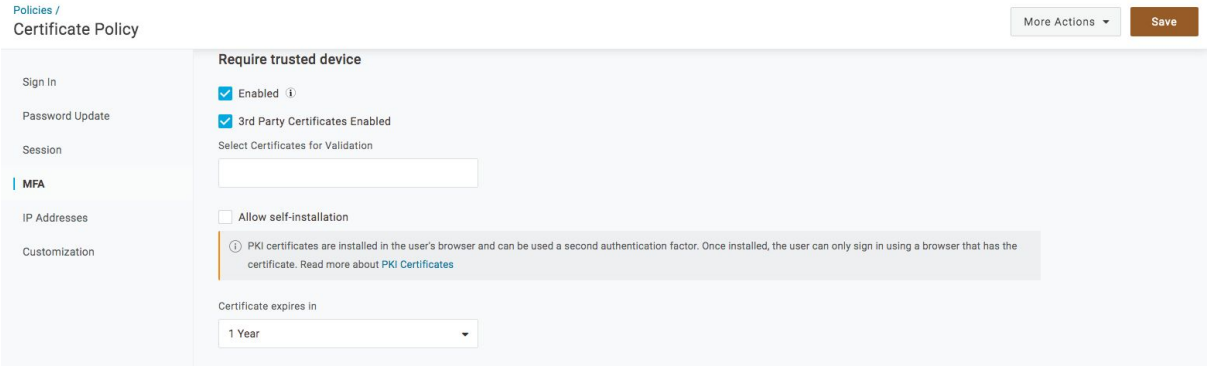
1. After the certificate is loaded in to your OneLogin account, navigate to your OneLogin account and log in as an Administrator
2. Navigate to Administration → Security → Policies
3. Create or modify an existing policy. For testing, OneLogin recommends creating a new policy
4. In the policy, navigate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



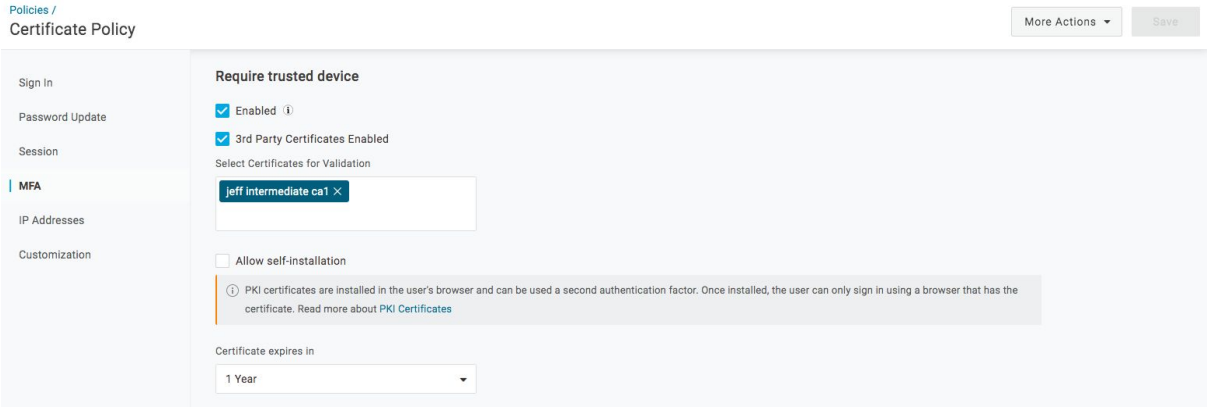
5. Check the box to enable trusted device



6. Check the box to enable 3rd Party Certificates

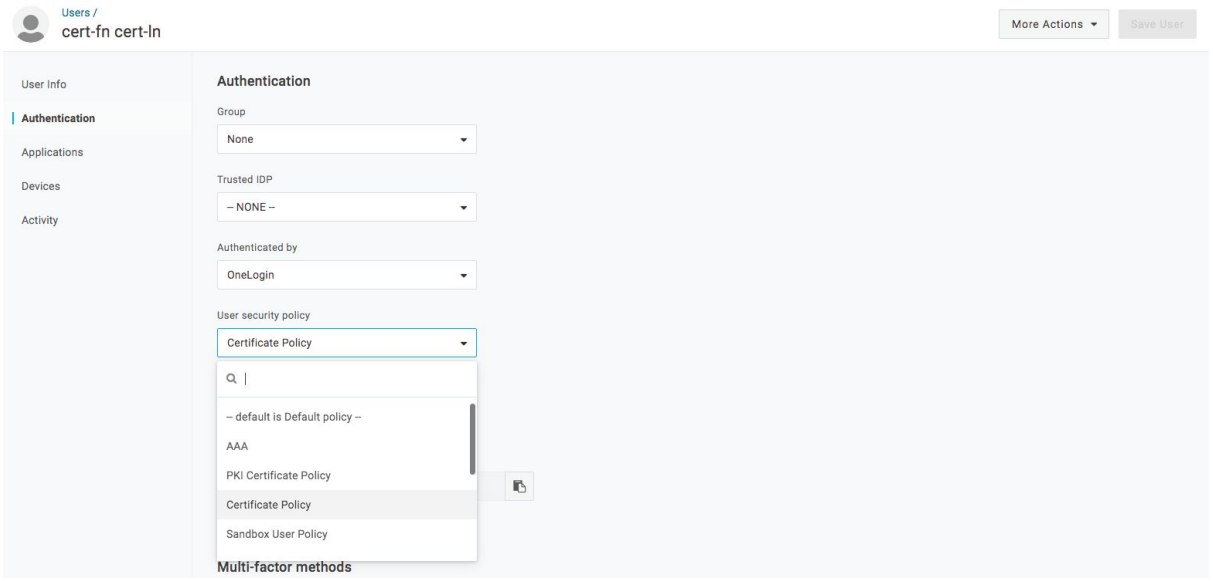


7. Select the certificate(s) for validation under this policy

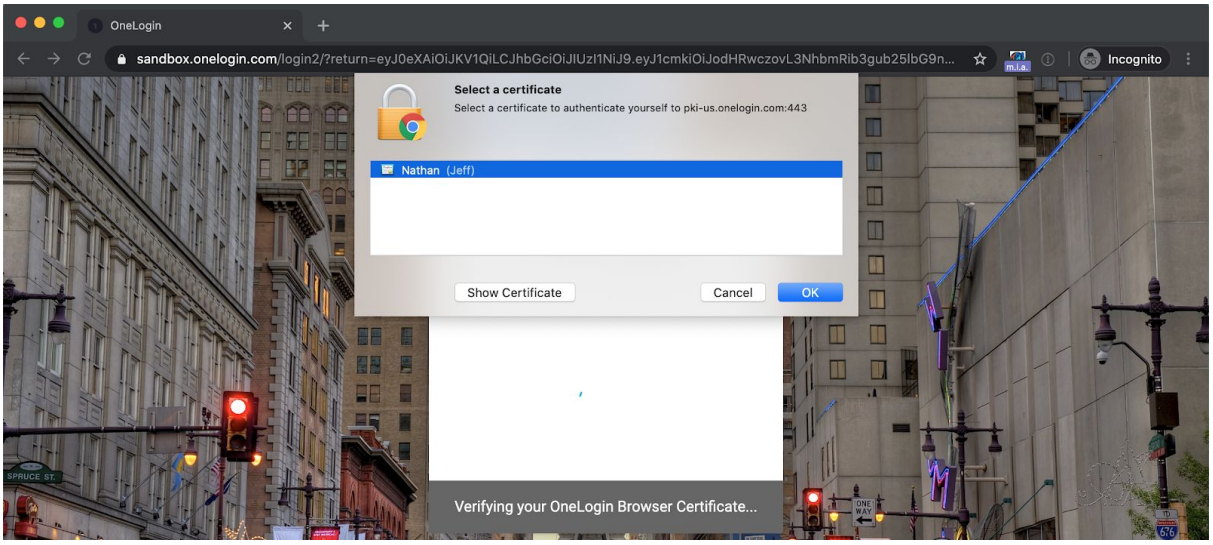


Assigning a Policy to a User

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



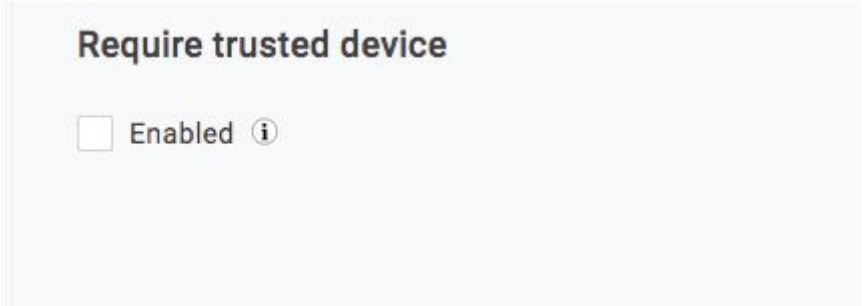
4. Test the certificate policy by logging in as the user. OneLogin will prompt the user for the certificate on log in



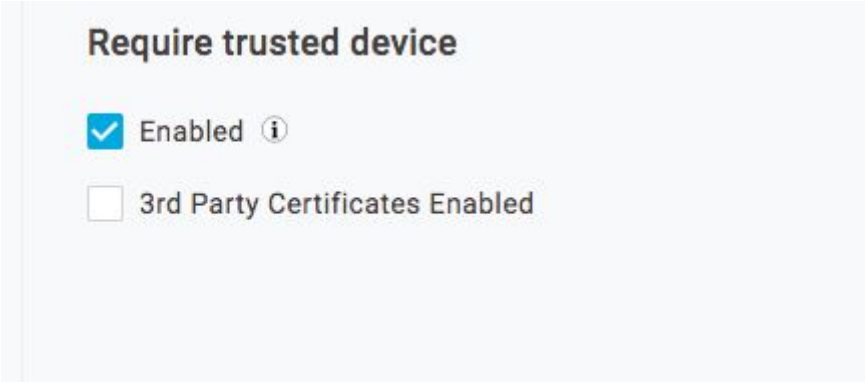
Application Policy Configuration

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

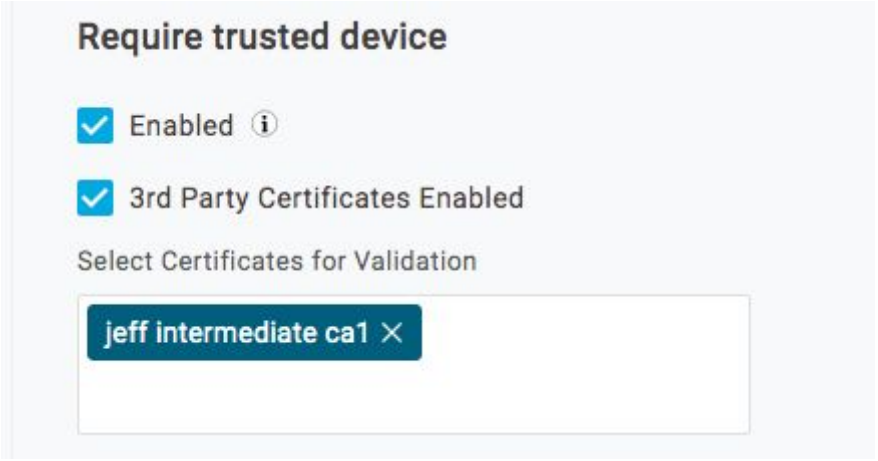
1. As a OneLogin Administrator, navigate to Administration → Security → Policies
2. Create or modify an existing App Policy
3. In the policy, navigate to Require trusted device
4. Check the box to enable trusted device



5. Check the box to enable 3rd Party Certificates

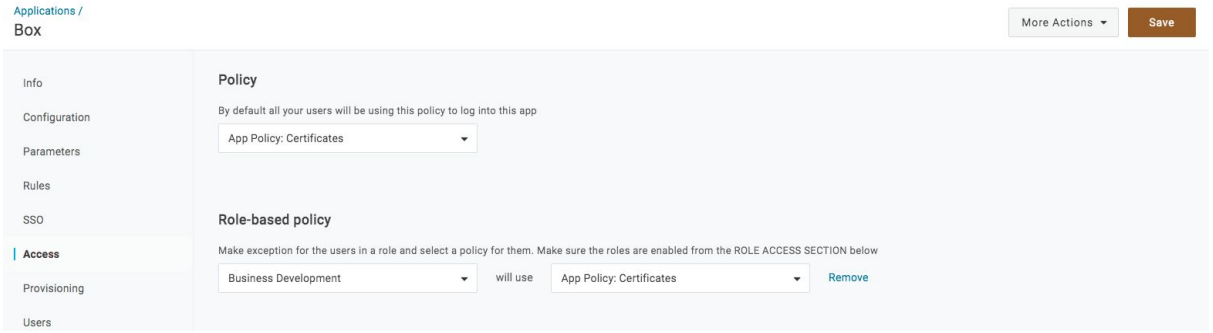


6. Select the certificate(s) for validation under this policy



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



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 with any questions or partners@onelogin.com