Advanced integrations with Okta: MobileIron

v1.1
August 2018

Okta Inc.

301 Brannan Street, 3rd Floor
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Table of Contents

What is this document **3**
What is Okta 3
What is MobileIron Core 3
What is MobileIron Cloud 3
What is MobileIron Access 3

Solving complex business problems **5**
General Considerations 6
Documentation of Services 6
User Provisioning and lifecycle management 6
Authentication Provider 7
Device authentication 7
Multi-factor authentication 7
Federation Provider 7
Device Trust 8
Okta 8
MobileIron Access 8

Use Cases **9**
Streamlined (simplified and secured) device enrollment 9
Benefits 9
Limitations 9
Steps to Implement 10

Device Trust through network rules 10
Benefits 10
Limitations 10
Steps to Implement 11

Identity Provider Routing Rules 11
Benefits 11
Limitations 11
Steps to Implement 11

Device Trust 12
Benefits 12
Limitations 12
Steps to Implement 12

Mobile SSO 13
Benefits 13
Limitations 14
Steps to Implement 14

Federation Relationships 14
Okta as IdP to all applications (MobileIron Core, Cloud) 14
MobileIron Access as IdP to Okta 14

Configuration Guides 15
Okta as Federation Provider to MobileIron Core 15
MobileIron Core Config 16
Core Settings 16
Okta Config 18
Application Creation Wizard 18
Complete MobileIron Core Config 18
Bookmark creation 19

Okta as Federation Provider to MobileIron Cloud 20
MobileIron Cloud Config 21
Okta App Config 23
MobileIron Cloud Service Test 25
Bookmark creation 25

MobileIron Access for Okta 26
Prepare MobileIron Access 26
Prepare MobileIron Tunnel 26
Prepare App(s) to be Secured 27
Get MobileIron Access Signing Certificate 28
Add Identity Provider in Okta 28
Verify MobileIron Access Profile and Mapping Values 31
Add Identity Provider in MobileIron Access 35
Update MobileIron Access details in Okta 39
Configure Identity Provider Routing Rules in Okta 41
Verify Configuration 42

Network Zones and Sign on Policies in Okta 43

References 43

Sequence Diagrams 45
SP Initiated - User accessing SaaS application from a mobile device 46

What is this document

This document is intended for Okta sales engineers and partners looking to integrate Okta with MobileIron's UEM and Access products. This document will provide an in-depth review of the involved components and how they can be paired. When combined, Okta and MobileIron deliver security, streamlined enrollment and painless experience for the end-user.

What is Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to both secure and manage their extended enterprise, and transform their customers' experiences. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely adopt the technologies they need to fulfill their missions. Over 4,000 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio trust Okta to securely connect their people and technology.

What is MobileIron Core

The MobileIron Core UEM is an on-premise or hosted purpose-built mobile IT platform. It provides users with seamless access to the business processes and content they need on mobile devices of their choice while providing IT the ability to secure corporate data. With MobileIron Core, enterprises can effortlessly begin and progress on their journey towards mobility.

What is MobileIron Cloud

MobileIron Cloud provides users seamless access to business apps and data through secure mobile devices and cloud services. IT benefits from advanced mobile and cloud security capabilities such as posture-based access control and selective wipe to prevent business data from falling into the wrong hands. By providing a robust Mobile and Cloud security solution that supports both business productivity and IT security requirements, MobileIron enables today's enterprises to become truly Mobile and Cloud first.

What is MobileIron Access

MobileIron Access is a cloud security solution for organizations deploying services such as Office 365, Salesforce, Box, and G Suite. Access provides multi-factor authentication (MFA), single sign-on (SSO), and a risk-based policy engine to enforce security for the mobile-cloud world. Access works in conjunction with MobileIron UEM solutions to evaluate device and application trust as part of conditional access policies.

Solving complex business problems

Customers can achieve increased value and satisfy unique use cases when leveraging the varied strengths of different technologies they have invested in. In many cases the sum value of the integrated parts is greater than the individual technologies could deliver on their own.

The strength of this integration is the ability to take full advantage of capabilities provided by both companies, MobileIron as the platform capable of robust Unified Endpoint Management and Okta as the best in breed Cloud first Identity and Access management service, providing Single Sign-on, Multi-Factor Authentication and Lifecycle Management to a ever growing catalog of applications in the Okta Integration Network (OIN) including SaaS and On-Premises applications.

When appropriately configured, the seemingly small integrations grow into full interOp stories that help organizations solve complex business problems. The breadth of which span from security enhancements to simplified architecture.

Prevent Data Breaches and Unauthorized access with AMFA

Integrate Okta's Adaptive MFA into the management of your MobileIron environment to provide the security your company requires for your privileged accounts. You can also extend this coverage to end users ensuring that device enrollment and application access tightly controlled.

Enforce device compliance as a requirement to access applications and services
Corporate Owned/Issued and BYOD are equally compliant at the end of the day.

With MobileIron enforcing device compliance and informing Okta, you can rest assured that your applications -- in the public or private cloud -- are being accessed only by devices that met the compliance criteria you enforce.

General Considerations

Throughout this document and within the referenced configuration guides there are common capabilities and constraints. Use this section as a primer or a reference to provide additional context.

Documentation of Services

Before attempting to architect or engage Access, it is imperative that existing authentication flow and Okta services (SSO, Provisioning, etc) be documented. Ensure that documentation includes a save of existing SP/IdP metadata and values used by each service such as GUID, UPN, Email Address or sAMAccountName, etc.

User Provisioning and lifecycle management

The concepts of user account provisioning aren't covered in depth in these articles but they play an important role.

Similar to Directory Alignment, user account provisioning is used to describe the process of creating accounts or directory entries for users in subordinate systems (Service Provider or Relying Party), usually SaaS applications.

User account provisioning can take place in a variety of ways including but not limited to:

- Manual creation
- Out of band batch sync
- JIT provisioning from federated assertions
- Real time provisioning through APIs

In some cases, it can include combinations of these and other methods.

While all data replicated to a target system should be considered important, there are certain attributes in federated authentication that are especially critical and must match. These attributes vary between systems but generally revolve around usernames and email addresses.

Authentication Provider

The authentication provider is the system responsible for verifying the claims made by an actor. In its most common form, this is the system that is going to verify the credentials (username and password) provided by users.

In this ecosystem, the concept of an authentication provider extends to include:

Device authentication

Usually accomplished through a device certificate that is issued and maintained by MobileIron UEM (Core or Cloud). The validity of a certificate is used to ascertain the compliance of a device against a configurable list of conformance items.

Multifactor authentication

Something I know, Something I have, Something I am. Okta supports the enrollment and validation of a varied range of factors. These factors offer different levels of authentication assurance to help meet the varying needs customers will face. Refer to Multifactor Authentication for more information.

Federation Provider

A federation provider is a system that asserts identity claims to systems to which trust has been established. This is generally accomplished through standards such as SAML and OIDC. In these standards the federation provider is the IdP or OP respectively.

Both Okta and Access are capable of being and IdP or OP.

Considerations such as account provisioning, user experience, system availability, infrastructure architecture may dictate that either party play the role of IdP.

One of the goals of this guide is to ensure that regardless of which system is the IdP, that the user experience, security and simplicity are maintained.

Device Trust

Devices are not users.
Users are not devices.
Applications running on devices are also not users but they act on behalf of them.
What does all of this mean and how do we reconcile it?

Device authentication was touched on briefly in the context of an authentication provider but the concept of device trust is different from the act of authenticating the device.

There are a variety of terms that are used -- often interchangeably -- to describe this, they include but are not limited to:

- Managed Device
- Trusted Device
- Known Device
- Enrolled Device
- Compliant Device
- Device Compliance
- Domain Joined

Regardless of the name, the concept of a trusted or managed device is dealt with in the following ways.

Okta

How does Okta establish device trust?
Satisfied through a variety of ways, Device trust is a condition of an access policy, like being on a specific network.

- https://help.okta.com/en/prev/Content/Topics/Mobile/device-trust.htm
- https://help.okta.com/en/prev/Content/Topics/Mobile/device-trust-mobile.htm

MobileIron Access

How does MobileIron Access establish device trust?
MobileIron Access has several feeds in terms of device trust, courtesy of the relationship it establishes with UEM services. However, in this context the primary driver for evaluation of trust on mobile devices stems from Core and Cloud. At its most basic form, trust is evaluated via the underlying device MDM relationship. Native agents then deliver a standard set of data based on posture of the device in question. This data (along with additional values received from MobileIron agentry) is used to calculate and assign the state of trust for said device.

Use Cases

We are talking about concepts here, the result of a specific configuration used to solve a business problem

To better illustrate solutions to the previously outlined business challenges, these overviews will walk through the high-level steps required to configure and the expected user experience. This is not intended to be an exhaustive list of use cases as there are numerous deviations a customer could make to meet their own unique requirements, rather this should provide enough detail of the different point integrations in the context of an overarching configuration to allow a customer to see the various possibilities.

From these stated use cases a reader may choose to take a similar approach to address their own unique challenges or adapt these use cases keeping the General Considerations in mind.

Streamlined (simplified and secured) device enrollment

Directing users to a familiar Okta login experience reduces training requirements for end users -- which also serves to combat phishing. Along with that it also provides opportunity to enforce adaptive MFA providing a higher level of assurance to your enrollment process, if device trust is an important factor controlling the process of enrollment is critical

The benefits of security and ease of use aren't limited to end users enrolling devices or managing enrolled devices. The same benefits of security and ease of use can be extended to your MobileIron administrators. Protecting privileged access to a critical system like MobileIron will further enhance your overall security posture.

Benefits

- Simplified user experience, increased user adoption
- Reduced IT burden, less training required
- Secure access to User and Admin portals, conditional

Limitations

- None

Steps to Implement

1	Configure Okta as Federation Provider to MobileIron Core	Configure Okta as the IdP for MobileIron Core
2	Configure Okta as Federation Provider to MobileIron Cloud	Configure Okta as the IdP for MobileIron Cloud

---

Device Trust through network rules

Device trust through network rules, MobileIron tunnel pushed from Core/Cloud along with app policies to route Okta bound traffic through tunnel, Okta policies applied for Sign-on or application level policies to restrict access to applications from untrusted devices (inferred by source of net traffic) This is also a continuous auth story.

A customer with Okta and MobileIron deployed may choose to deploy this configuration to help reduce the surface area of attack and increase the security posture of at-risk applications.

In this example an administrator would deploy App tunneling and per-app VPN policies using MobileIron and then setup application sign on policies in Okta to restrict access from unknown networks to targeted or all applications in Okta.

This is a dynamic extension of the “on network” concept that many organizations leverage but comes with additional benefits. The VPN connection is authenticated with a certificate that is issued to the device by MobileIron, in the case of MobileIron Tunnel the successful connection to the VPN is also contingent on the device being in a compliant state. If you have required MFA for users to enroll a device in MobileIron, You’ll have a high degree of certainty of the user and device identity as well as the security posture of the device.

Benefits

- Allows only machines on trusted source networks to access services
- Ensures services are accessed from only managed/trusted mobile devices
- Per-App VPN permits access to services only from managed apps on compliant devices
- MFA can be triggered if attempt to access is made from unknown network

Limitations

- If machine is not on trusted network (or without VPN), service may be inaccessible (based on policy configuration)

Steps to Implement

1	Configure App Tunneling and Per-App VPN Profiles in MobileIron Core/Cloud for iOS Devices	Configure and assign to target iOS devices
2	Configure Network Zones and Sign on Policies in Okta	Apply conditional access policies to restrict access or require multi factor authentication for users accessing applications from unknown network zones

---

Identity Provider Routing Rules

In situations where Okta and MobileIron Access are to co-exist, Identity provider routing rules (EA) make for the perfect compromise between owners of the two services. This allows for Okta to remain the primary point of contact for identity, with a rule that dynamically redirects mobile platforms/apps to Access. Below is a breakout of the benefits/limitations in this scenario and and steps that would be taken by a customer to implement this arrangement.

Benefits

- Highly configurable
- Retains Okta desktop SSO (IWA) capabilities
- Used to redirect Mobile to Access to engage SSO capabilities

Limitations

- Currently EA
- Allows for potential bypass of Okta device policy enforcement

Steps to Implement

1	Configure Access As an Identity Provider in Okta	Establish relationship with Access
2	Configure Okta Identity Provider Routing Rules	Route Specified Devices/Sessions to Access
3	Configure Conditional Access Policies in Access	Establish/Review Access Policies

Device Trust

As the amount of mobile devices deployed in enterprises continue to proliferate, so does the size of the attack surface for an organization and its data. To mitigate risk, trust of devices must be validated. Use of passwords must be eliminated. Fortunately, this is an area where Okta and MobileIron come through with a plan of attack.

In most situations, Okta is the first point of entry for authentication requests. That said, it is necessary that the system understand the state of trust for mobile devices from which requests originate. Trust is identified by Okta checking for the presence of Okta Mobile, which will validate whether said device is managed and trusted by the management platform (MobileIron Core/Cloud). If a managed instance of Okta Mobile is not found, trust validation effectively fails and the request is denied.

On the Access side, trust is determined by evaluating posture of the device via MDM relationship (e.g compliant with security policies/device encryption/data protection) and values reported by the MobileIron Agent (jailbroken). This state then dictates whether the device is allowed to continue participating in enterprise services, or if it is placed into quarantine. If placed in quarantine, managed profiles/ apps (including Okta Mobile) are removed. This effectively invalidates the trust of the device across the MobileIron and Okta landscapes.

Benefits

- Trust established using typical components, with no disruption in user experience
- Cross-platform evaluation, performed at time of auth request
- Loss of trust results in removal of enterprise apps/data and denial of auth request

Limitations

- Device management required

Steps to Implement

1	Configure Okta as Federation Provider to MobileIron Core	Configure Okta as IdP for Core
	Configure Okta as Federation Provider to MobileIron Cloud	Configure Okta as IdP for Cloud
2	Configure MobileIron UEM Compliance Core Policies / Cloud Policies	Validate device Trust
3	Configure Okta Device Trust for Mobile Devices	Engage Okta Device Trust

4	Initiate Enrollment of Devices to MobileIron UEM	Manage Devices with MobileIron

---

Mobile SSO

As a means to further secure the mobile login experience (and further drive ease-of-use), MobileIron Access includes SSO services for both iOS and Android mobile devices. Devices are enrolled, evaluated for trust and subsequently issued components that will automate the authentication process. Once redirected to MobileIron Access by Okta Identity Provider Routing Rules, SSO engages and attempts to authenticate on behalf of the user. Below, we will discuss at a high level the flow of authentication when SSO is engaged on the iOS and Android platforms.

iOS

Single Sign-On is achieved by use of MobileIron Tunnel, identity certificate and Access endpoint. When an SSO-enabled app attempts to access the Access URL, MobileIron Tunnel engages. MobileIron Access then extracts the identity of the user, validates trust of source device and (if trust is found) issues a SAML assertion. The managed app then utilizes the assertion to login the user.

Android

On Android, Single Sign-On is achieved by use of MobileIron Tunnel, identity certificate and Access endpoint. When an SSO-enabled app attempts to access the Access URL, MobileIron Tunnel engages. The identity certificate is offered-up. Access extracts the identity of the user, validates trust of source device and (if trust is found) issues a SAML assertion. The managed app then utilizes the assertion to login the user.

Benefits

- Automated SSO for iOS and Android devices
- Seamless login for user in SSO-enabled apps
- No disruption in user experience
- Apps/Access revoked immediately if device trust state changes

Limitations

- Device management required
- Android Enterprise recommended (legacy administrator is EOL 2019)

Steps to Implement

1	Okta + MobileIron Access	Integrate MobileIron Access with Okta

Federation Relationships

A large portion of this integration revolves around SAML federation relationships. In some flows you can have many federation relationships involved. This section is used to provide a high level description of the 4 distinct federation relationships that will be encountered and provide a quick summary of their purpose in this relationship.

Okta as IdP to all applications (MobileIron Core, Cloud)

This is the huge value of having Okta, the power of the OIN and simplicity of Okta acting as the IdP inclusive of account lifecycle management.

MobileIron Access as IdP to Okta

Incorporating MobileIron Access as IdP in conjunction with Okta IdP routing rules allows for a streamlined integration to provide device and application posture context as well as convenience features like Mobile SSO.

Configuration Guides

Step by Step instructions below, refer to Use Cases above for additional context

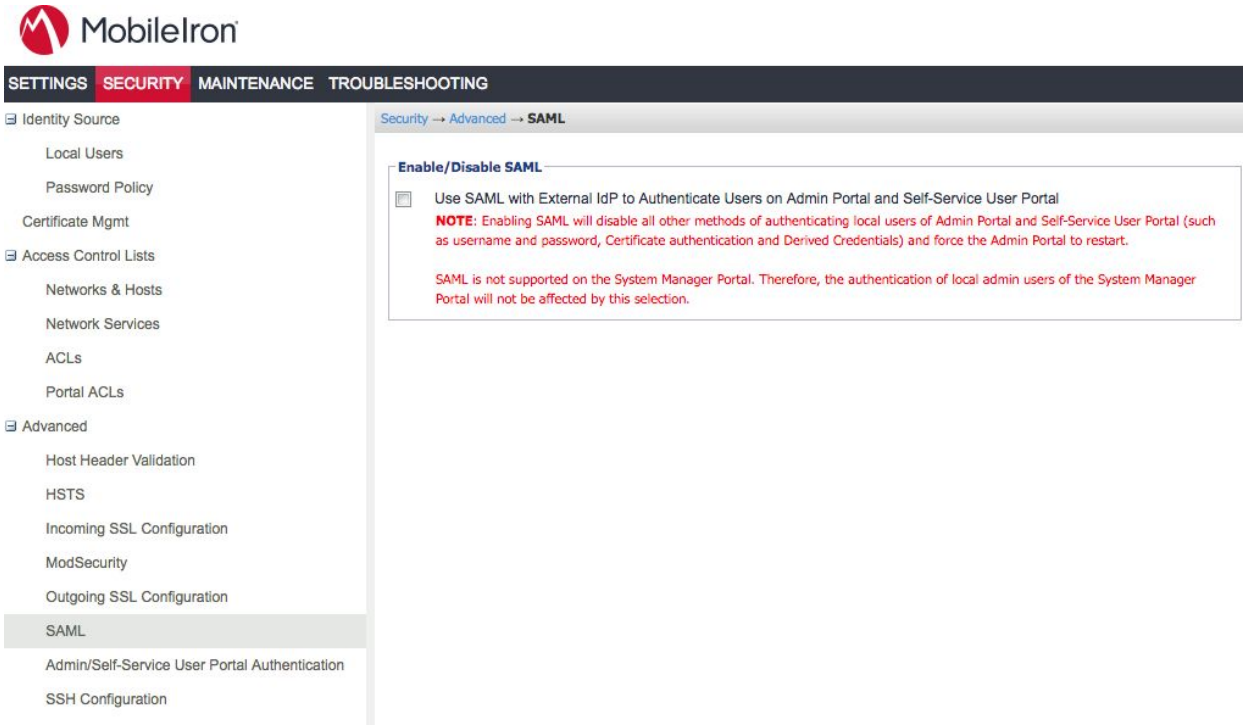
In the following sections we will provide an overview of the tactical configuration guides that are referenced in the Use Case Guides above. This will provide enough context for a reader to get the gist of the integration and will also include links to the appropriate guides.

Since many of these integrations are commonly used so rather than document them in multiple places they have been broken out into individual components and will be referenced above. This document will provide a high level overview of their contents, the detailed instructions are contained in an external link.

Okta as Federation Provider to MobileIron Core

This Guide describes the process of configuring MobileIron Core as a target application in Okta. This can be used to provide Single Sign on and Multi Factor Authentication into the Admin and User Self-Service Portals of MobileIron Core.

This step configures Okta as the IdP for your Users and potentially admins that use MobileIron Core. Make note of the User Name mapping defined for your users as it will impact the User Name defined in Okta. The values between Okta and MobileIron Core must align.

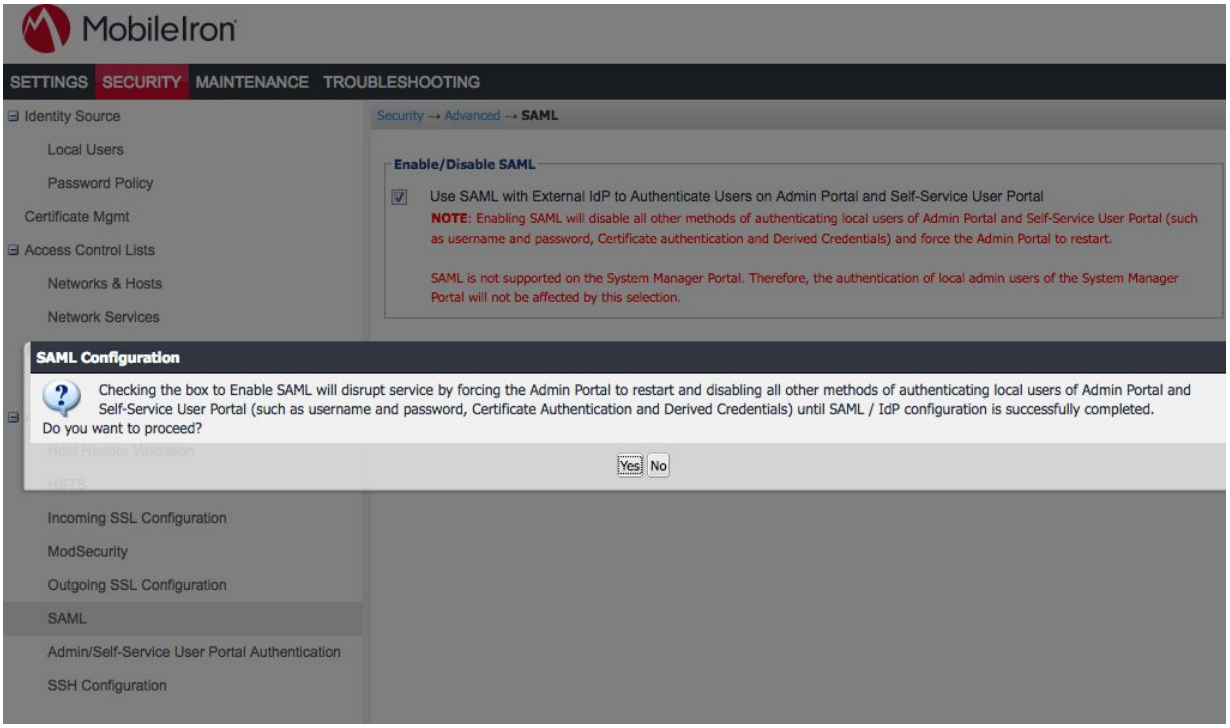


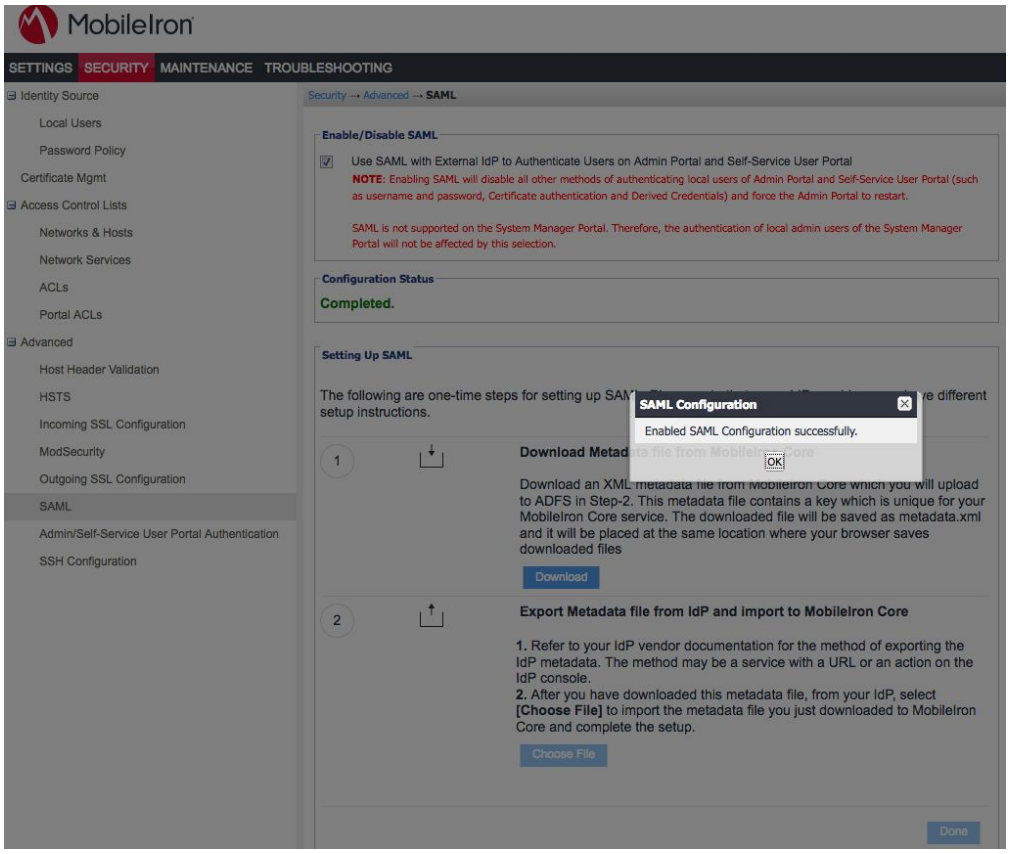
MobileIron Core Config

Login to the MobileIron Core MICS Console with Administrator privileges and prepare Core for use with Okta.

Core Settings

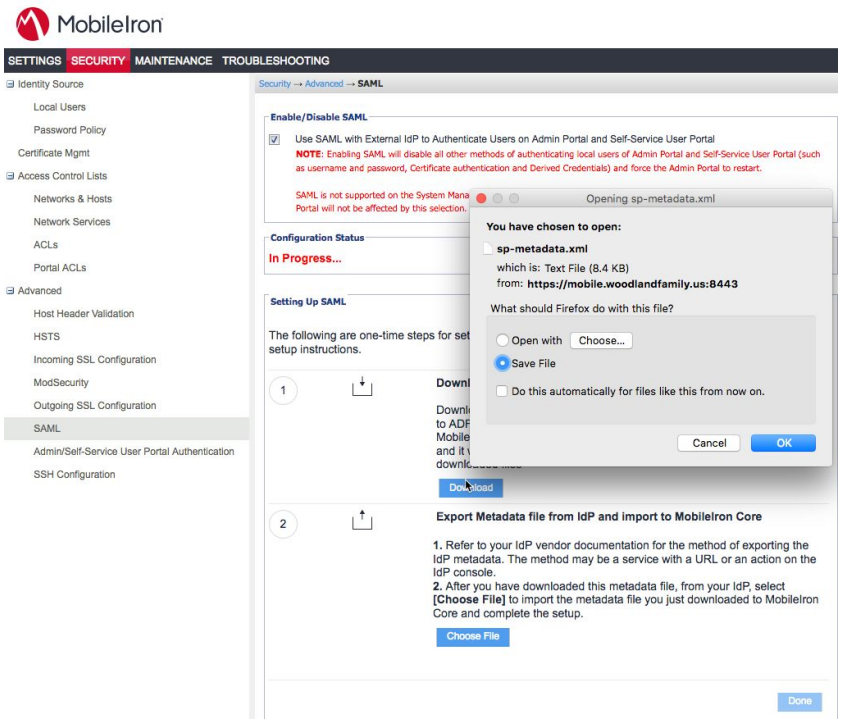
1. Log into System Manager Portal (https://Core.FQDN:8443)
2. Go to **Security** > **Advanced** > **SAML**
    a. Click the box to **Enable SAML**
    b. Read warning message
    c. Click **Yes** to restart Core services and turn on SAML
    d. This can take a few minutes
    e. The **Configuration Status changes** from **Restarting Tomcat**… to In Progress, followed by Completed





f. Click OK at the SAML configuration message

3. Click Download to download the XML metadata file from MobileIron Core
4. This action is taken to satisfy the wizard, but not needed for Okta integration



Okta Config

In this step we will add a new application in Okta for MobileIron Core. We will also create a bookmark apps used to trigger usages SP Initiated SAML flows like Admin Portal and User Device Management Portal.

Application Creation Wizard

1. Navigate to **Applications -> Applications**
2. Click **Add Application**
3. Search **MobileIron Core**

4. Click **Add**
5. Provide App Name
    a. **MobileIron Core**
6. Provide Core URL Details (https://Core.FQDN:443)
7. Leave ***Login URL*** **blank**
8. App Visibility
    a. Check Box - **Do not display application icon to users**
    b. Check Box - **Do not display application icon in the Okta Mobile app**
9. Click **Next**
10. Click the **View Setup Instructions** Button
11. Right-Click and download the **Identity Provider metadata**
    a. Save as metadata.xml
12. Assign MobileIron Core to Okta Users
13. Validate users entitled to app are assigned roles in MobileIron Core

Complete MobileIron Core Config

1. Log into **System Manager Portal** (https://Core.FQDN:8443)
2. Go to **Security** > **Advanced** > **SAML**
3. In Box 2, Provide the IDP Metadata that you saved in Step 9 above
4. In separate browser, access Core User or Admin Portal
    a. User Self-Service Portal - https://Core.FQDN
    b. Admin Portal - https://Core.FQDN/mifs
5. Observe redirect to Okta sign-in form
6. Provide test user credential
7. Observe hand-off and redirect to desired MobileIron portal
8. Verify MobileIron portal functionality as test user

Bookmark creation

Since the SAML flows for MobileIron are SP Initiated flows you'll need to create bookmarks to direct your users to those usage specific SP Initiated flows.

- End User Device Management: https://<hostname>
- Core Admin Login: https://<hostname>/mifs

Create sign on policies and apply them to the SAML app, assign the SAML app to the entire audience (admins and users)

Assign the bookmarks to the targeted audiences, admin bookmarks for admins only.

Okta as Federation Provider to MobileIron Cloud

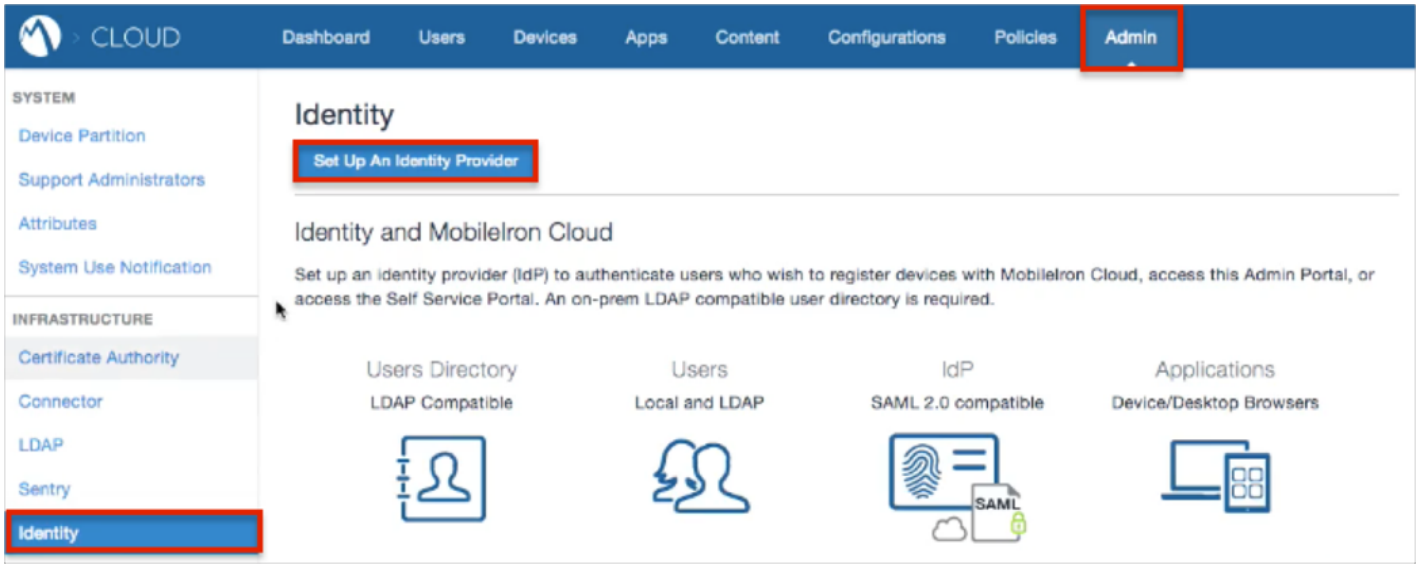
This Guide describes the process of configuring MobileIron Cloud as a target application in Okta. This can be used to provide Single Sign on and Multi Factor Authentication into the Enrollment, User Device Management as well as Administrative interfaces of MobileIron Cloud.

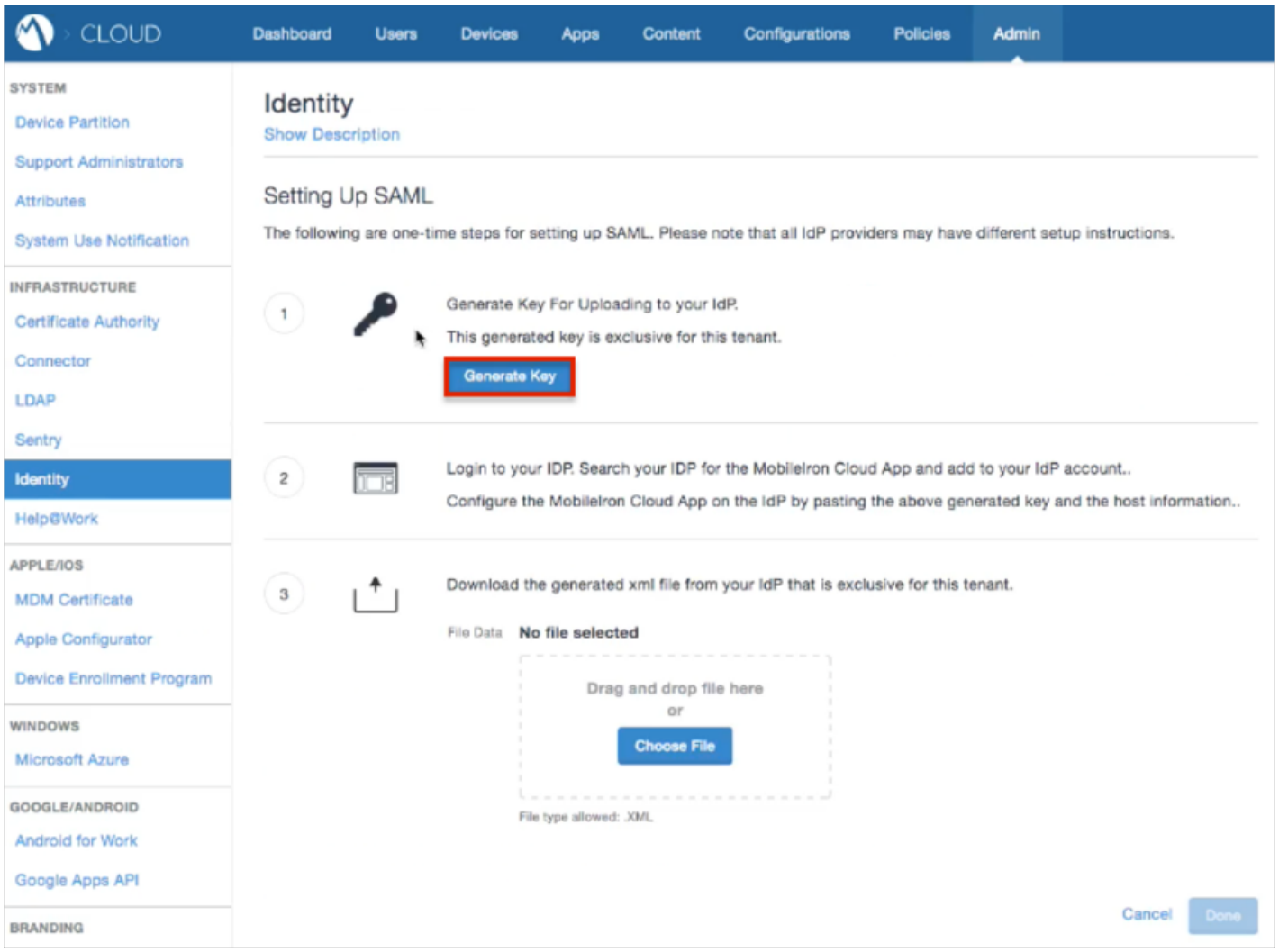
This step configures Okta as the IdP for your Users and potentially admins that use MobileIron. Make note of the User Name mapping defined for your users as it will impact the User Name defined in Okta. The values between Okta and MobileIron must align.

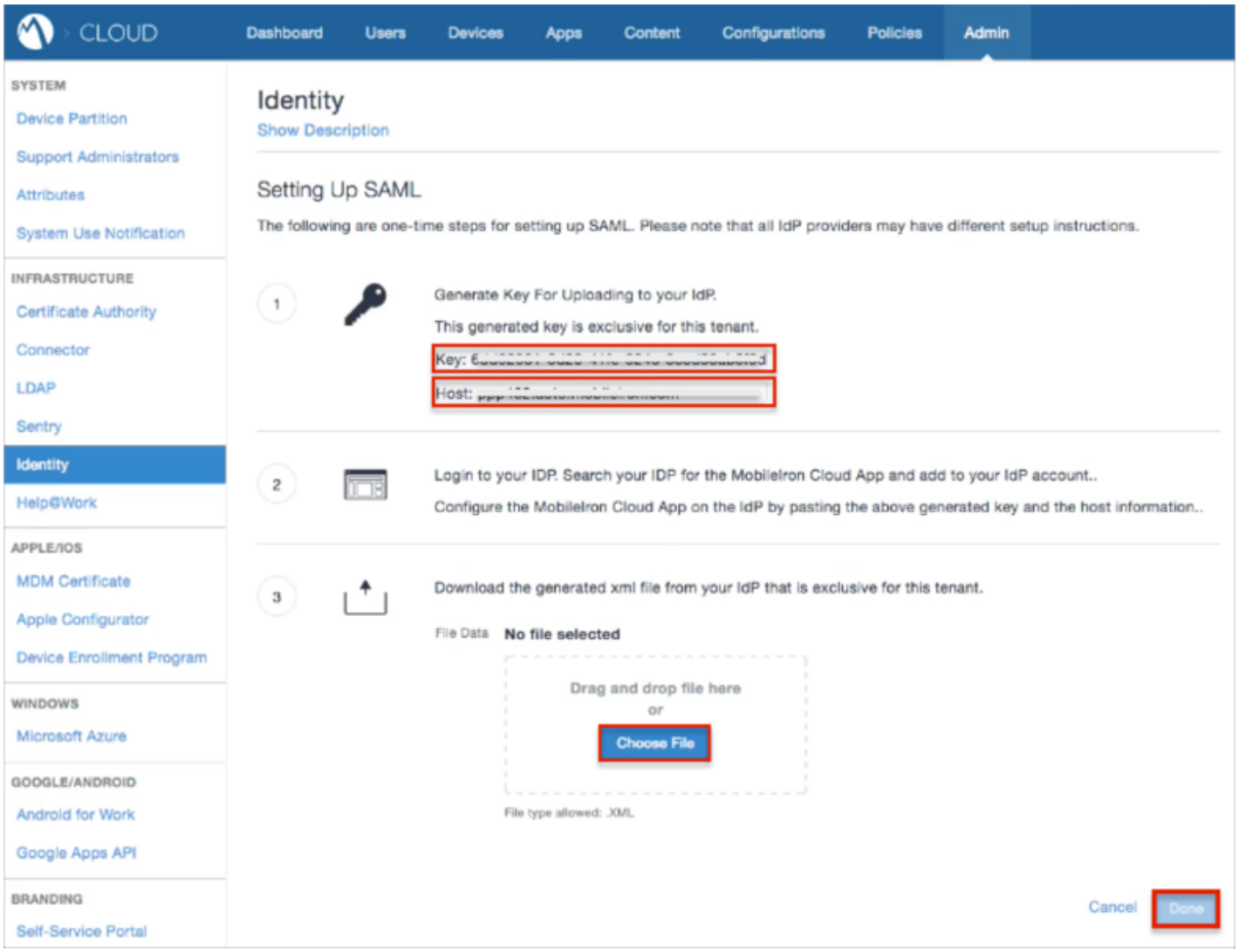
MobileIron Cloud Config

Login to the MobileIron Console with Console Administrator privileges or other role with the ability to edit the Directory Services page under System.

1. Login to MobileIron Cloud as an **administrator**.
2. Navigate to ***Admin > Identity***.
3. Click the ***Set Up An Identity Provider*** button
4. Select ***Okta*** from the drop-down menu
5. Click the ***Generate Key*** button:
6. **Make a copy** of the **Key and Host** values.



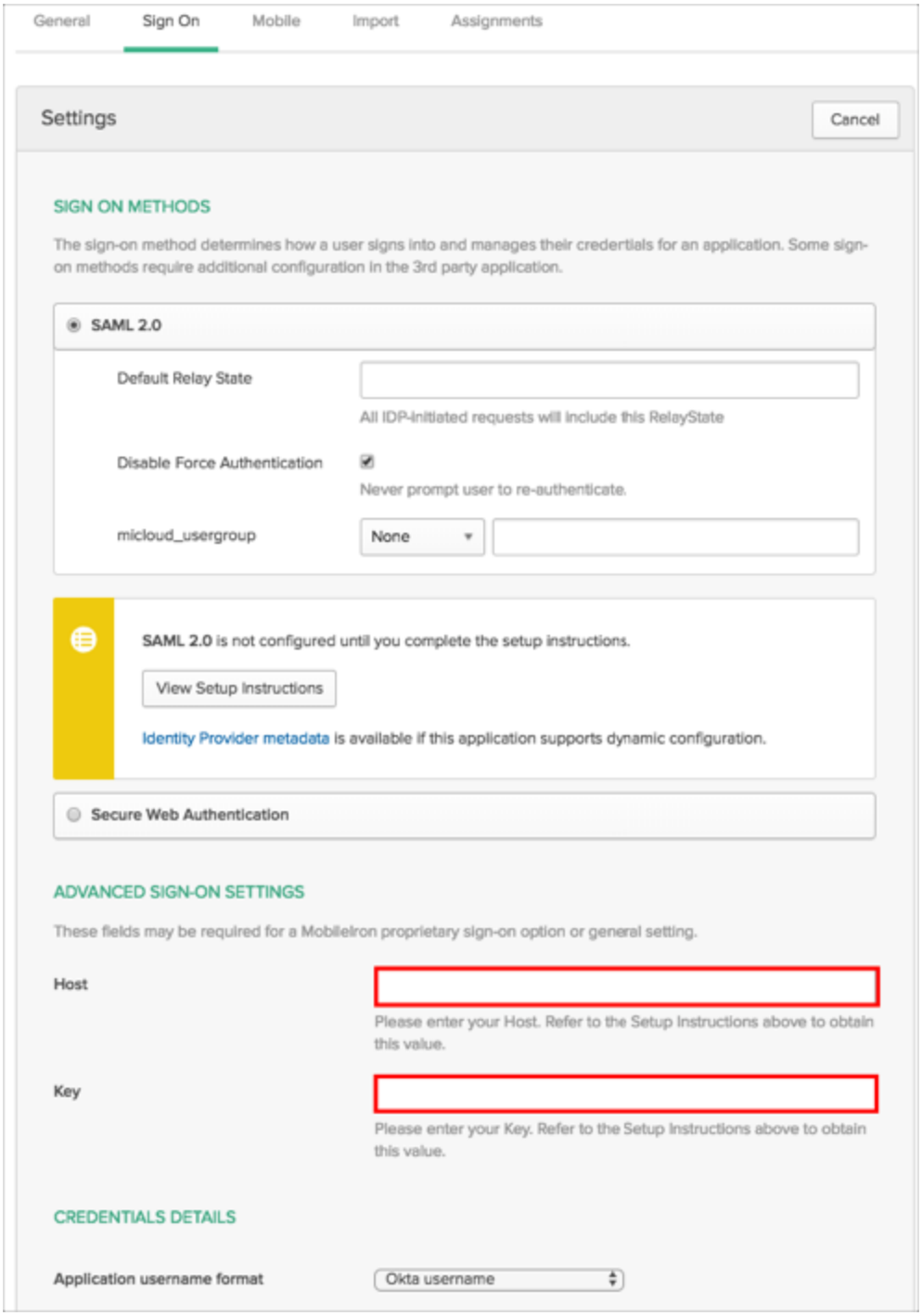

CLOUD
Dashboard
Users
Devices
Apps
Content
Configurations
Policies
Admin
SYSTEM
Device Partition
Support Administrators
Attributes
System Use Notification
INFRASTRUCTURE
Certificate Authority
Connector
LDAP
Sentry
Identity
Help@Work
APPLE/IOS
MDM Certificate
Apple Configurator
Device Enrollment Program
WINDOWS
Microsoft Azure
GOOGLE/ANDROID
Android for Work
Google Apps API
BRANDING
Identity
Show Description
Setting Up SAML
The following are one-time steps for setting up SAML. Please note that all IdP providers may have different setup instructions.
1
Generate Key For Uploading to your IdP.
This generated key is exclusive for this tenant.
Generate Key
2
Login to your IDP. Search your IDP for the MobileIron Cloud App and add to your IdP account..
Configure the MobileIron Cloud App on the IdP by pasting the above generated key and the host information..
3
Download the generated xml file from your IdP that is exclusive for this tenant.
File Data
No file selected
Drag and drop file here
or
Choose File
File type allowed: .XML
Cancel
Done



Okta App Config

1. Open a new browser tab
2. Log-in to the Okta Dashboard
    a. https://companyname-admin.okta.com/admin/dashboard
    b. Go to **Applications** menu
    c. Click **Add Application** —> **Create New App**
    d. **Search** and add ***MobileIron Cloud***
    e. Leave ***Login URL*** **blank**
    f. App Visibility
        i. Check Box - **Do not display application icon to users**
        ii. Check Box - **Do not display application icon in the Okta Mobile app**
    g. Click ***Next***
    h. At Bottom of Sign-On Options, **provide *Key/Host values from step 6***
    i. Click ***Done***
3. Under Sign-On, Click **Identity Provider Metadata**

4. Okta Metadata will download to your default folder as *metadata*
5. Locate file named metadata and rename to *Okta-MICloud-metadata.xml*
    a. Ensure the XML extension is added
6. Inside MobileIron Cloud browser tab, upload *Okta-MICloud-metadata.xml*
7. Click Assignments menu and assign MobileIron Cloud to test user(s)



MobileIron Cloud Service Test

1. In separate browser, access any of the MobileIron Cloud portals
    a. Device Enrollment - https://mobileiron.com/go
    b. User Self-Service Portal - https://mydevices.mobileiron.com
    c. Admin Portal - https://login.mobileiron.com
2. Provide User ID (Email Address)
3. Observe redirect to Okta sign-in form
4. Provide test user credential
5. Observe hand-off and redirect to desired MobileIron portal
6. Verify MobileIron portal functionality as test user

Bookmark creation

Since the SAML flows for MobileIron are SP Initiated flows you'll need to create bookmarks to direct your users to those usage specific SP Initiated flows.

- End User Device Management: https://mydevices.mobileiron.com
- End User Device Enrollment: https://mobileiron.com/go
- Cloud Admin Login: https://login.mobileiron.com

Create sign on policies and apply them to the SAML app, assign the SAML app to the entire audience (admins and users)

MobileIron Access for Okta

This section describes the process of joining forces between MobileIron Access with Okta products. When configured, this will allow Okta to hand-off mobile authentication requests to MobileIron. Access and the UEM platform can then assess the posture of the device and decide whether the request should be approved or denied. If approved, Mobile SSO (passwordless authentication) initiates and leads the user into the app. If denied, custom verbiage may be displayed per the company's policy such as detail as to why the device was denied or a link to allow a user to formally enroll in the BYOD program.

Prepare MobileIron Access

MobileIron Access (On-Premise via Sentry or Cloud-Hosted) should be initialized before proceeding through this guide. Please refer to the Access implementation guide in order to ready your services:

https://community.mobileiron.com/docs/DOC-4417

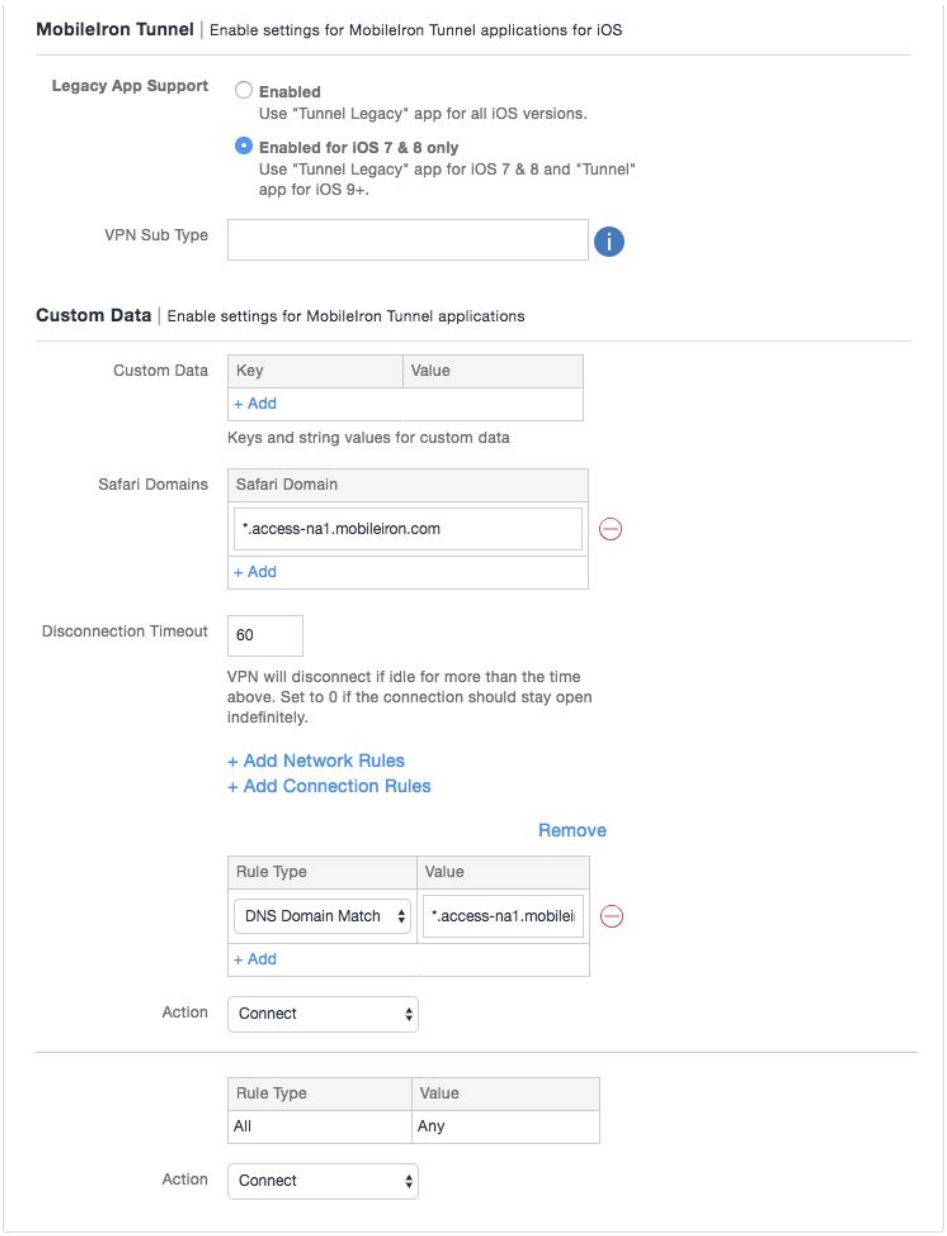
Prepare MobileIron Tunnel

Rather than re-document, this guide will make partial reference to MobileIron materials on the subject. Base configuration guides can be found at:

MobileIron Tunnel on iOS for Core and Cloud: https://community.mobileiron.com/docs/DOC-8202
MobileIron Tunnel on Android for Core and Cloud: https://community.mobileiron.com/docs/DOC-7691

In order to route Access traffic through Tunnel, utilize the Access implementation guide, located at: https://community.mobileiron.com/docs/DOC-4417

Once implemented, Tunnel configuration for Access should look similar to the visual below:



Prepare App(s) to be Secured

To ensure successful testing at the end of this guide, we recommend creating an application in your Okta tenant that will ultimately be secured and seamlessly signed-in using MobileIron Access. While the specific steps are not listed here, references are provided to several types of documentation to assist in adding your app for use.

Interested in what applications Okta has existing integrations? Please see the App Search feature of our website. If your application does not yet have a formal integration, use the App Integration Wizard. Several examples of how to add an existing app can be found below:

Salesforce

Workday

ServiceNow

Get MobileIron Access Signing Certificate

In this section we will retrieve information required by Okta to begin setup an Identity Provider (IdP).

Login to the MobileIron Access Administration Console with Administrator privileges.

1. Click the **Profile → Access Certificates**
2. Click **Download** on the primary signing certificate
3. Note location of downloaded PEM file for use in the next section

Add Identity Provider in Okta

In this section we will create the Identity Provider (IdP) record in Okta

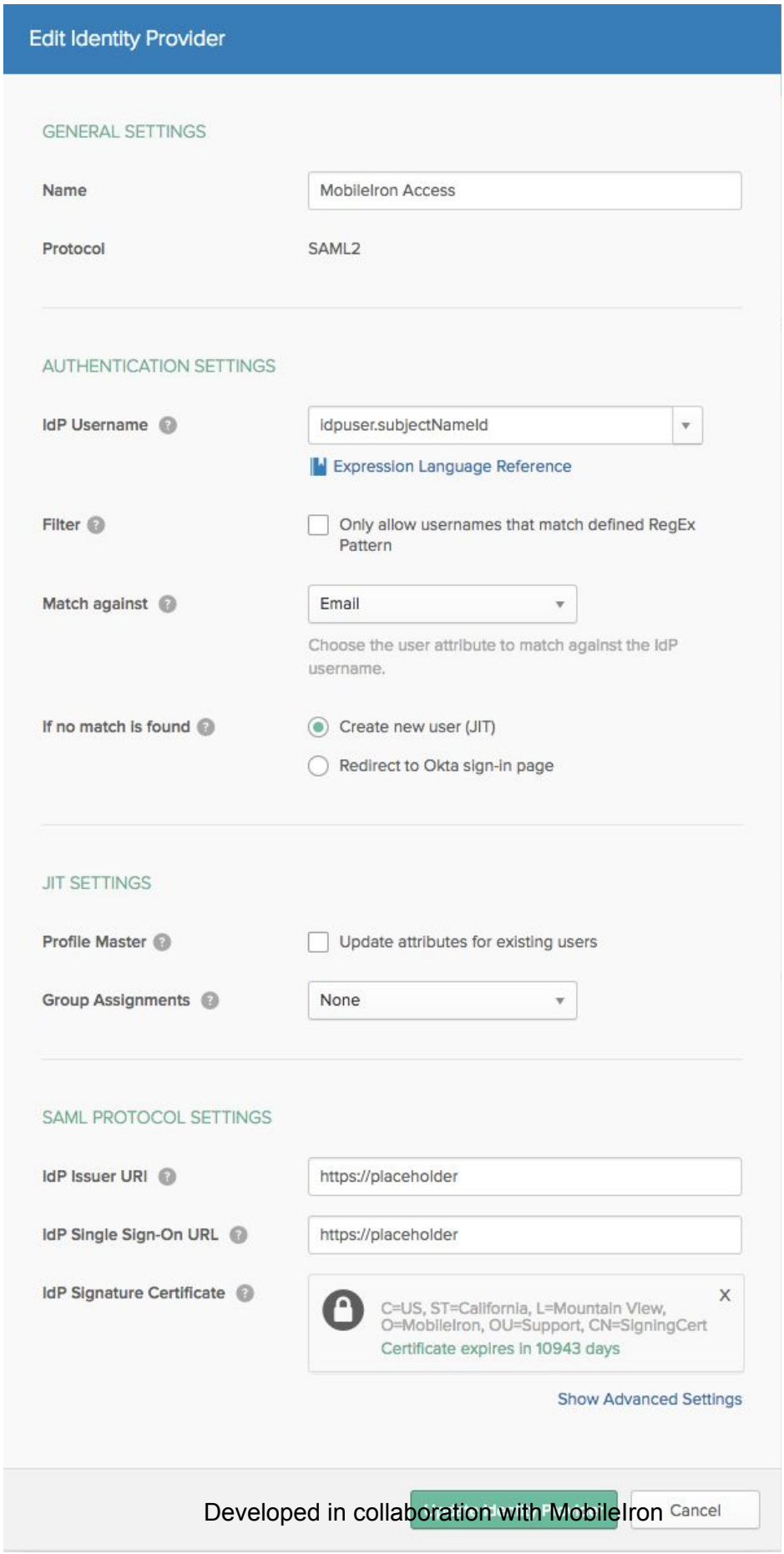
Login to the Okta admin UI with Administrator privileges or any other role entitled to add an Identity Provider.

For additional information about how Okta deals with external identity providers review our product help guide on Identity Providers

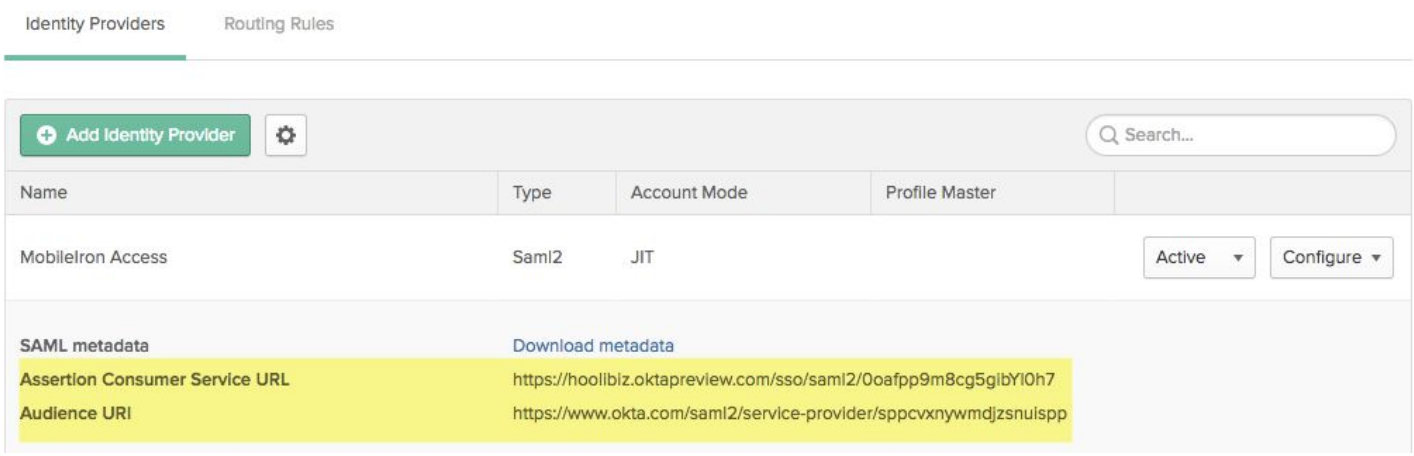
1. Navigate to **Security -> Identity Providers**
2. Click **Add Identity Provider**
3. Provide a Name: ***MobileIron Access***
4. IdP Username: ***idpuser.subjectNameId***
    a. Filter: ***Unchecked***
5. Match Against: ***Email Address***
    a. Refer to the Directory Alignment chapter for information
6. If no match is found: ***Create new user (JIT)***
7. IdP Issuer URI: Enter a temporary value
        i. We will update after creating the Access config in later steps
8. IdP Single Sign-On URL: Enter a temporary value

i. We will update after creating the Access config in later steps

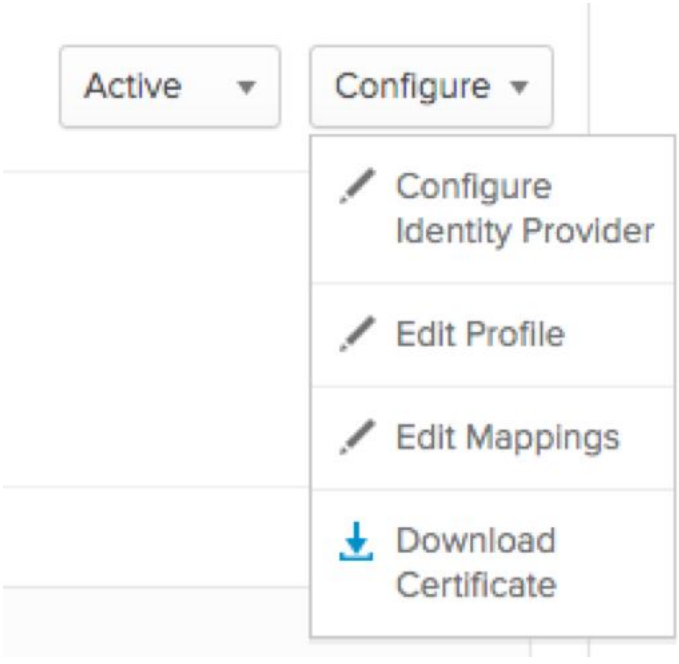
9. IdP Signature Certificate
    a. Browse and select the Signing Certificate from MobileIron Access
        i. *Hint: you may need to change the file extension or default browser filter looking for *.crt and *.pem files*
10. Click **Add Identity Provider**


Edit Identity Provider
GENERAL SETTINGS
Name
MobileIron Access
Protocol
SAML2
AUTHENTICATION SETTINGS
IdP Username
idpuser.subjectNameId
Expression Language Reference
Filter
Only allow usernames that match defined RegEx Pattern
Match against
Email
Choose the user attribute to match against the IdP username.
If no match is found
Create new user (JIT)
Redirect to Okta sign-in page
JIT SETTINGS
Profile Master
Update attributes for existing users
Group Assignments
None
SAML PROTOCOL SETTINGS
IdP Issuer URI
https://placeholder
IdP Single Sign-On URL
https://placeholder
IdP Signature Certificate
C=US, ST=California, L=Mountain View, O=MobileIron, OU=Support, CN=SigningCert
Certificate expires in 10943 days
Show Advanced Settings
Cancel

11. Observe the following
    a. Assertion Consumer Service URL
    b. Audience URI
12. Download the Okta SAML metadata



13. Download and save the certificate file
    a. Click the Configure button
    b. Select Download Certificate
    c. *Note the location of the Okta.cert file to be used during our next steps*



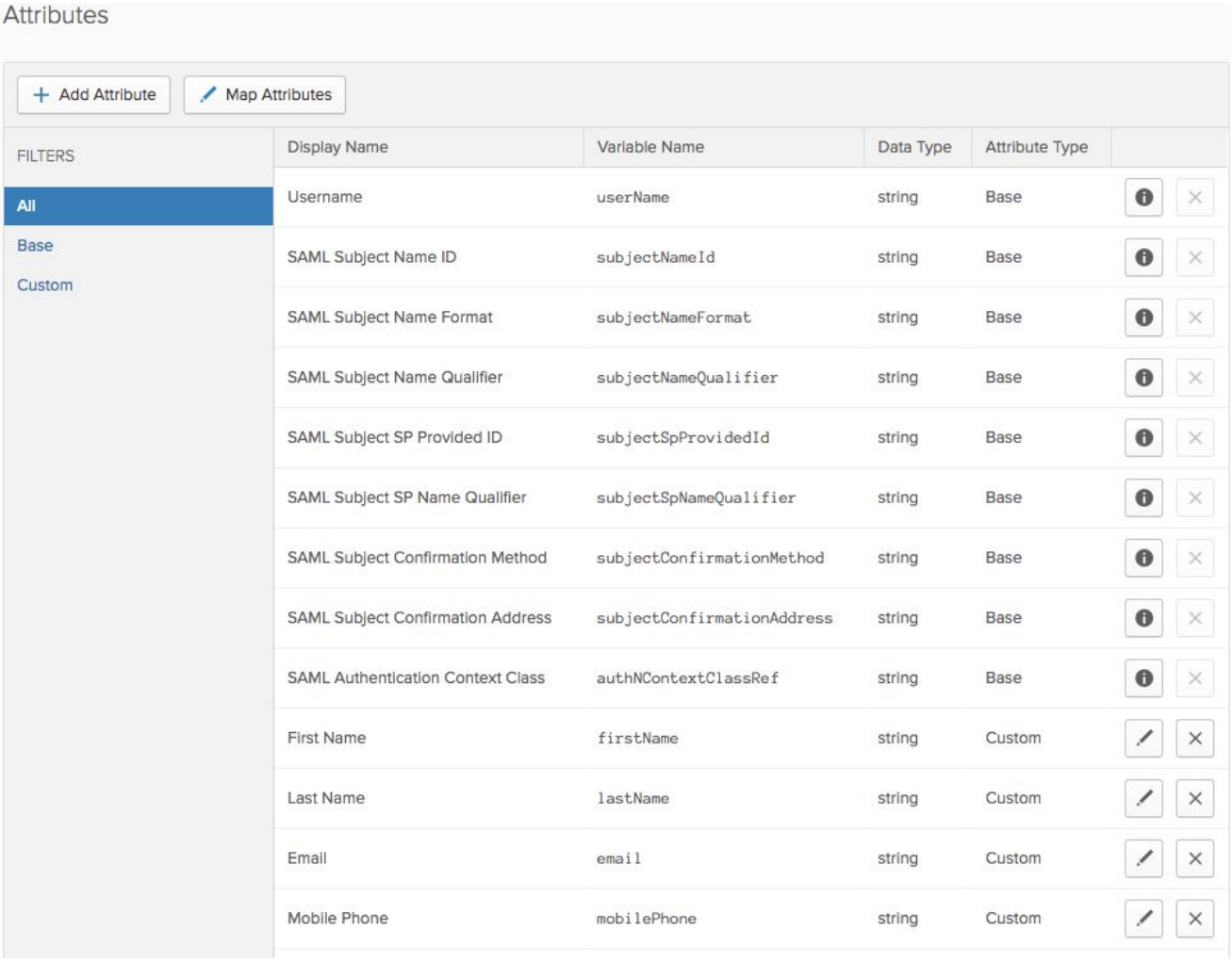
Verify MobileIron Access Profile and Mapping Values

In this section we will briefly review the Profile and Mappings of the MobileIron Access entry in Okta. No changes *should* be necessary, however it is important to review before proceeding.

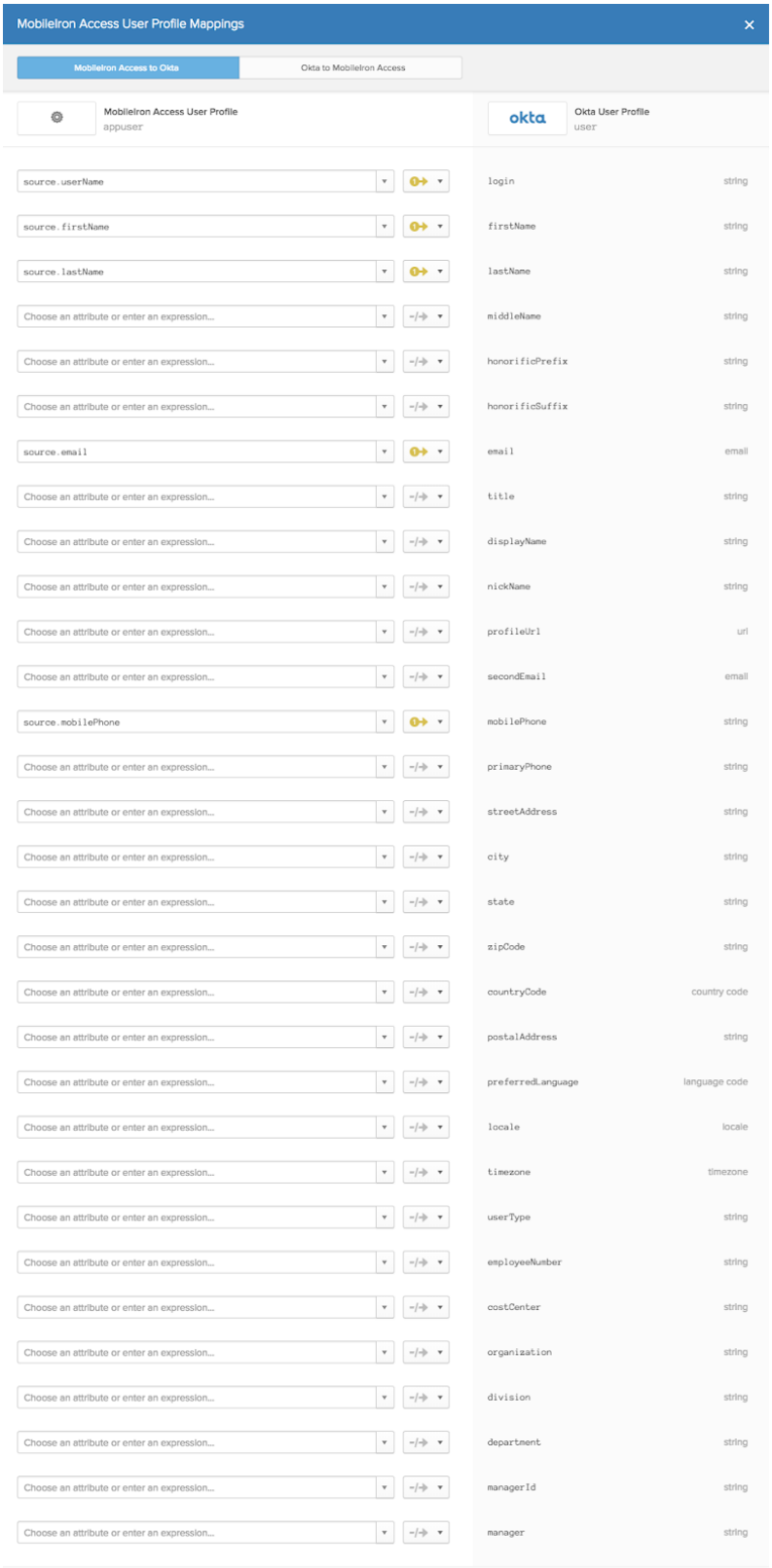
Login to the Okta admin UI with Administrator privileges.

1. Navigate to **Security -> Identity Providers**
2. Find the entry for **MobileIron Access**
3. Click the **Configure** drop-down and select Edit Profile / Edit Mappings
4. Review the two sections to ensure they match the mappings shown below:

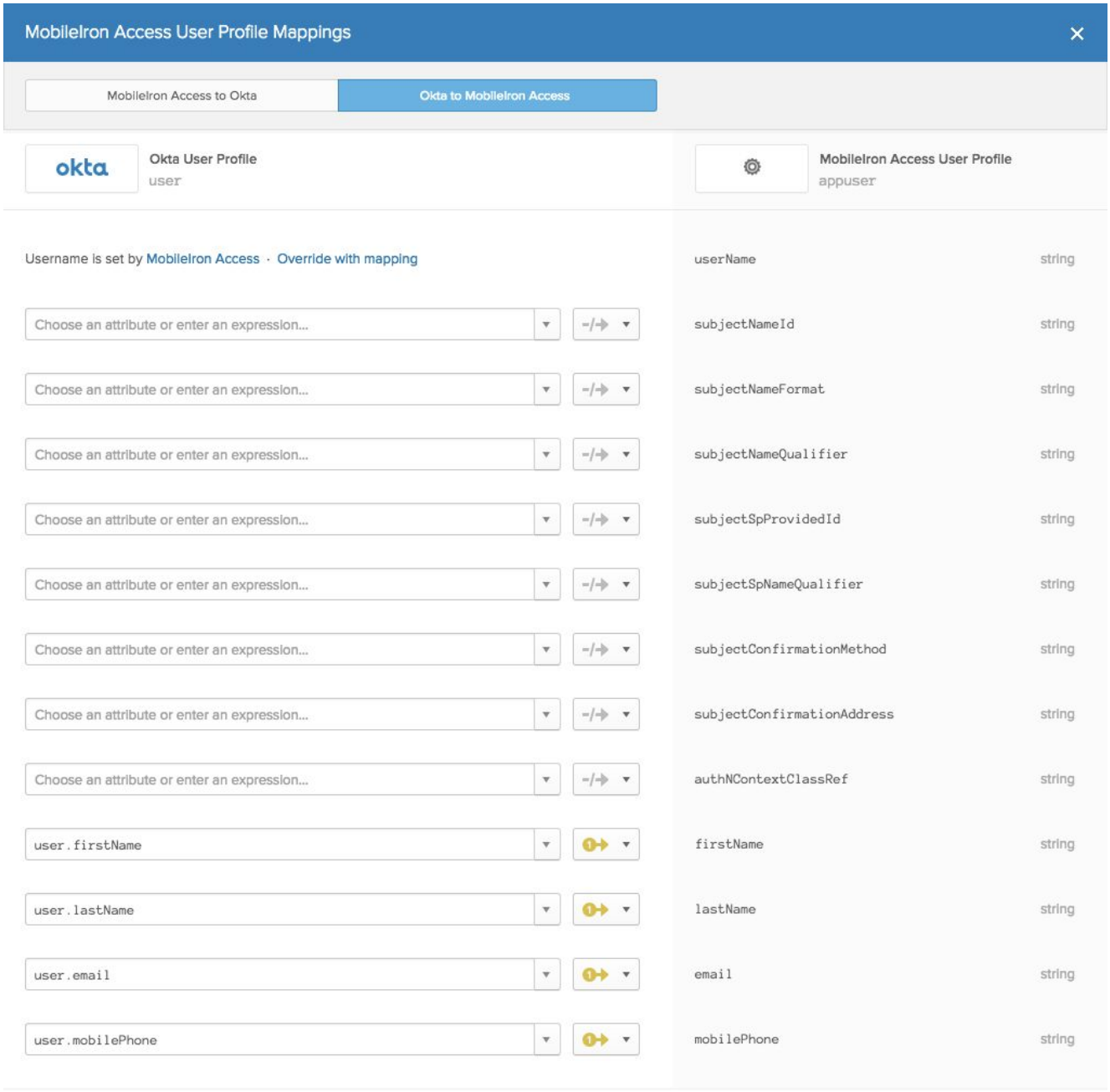
Profile:



Mappings: MobileIron Access to Okta



Mappings: Okta to MobileIron Access

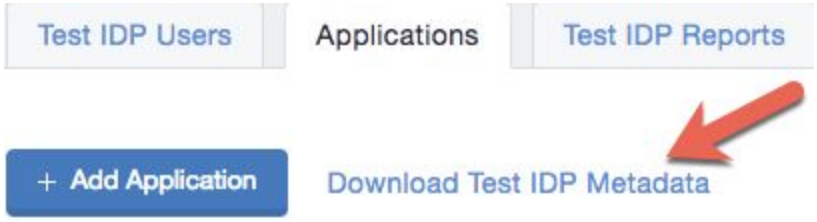


Add Identity Provider in MobileIron Access

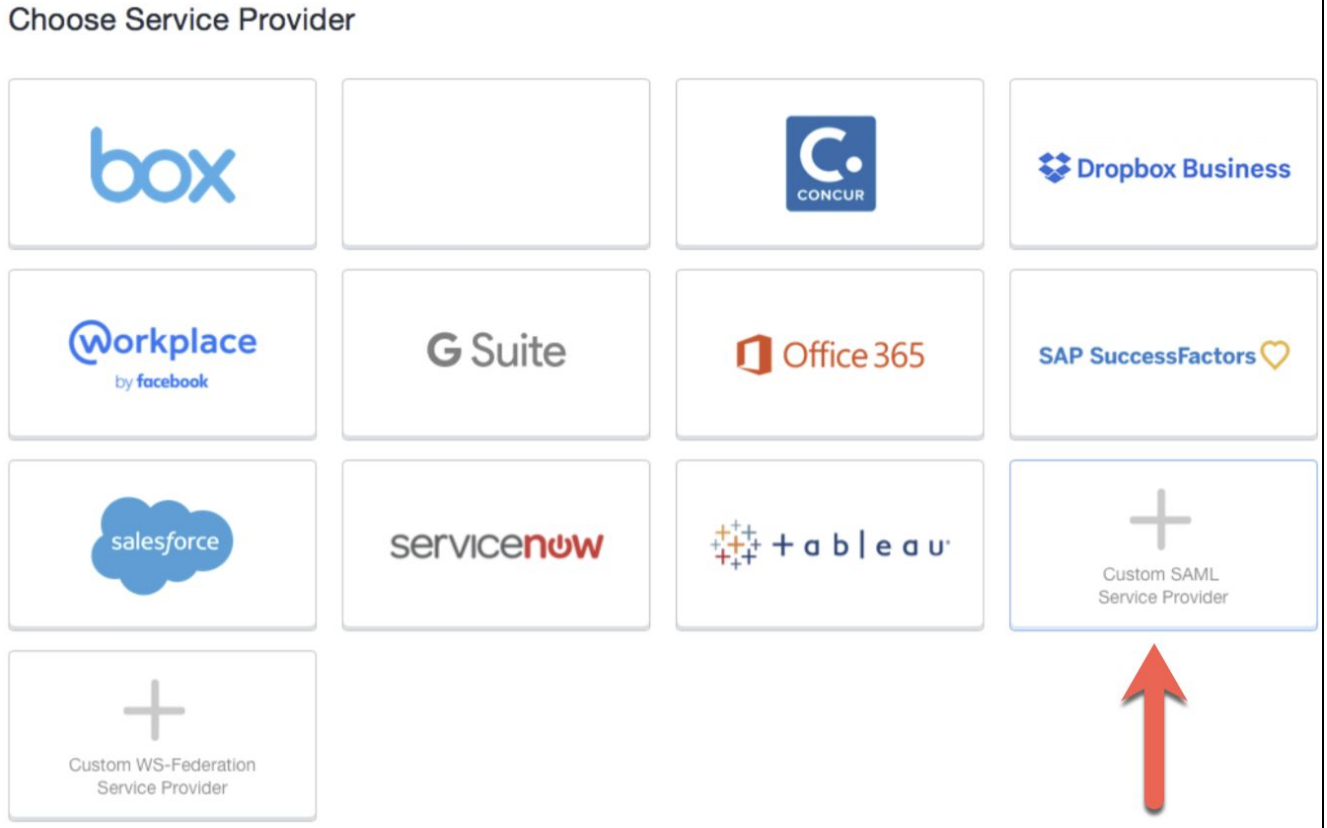
In this section we will create the Identity Provider (IdP) record for Okta in MobileIron Access. This assumes you have already performed a baseline configuration of your Access tenant (documentation found here).

Login to the MobileIron Access admin portal with Administrator privileges.

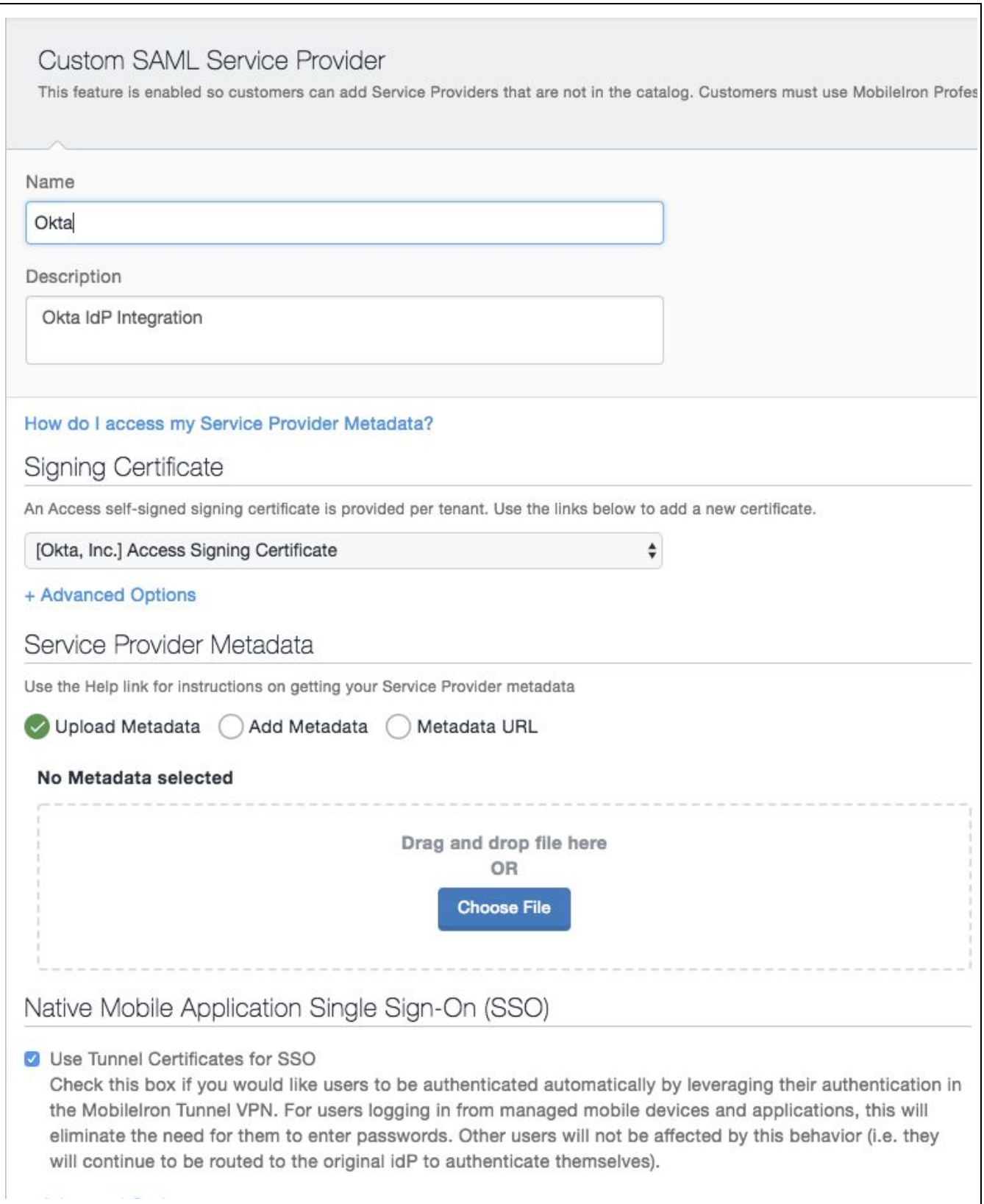
1. Navigate to **Settings → Test IDP → Applications** tab
2. Click **Download Test IDP Metadata**



3. Navigate to **Profiles >** click on **Federated Pairs**
4. Click on **+ADD**
5. Select **Custom SAML Service Provider**

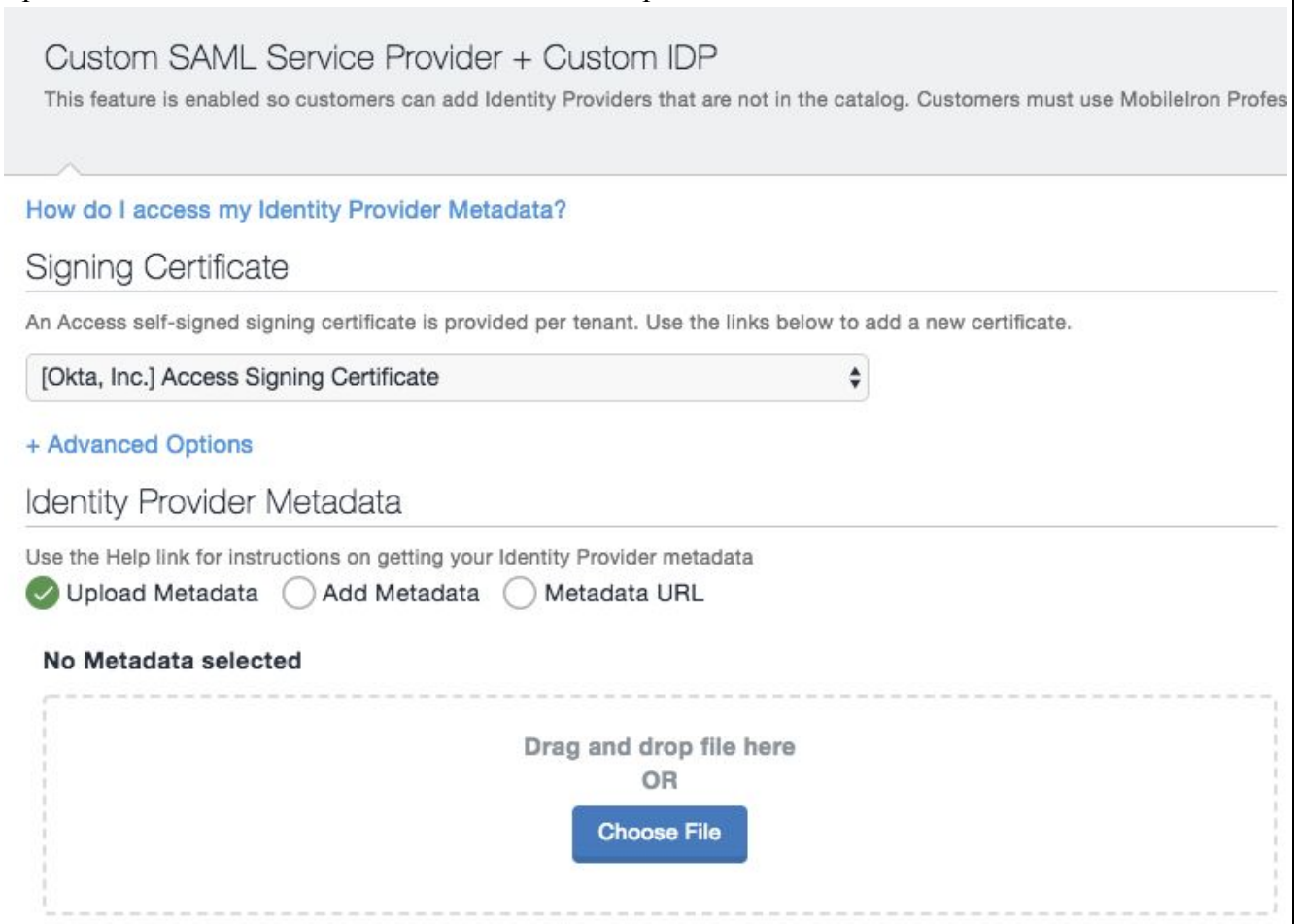


6. Enter Name: **Okta**
7. Enter Description: **Inbound SAML from Okta**
8. Choose **existing Signing Certificate** or **Upload SPProxy Certificate**
9. **Upload** the **Okta SAML metadata** downloaded in the previous section
10. Select **Use Tunnel Certificates for SSO** check box



11. Click **Next**
12. Choose **Custom Identity Provider** as Identity Provider
13. Use **existing Signing Certificate** or **Upload SPProxy Certificate**
14. Click **Next**

15. Upload **Access Test IDP Metadata** saved from Step 2



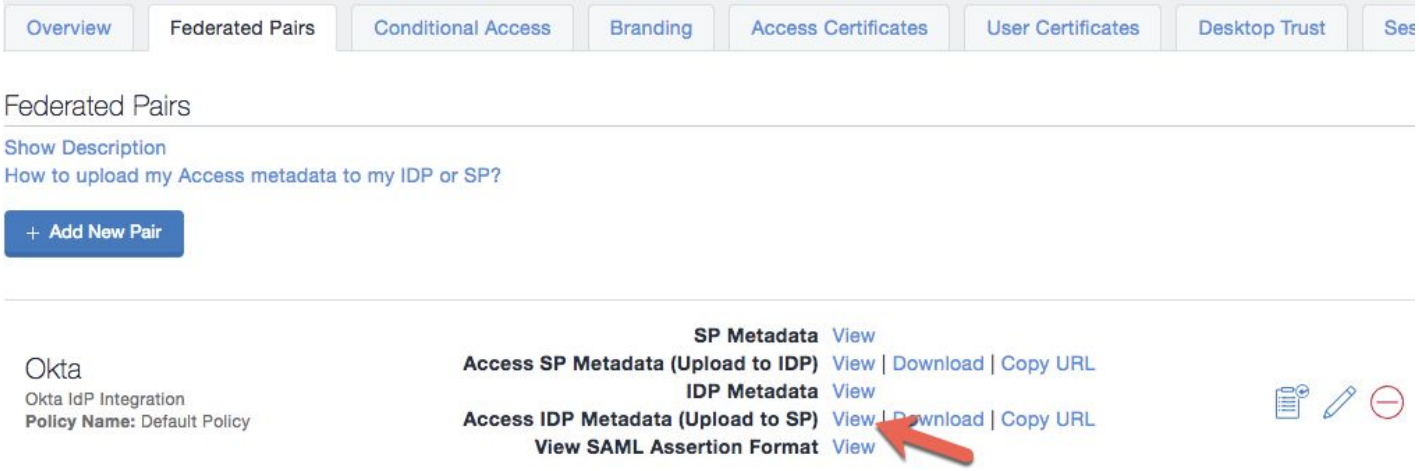
16. **Complete Wizard**
17. Publish Profile

Update MobileIron Access details in Okta

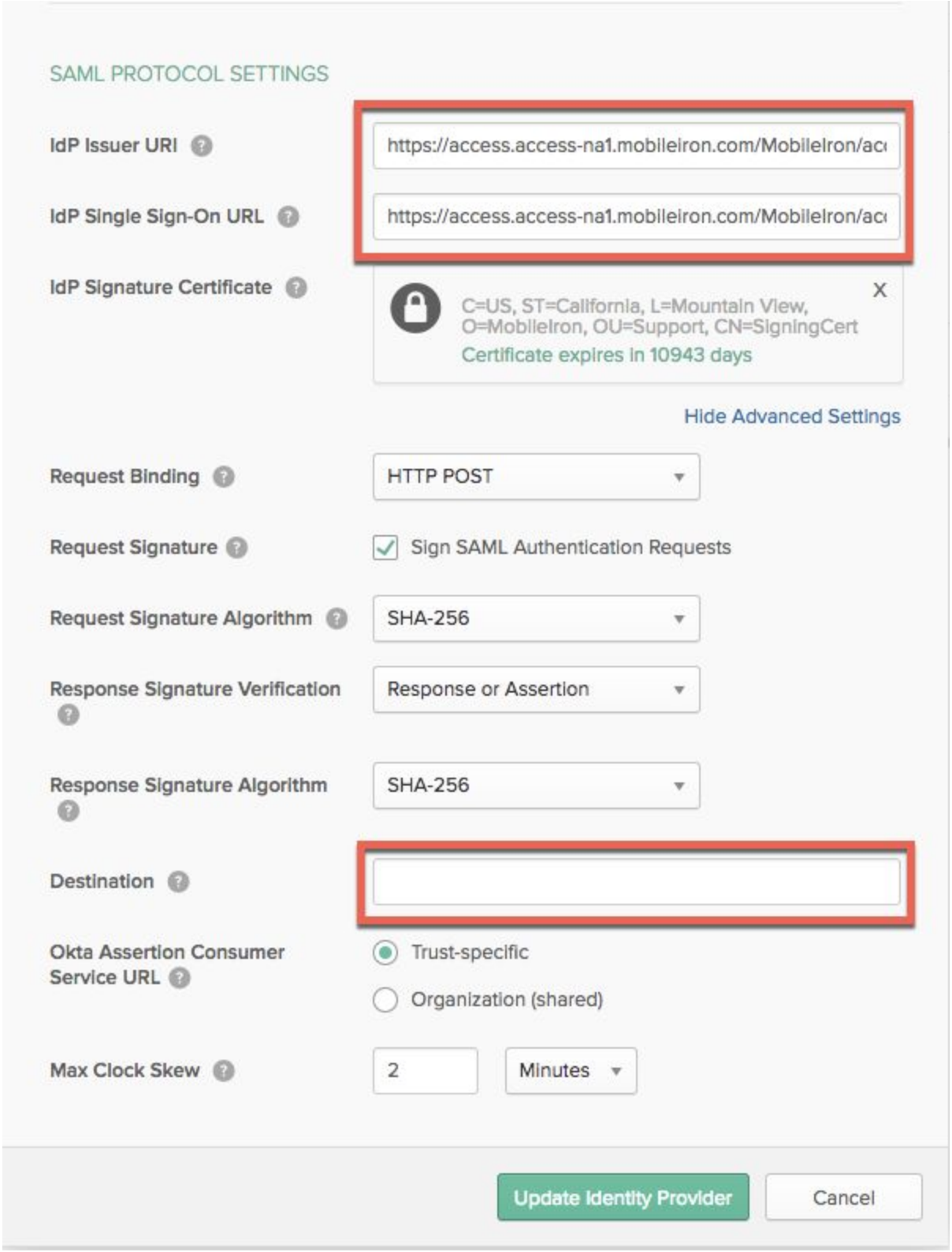
In this section we will update the Identity Provider (IdP) details for MobileIron Access in Okta.

Login to the MobileIron Access admin portal with Administrator privileges.

1. Navigate to **Profiles >** click on **Federated Pairs**
2. Locate the entry for **Okta**
3. View the file under the area named **Access IDP Metadata (Upload to SP)**



4. While viewing the metadata, **look to the bottom area for a section that contains** *SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"*.
5. Then **copy the URL** that follows (e.g https://access.access-na1.mobileiron.com/MobileIron/acc/ab7d46f1-283c-450a-8aa8-be233ded0d56/idp
6. **Login to the Okta admin UI with Administrator privileges** or any other role entitled to modify an Identity Provider.
7. Navigate to **Security -> Identity Providers**
8. **Configure Identity Provider** the **MobileIron Access** entry
9. **Update IdP Issuer URI** to value copied from Access IdP Metadata
10. **Update IdP Single Sign-On URL** to value copied from Access IdP Metadata
11. Under **Advanced settings**, clear-out the value for Destination.
    a. This will re-populate with the correct entries upon save



12. Click **Update Identity Provider**

Configure Identity Provider Routing Rules in Okta

This feature is currently EA and requires the IDP_DISCOVERY feature flag on your Okta tenant.
See our online documentation for Identity Provider Discovery

Identity Provider Routing rules is a feature provided by Identity Provider (IdP) Discovery in Okta. This feature allows an Okta admin to route users to different authentication sources based on the user, user property, target application, source network or device type.

In the context of this guide, the primary use case would be to direct authentication to MobileIron Access if the user is attempting to login from a mobile device.

Login to the Okta admin UI with Administrator privileges or any other role entitled to modify Identity Providers and Routing

Identity Provider Routing Rules are evaluated in order, you can rearrange the order of listed rules. If no user configured rules apply to an authentication attempt the system provided **Default Rule** is used.

1. Navigate to **Security -> Identity Providers**
2. Click the **Routing Rules**
3. Click the **Add Routing Rule** or select a rule from the list and click **Edit**
4. Define a rule name (e.g Mobile Requests to MI Access)
5. Define the conditions

User's IP is	• Anywhere • In a specific Zone or list of Zones • Not in a specific Zone or list of Zones
User's device platform is	• A device form factor • A device operating system
User is accessing	• Selective Target application • Any application

User matches	• Evaluate properties of the login value
	  ○ Regex on Domain
	  ○ Domain in a list
	• Pattern matching on specific user attributes
	  ○ Equals
	  ○ Starts with
	  ○ Contains
	  ○ Regex

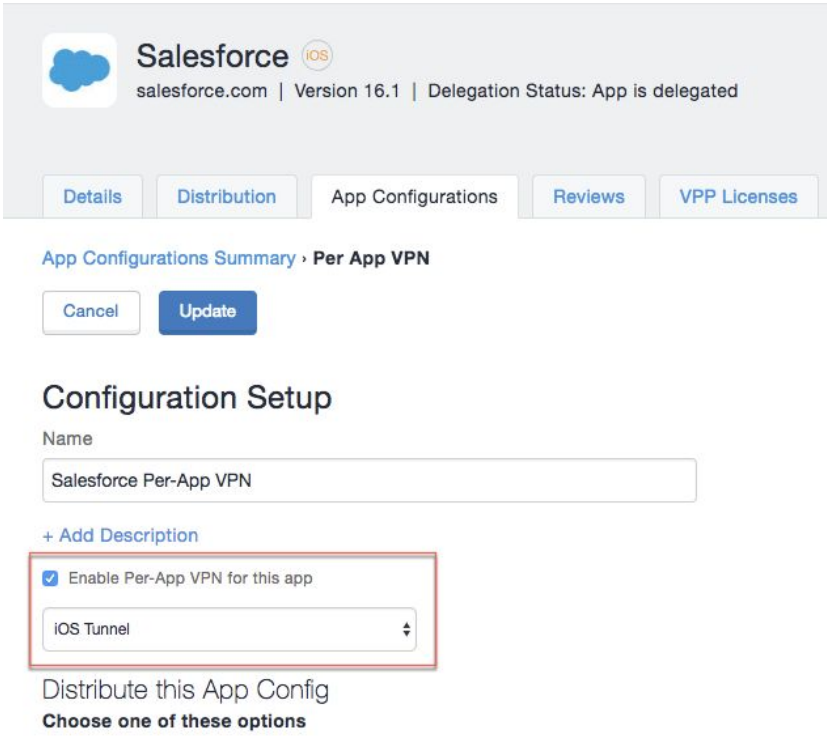
6. Define the action

Use this Identity Provider	• Okta
	  ○ Authenticate the user locally or via delegated Auth
	• IWA
	  ○ Redirect the user to an IWA server for Desktop SSO
	• MobileIron Access
	  ○ Redirect the user/device to MobileIron access

7. Note that **if using Okta as Federation for MobileIron Cloud,** it should be **excluded** from routing to MobileIron Access. Otherwise it **may result in a scenario where an unmanaged device is unable to enroll.**
8. **Save** Routing Rule

Verify Configuration

1. **Register** an **iOS or Android** device to MobileIron **Core or Cloud**
2. **Publish App** for Service to be verified (e.g Salesforce)
   a. **Ensure Per-App VPN (Tunnel) is applied**



3. **Install and Open the App**, which should **trigger Per-App-VPN**
4. If Per-App VPN and Cert-based SSO is working, **user should be authenticated without prompting for a password.**
5. **If the transaction is successful**, a **SAMLCertIdp type transaction will be logged in the MobileIron Access reports section** indicating as such:

Network Zones and Sign on Policies in Okta

When coupled with App Tunneling and Per-App VPN Profiles this feature allows Okta to substitute a network traffic rule for device trust.

Since traffic flowing through a MobileIron Tunnel appliance is authenticated using a device certificate that is issued by MobileIron and revoked by MobileIron if the device drifts out of compliance an Okta administrator can trust that a user logging in with traffic coming from the network associated with their MobileIron Tunnel is using a trusted device.

See IP Zones to create a new network zone with the egress IP address of your MobileIron Tunnel or other VPN appliance and then review Sign On policies for applications to help guide the creation of application sign on policies that adapt to require MFA or even restrict access to users accessing an application from outside the network that represents your MobileIron Tunnel or other trusted VPN traffic.

References

Below are links to relevant materials from Okta and MobileIron

Owner	Details	Link

Sequence Diagrams

Refer to these example web sequence diagrams to gain a better understanding of the various flows

SP Initiated - User accessing SaaS application from a mobile device