Advanced integrations with Okta: VMware Workspace ONE

v1.5
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

This document is intended for Okta sales engineers and partners looking to integrate Okta with VMware's Workspace ONE product suite. This document will provide an in-depth review of the involved components and how they can be paired. When combined, Okta and Workspace ONE deliver optimal 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 5,500 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 Workspace ONE

VMware Workspace™ ONE™ is the simple and secure enterprise platform that delivers and manages any app on any smartphone, tablet, or laptop. It begins with consumer grade self-service, single-sign on access to cloud, mobile, and Windows apps and includes powerfully integrated email, calendar, file and collaboration tools that engage employees.

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 the best of breed capabilities provided by both companies, Workspace ONE as the platform capable of weaving the Unified Endpoint Management capabilities of AirWatch and virtualized application delivery capabilities of Horizon with a Common Identity Management framework. 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 interops stories that help organizations solve complex business problems. The breadth of which span from security enhancements to simplified architecture.

<u>Prevent Data Breaches and Unauthorized access with AMFA</u>

Integrate Okta's Adaptive MFA into the management of your AirWatch and Workspace ONE 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.

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

Workspace ONE 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.

<u>Keep your digital transformation moving like a well oiled machine</u>
The struggle is real… tell the tale of inefficiency and fatigue that employees face with each new application deployed. -- better user experience, streamlined access, one portal to rule them all.

Consolidate access to your legacy applications, virtual desktop infrastructure and cloud applications in once location allowing your users to move securely from application to application regardless of device.

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.

Directory Alignment

Throughout this guide the concept and reality of multiple sources of identity data is on display. Referred to as Directory Mapping, Attribute mapping, Profile mapping or a variety of other names. Replicating user account information such as Names, Email addresses and Phone numbers is important but should be thought of separately from federation providers and authentication providers.

Okta, VMware UEM (AirWatch) and VMware Identity Manager are distinct systems with separate internal user databases that can be synchronized in a variety of ways. While not required, often times all three of these will synchronize with a fourth external directory like Active Directory or LDAP.

There aren't any known limitations to how they are integrated but careful consideration should be given to the different directory schemas in each system, how attributes are mapped and how changes are propagated between them.

As the reasons for arranging directory replication in a specific manner are very specific to an organization, this guide makes no recommendations or assumptions about how a directory is configured. This guide only assumes that the data between the systems is consistent. Refer to Okta and VMware for more information on this.

While all attributes and their respective values are important, the following attributes are the most critical to seamless access for users across the different systems:

	AD	**Okta**	**AirWatch**	**Workspace ONE**
Short Username	sAMAccountName	n/a	UserName	userName
Qualified Username	userPrincipalName	login	UserPrincipalName	userPrincipalName
Email Address	mail	mail	EmailAddress	email

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 attribute vary between SPs 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 VMware UEM (AirWatch). 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 Workspace ONE 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

Workspace ONE

How does Workspace ONE establish device trust?
Workspace ONE has several feeds in terms of device trust, courtesy of the Workspace ONE Trust Network. However, in this context the primary driver for evaluation of trust on mobile devices stems from AirWatch (now known as Workspace ONE UEM). 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 AirWatch 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 AirWatch administrators. Protecting privileged access to a critical system like AirWatch 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 Airwatch	Configure Okta as the IdP for AirWatch

2	Configure Network Zones and Sign on Policies in Okta	Apply conditional access policies including things like limiting access to users from dynamic network zones or requiring multi factor authentication for users with elevated privileges.

Consolidated application portals

The gist of this use case is
- Ease of use
- Efficiency
- Much of the consolidation comes along with SSO (increased ease and security)
- Security by proxy - usually security comes at the expense of convenience, providing convenience to users gives something back or provides some goodwill to spend on other projects that may hurt convenience elsewhere
- Reduced support = more time to do better things

Consolidated Application Portals, Okta MFA for WS1
Mutual IdP story, SAML setup on both ends, Auth Policy in Okta for contextual MFA and access policies in WS1 to send users to Okta so they can trigger MFA

Benefits

- Simplified user experience, increased user adoption
- Reduced IT burden, less training required

Limitations

- Manual configuration required to replicate
- Conditional access policies applied in Workspace ONE can possibly be bypassed if less secure policies allow a user to access some apps in Okta and the Okta session is maintained

Steps to Implement

1	Create a link to a Workspace ONE app from Okta	Create corresponding link to Workspace ONE app in Okta
2	Create a link to an Okta app from Workspace ONE	Create corresponding link to Okta in Workspace ONE

Device Trust through network rules

Device trust through network rules, VMware tunnel pushed from AW 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 AirWatch 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 AirWatch and then setup application sign on policies in Okta to restrict access from unknown networks to targetted 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 AirWatch, in the case of VMware 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 AirWatch, You'll have a high degree of certainty of the user and device identity as well as the security posture of the device.

Follow these steps to Configure App Tunneling and Per-App VPN Profiles and then follow the steps outlined in Network Zones and Sign on Policies in Okta to apply conditional access policies to restrict access or require multi factor authentication for users accessing applications from unknown network zones.

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 AirWatch	Configure and assign to target 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 Preference and Routing

Scenarios will arise when multiple IdPs exist in an environment. Most times (and in the case of Workspace ONE) this occurs when an IdP performs a unique style of authentication for a subset of requests. In this section, we will discuss potential situations that may arise when working with customers of Okta and Workspace ONE, pros/cons and solutions to satisfy the interests of all involved parties.

In the interest of optimal user experience and/or tailored service, a customer may choose to pair a specific Identity provider to be used with their application. Because the Workspace ONE suite delivers a solid SSO offering for mobile devices, an inherent affinity may be found towards solely using the included WS1 Identity provider service. 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.

Workspace ONE as the Default Identity Provider

Benefits

- All access regardless of user, device or target application are directed to Workspace ONE
- Device based conditional policies are always enforced
- “Passwordless” / Mobile SSO for enrolled devices

Limitations

- Removes functionality provided by Okta desktop SSO (IWA)
- Potential introduction of latency (extra redirects between providers)
- Loss of flexibility in the Okta platform (advanced login capabilities provided by Okta)

Steps to Implement

1	Configure Workspace ONE as an Identity Provider in Okta	Establish relationship with Workspace ONE
2	Configure Conditional Access Policies in Workspace ONE	Establish/Review Workspace ONE Policies
3	Configure the newly created Identity Provider to be the Default IdP	Distinguish Workspace ONE as default IdP

Identity Provider Routing Rules

In situations where Okta and Workspace ONE 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 Workspace ONE. 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 WS1 to engage SSO capabilities

Limitations

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

Steps to Implement

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

Custom Login Page

As a generally available (GA) solution to situations where Okta and Workspace ONE are to co-exist, Custom Login Pages can be implemented. While manually created on a per-service basis, they provide the ability to not only redirect an Okta app to Workspace ONE, but to also display a custom page with (as an example) AirWatch enrollment instructions/links for devices that are not currently enrolled. 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

- Available / GA now
- More flexibility than default Identity Provider route

Limitations

- Apply at application target only
- Manual / complex configuration of Workspace ONE required

Steps to Implement

1	Configure Workspace ONE as an Identity Provider in Okta	Establish relationship with Workspace ONE
2	Configure Conditional Access Policies in Workspace ONE	Establish/Review Workspace ONE Policies
3	Configure Workspace ONE as custom login page target for target applications in Okta	Determine when traffic should be directed to Workspace ONE

Device Trust and Mobile SSO

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 Workspace ONE come through with a plan of attack.

Device Trust

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 (AirWatch, now known as Workspace ONE UEM). If a managed instance of Okta Mobile is not found, trust validation effectively fails and the request is denied.

On the Workspace ONE UEM 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 AirWatch 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 Workspace ONE UEM and Okta.

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 Workspace ONE UEM	Configure Okta as IdP for AirWatch
2	Configure Workspace ONE UEM Compliance Policies	Validate device Trust
3	Configure Okta Device Trust for Mobile Devices	Engage Okta Device Trust
4	Initiate Enrollment of Devices to Workspace ONE UEM	Manage Devices with AirWatch

---

Mobile SSO

As a means to further secure the mobile login experience (and further drive ease-of-use), Workspace ONE 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 Workspace ONE 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 an iOS SSO payload, native kerberos agent and identity certificate. When a SSO-permitted app attempts to access the Workspace ONE URL, iOS offers-up an identity certificate on behalf of the user. Workspace ONE extracts the identity of the user, validates trust of source device and (if trust is found) issues a SAML assertion. Managed app then utilizes the assertion to login the user.

Android

On Android, Single Sign-On is achieved by use of VMware Tunnel, identity certificate and Workspace ONE certificate proxy. When a SSO-enabled app attempts to access the Workspace ONE URL, VMware Tunnel engages. Tunnel configuration instructs the device to use Workspace ONE's certificate proxy as the endpoint. The identity certificate is offered-up. Workspace ONE extracts the identity of the user, validates trust of source device and (if trust is found) issues a SAML assertion. 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	Configure Okta as Federation Provider to Workspace ONE UEM	Configure Okta as IdP for AirWatch
2	Configure Workspace ONE as an Identity Provider in Okta	Establish relationship with Workspace ONE
3	Configure Okta Identity Provider Routing Rules	Route mobile auth to Workspace ONE
4	Configure Workspace ONE UEM Compliance Policies	Validate device Trust
5	Configure Workspace ONE UEM SSO for iOS Devices	Configure SSO for iOS
6	Configure Workspace ONE UEM SSO for Android Devices	Configure SSO for Android

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

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.

Workspace ONE as IdP to Okta

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

Okta as IdP to Workspace ONE

Technically a restatement of Okta as an IdP to all applications we are calling this out specifically because it appears frequently in this guide. Configuring Okta as an IdP for Workspace ONE provides a conduit for

consistent login experiences and streamlined MFA for users that are accessing Workspace ONE resources from an unmanaged device or as the gatekeeper of enrolling a new device.

Okta as IdP to Workspace ONE UEM (formerly Airwatch)

Technically a restatement of Okta as an IdP to all applications we are calling this out specifically because it serves a special purpose in this guide as the back-end to Workspace ONE in terms of device trust, management, app deployment, etc.

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 Airwatch

This Guide describes the process of configuring AirWatch 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 AirWatch.

This step configures Okta as the IdP for your Users and potentially admins that use AirWatch. 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 AirWatch must align.

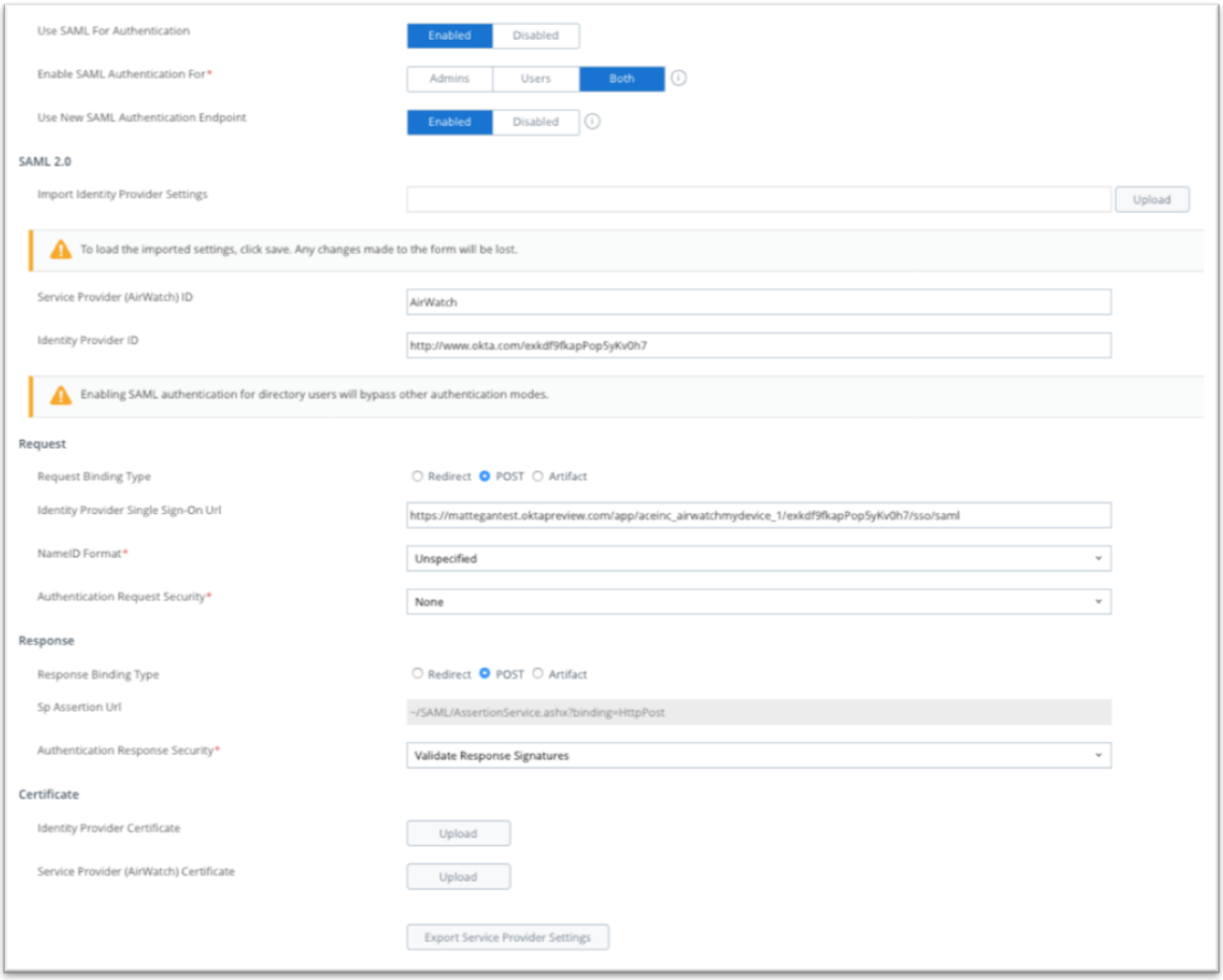
AirWatch Config

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

Server Settings

1. Navigate to **GROUPS & SETTINGS -> All Settings**
2. Expand **System -> Enterprise Integration -> Directory Services**

3. Below the **Advanced** Section Configure
    a. Use SAML for Authentication: **Enabled**
    b. Enable SAML Authentication for: **Both** *(adjust to your needs)*
    c. Use New SAML Authentication Endpoint: **Enabled**
    d. Service Provider (AirWatch) ID: ***AirWatch***
        i. *can be changed, needs to align with the Audience restriction defined in Okta*
    e. Identity Provider ID: Leave Blank or enter a temporary value
        i. We will update after creating the Okta App in later steps
    f. Request Binding Type: **POST**
    g. Identity Provider Single Sign-On Url: Leave Blank or enter a temporary value
        i. We will update after creating the Okta App in later steps
    h. NameID Format: **Unspecified**
    i. Authentication Request Security: **None**
    j. Response Binding: **POST**
    k. Authentication Response Security: **Validate Response Signatures**
    l. Click **Save** and then click **Export Service Provider Settings**
        i. Save the file, make note of this file location, it will be used in later steps



At this point we will move to the Okta setup. After we configure the application in Okta we will revisit this section and replace our blank or temporary values for the Identity Provider ID and the Identity Provider Single Sign-On URI as well as upload the Identity Provider Certificate.

Okta Config

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

Open the exported Service Provider Settings file (service provider metadata) with your favorite text editor.

It looks like this for me:


```
<md:EntityDescriptor entityID="AirWatch" ID="_7fd33467-af32-457b-9a24-50cebd94e337" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:SPSSODescriptor ID="_bea9305b-f156-450e-8815-2b06ca4fc5f7" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" AuthnRequestsSigned="true" WantAssertionsSigned="true">
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"  Location="https://ds888.awmdm.com/IdentityService/SAML/ArtifactResolver.ashx" index="1" isDefault="false" />
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://ds888.awmdm.com/MyDevice/SAML/ArtifactResolver.ashx"  index="2" isDefault="false" />
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://ds888.awmdm.com/DeviceManagement/SAML/ArtifactResolver.ashx" index="3" isDefault="false" />
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://cn888.awmdm.com/AirWatch/SAML/ArtifactResolver.ashx" index="4" isDefault="false" />
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://ds888.awmdm.com/Catalog/SAML/ArtifactResolver.ashx" index="5" isDefault="false" />
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:entity</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ds888.awmdm.com/IdentityService/SAML/AssertionService.ashx?binding=HttpRedirect" index="1" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ds888.awmdm.com/IdentityService/SAML/AssertionService.ashx?binding=HttpPost" index="2" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://ds888.awmdm.com/IdentityService/SAML/AssertionService.ashx?binding=HttpArtifact" index="3" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ds888.awmdm.com/MyDevice/SAML/AssertionService.ashx?binding=HttpRedirect" index="4" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ds888.awmdm.com/MyDevice/SAML/AssertionService.ashx?binding=HttpPost" index="5" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://ds888.awmdm.com/MyDevice/SAML/AssertionService.ashx?binding=HttpArtifact" index="6" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ds888.awmdm.com/DeviceManagement/SAML/AssertionService.ashx?binding=HttpRedirect" index="7" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ds888.awmdm.com/DeviceManagement/SAML/AssertionService.ashx?binding=HttpPost" index="8" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://ds888.awmdm.com/DeviceManagement/SAML/AssertionService.ashx?binding=HttpArtifact" index="9" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://cn888.awmdm.com/AirWatch/SAML/AssertionService.ashx?binding=HttpRedirect" index="10" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cn888.awmdm.com/AirWatch/SAML/AssertionService.ashx?binding=HttpPost" index="11" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://cn888.awmdm.com/AirWatch/SAML/AssertionService.ashx?binding=HttpArtifact" index="12" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ds888.awmdm.com/Catalog/SAML/AssertionService.ashx?binding=HttpRedirect" index="13" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ds888.awmdm.com/Catalog/SAML/AssertionService.ashx?binding=HttpPost" index="14" isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://ds888.awmdm.com/Catalog/SAML/AssertionService.ashx?binding=HttpArtifact" index="15" isDefault="false" />
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```


Locate the **5** AssertionConsumerService (ACS) Locations that have a Binding of ***urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST***

My list looks like this:

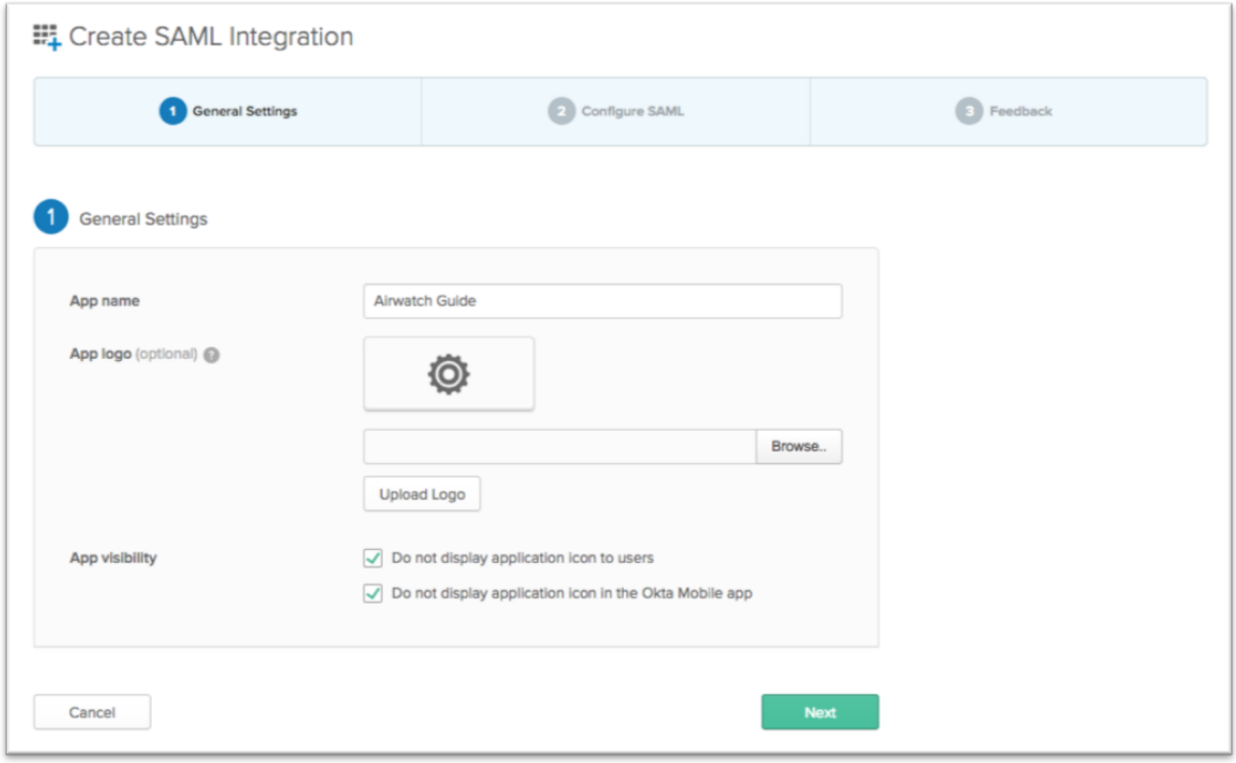
1. https://ds888.awmdm.com/IdentityService/SAML/AssertionService.ashx?binding=HttpPost
    a. https://ds888.awmdm.com/MyDevice/SAML/AssertionService.ashx?binding=HttpPost
    b. https://ds888.awmdm.com/DeviceManagement/SAML/AssertionService.ashx?binding=HttpPost
    c. https://cn888.awmdm.com/AirWatch/SAML/AssertionService.ashx?binding=HttpPost
    d. https://ds888.awmdm.com/Catalog/SAML/AssertionService.ashx?binding=HttpPost

Note the different hostnames and relative paths

With this list extracted we will now sign into Okta as an administrator with privileges sufficient to create new applications.

Application Creation Wizard (SAML)

1. Navigate to **Applications -> Applications**
2. Click **Add Application**
3. Click **Create New App**
4. Select **Web** as the Platform and **SAML 2.0** as the Sign on method
5. Click **Create**
6. Provide a name for the app: *AirWatch SAML*
7. Check both boxes: Do not display the app to users…
8. Click **Next**



9. Single sign on URL:
    a. From the list of ACS URLs paste the URL that has a relative path of **IdentityServices**
        i. *https://ds888.awmdm.com/IdentityService/SAML/AssertionService.ashx?binding=HttpPost*
10. Check the box to **Use this for Recipient URL and Destination URL**
11. Check the box to **Allow this App to request other SSO URLs**
12. Paste the remaining Location URLs WITHOUT the **?binding=HttpPost**
    a. Hint **Add Another**
    b. Keep the index numbers unique, the order doesn't matter as the AuthN Request doesn't reference the index number
13. Define the Audience URI (SP Entity ID): *AirWatch* (refer to entityID from metadata file or step xyz)
14. Set the Application Username to **Okta username**
    a. Note: AirWatch doesn't use the value of the Subject NameID, it relies on an additional SAML attribute defined in the next step, as such the selection here is inconsequential
15. Define an Attribute Statement
    a. Name: **uid**
        i. by default, the name of this attribute should be **uid** refer to the **Mapping Value** for the Attribute called **User Name** in the *Advanced section* of the *User* tab inside of the *Directory Services* section of the *AirWatch admin console* to confirm.
        ii. If misconfigured you'll see this error when trying to sign in "`an error "Authentication response does not contain "uid" nor configured username attribute."`
        iii. The name is case sensitive
    b. Name format: **unspecified**
    c. Value: **user.login**
        i. The value of this attribute needs to match the value of your AirWatch users User Name attribute
            1. Example1: Okta User login prefix

a. *String.substringBefore(user.login, "@")*

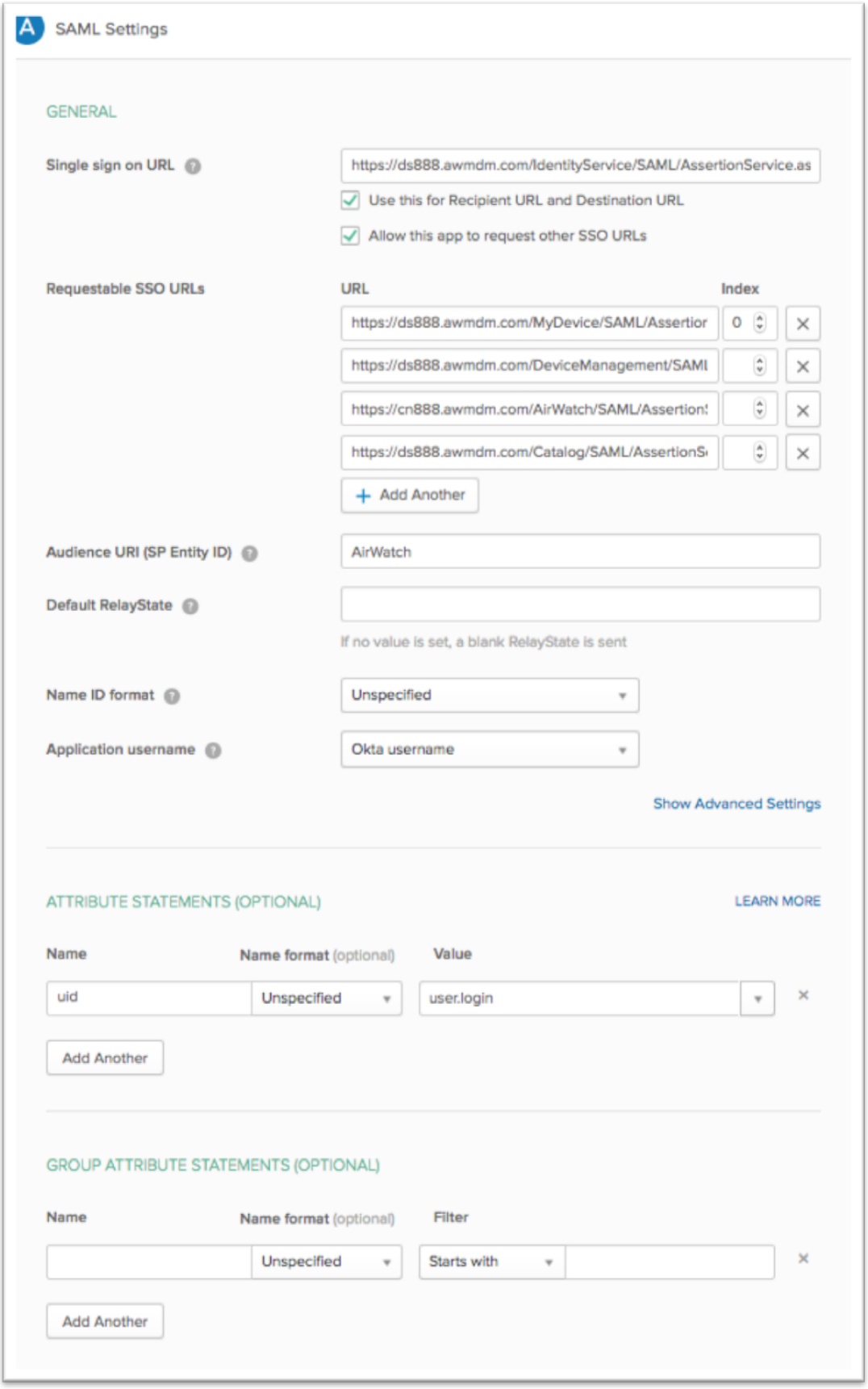
2. Example2: Active Directory sAMAccountName

a. *active_directory.sAMAccountName*

ii. Refer to our Okta Expression Language documentation for more information

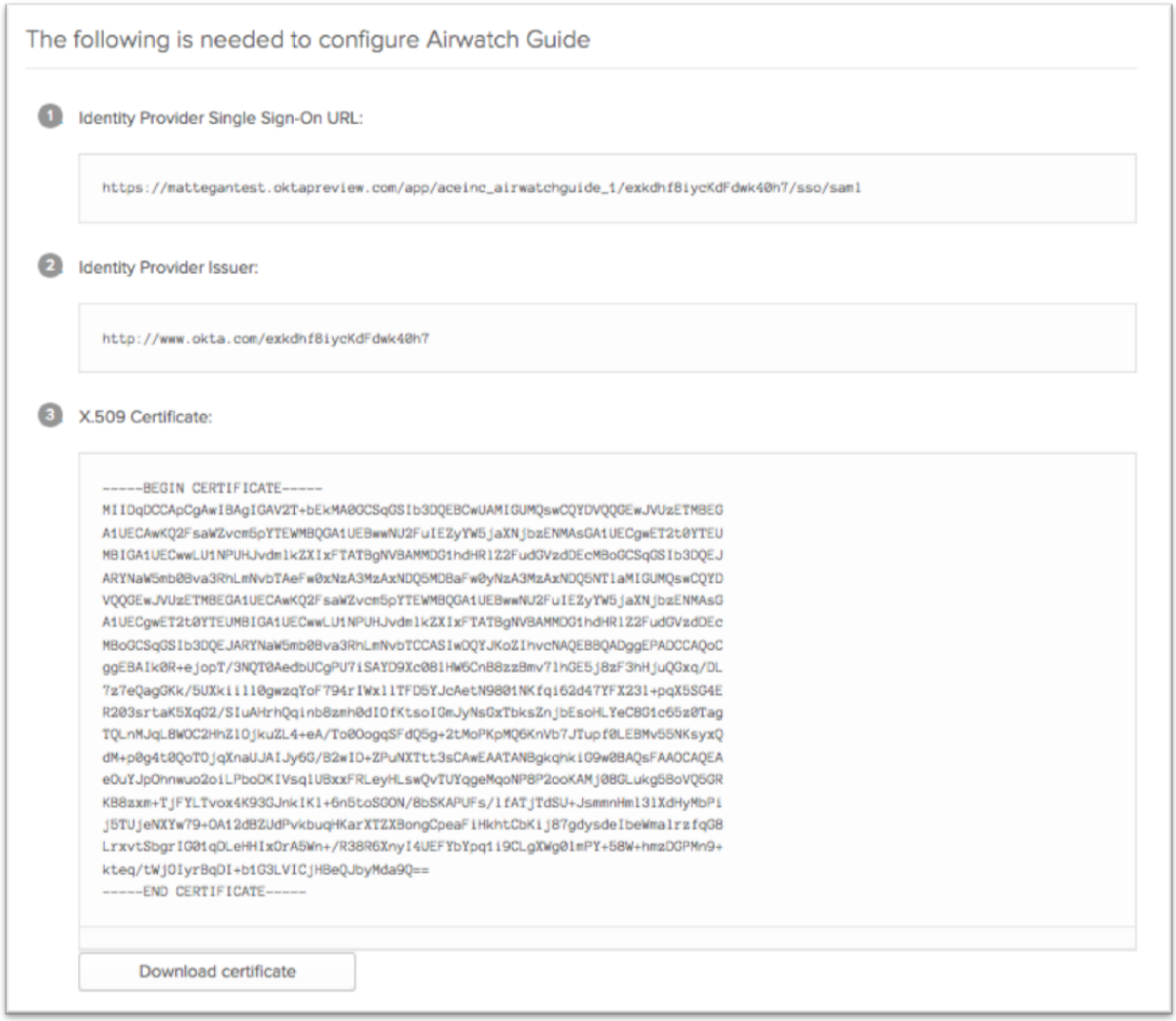
iii. Review directory mappings and sync sources between systems to ensure the correct values are selected

16. Click **Next**



17. Select the **I'm an Okta customer adding an internal app** button
18. Check the **This is an internal app that we have created** box

19. Click **Next**
20. Click the **View Setup Instructions** Button
21. Download the X.509 Certificate by clicking Download Certificate
22. Copy the **Identity Provider Single Sign-On URL** value and paste it into the AirWatch Identity Provider **Single Sign-On Url** field
23. Copy the **Identity Provider Issuer** value and past it into the AirWatch **Identity Provider ID** field



24. Upload the Certificate downloaded from Okta in Step 21 to AirWatch as the **Identity Provider Certificate**
25. Assign the application to users any Users or Admins that will be using it to login

Bookmark creation

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

AirWatch URLs will have all have a URL parameter of GID, this Identifier of the Organization Groups

defined in AirWatch, you can retrieve the Group ID values from AirWatch

- End User Device Management: https://<hostname1>/MyDevice/Login?GID=<AWgroupId>
- End User Device Enrollment: https://<hostname1>/enroll?GID=<AWgroupId>
- AirWatch Admin Login: https://<hostname2>/AirWatch/Login?GID=<AWgroupId>

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 Workspace ONE

This Guide describes the process of configuring Okta as the Identity Provider to Workspace ONE. This can be used to provide streamlined access to virtualized applications, Provide Okta's extensible Multi Factor Authentication to applications in Workspace ONE, Provide a consistent and familiar login experience for users and administrators alike.

This Document will be used to configure Okta as an Identity Provider (IdP) to your Workspace ONE environment.

Also documented here:

https://communities.vmware.com/blogs/identityville/2017/03/16/okta-and-vmware-workspace-one-integration-okta-as-idp-for-vmware-identity-manager

Start Create New Identity Provider in Workspace ONE

Login to the Workspace ONE Administration Console with Administrator privileges or any other role entitled to add a Third-Party Identity Provider.

1. Click the **Identity & Access Management** tab
2. Navigate to the **Identity Provider** sub menu
3. Click the **Add Identity Provider** button
4. Select **Create Third Party IDP**

5. Navigate to the bottom of the form
6. Locate the **SAML Metadata** item and open the link in a new tab
7. In the SAML Metadata locate the following information
    a. **entityID**
        i. e.g. *https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/sp.xml*
    b. HTTP-POST **AssertionConsumerService Location**
        i. e.g. *https://tenant.vmwareidentity.com/SAAS/auth/saml/response*

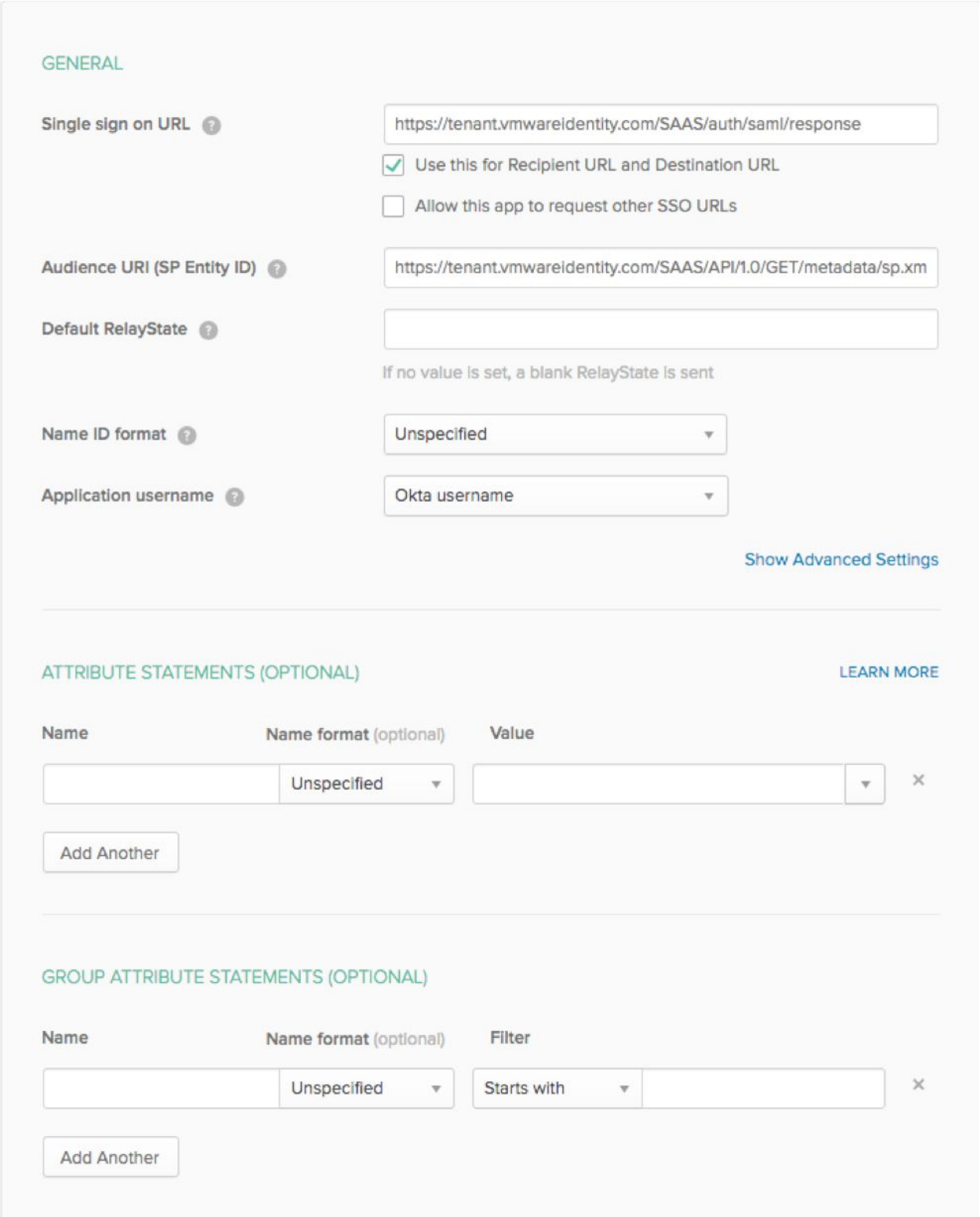
Create new SAML app in Okta

Login to your Okta org and navigate to the Admin UI.

1. Navigate to **Applications -> Applications**
2. Click **Add Application**
3. Click **Create New App**
4. Select **Web** as the Platform and SAML 2.0 as the Sign on method
5. Click **Create**
6. Provide a name for the app: *Workspace ONE SAML*
7. Click **Next**
8. Single sign on URL: ***AssertionConsumerService URL***
    a. Retrieved from the metadata in the previous section
        i. e.g. *https://tenant.vmwareidentity.com/SAAS/auth/saml/response*
9. Audience URI (SP Entity ID): ***entityID***
    a. Retrieved from the metadata in the previous section

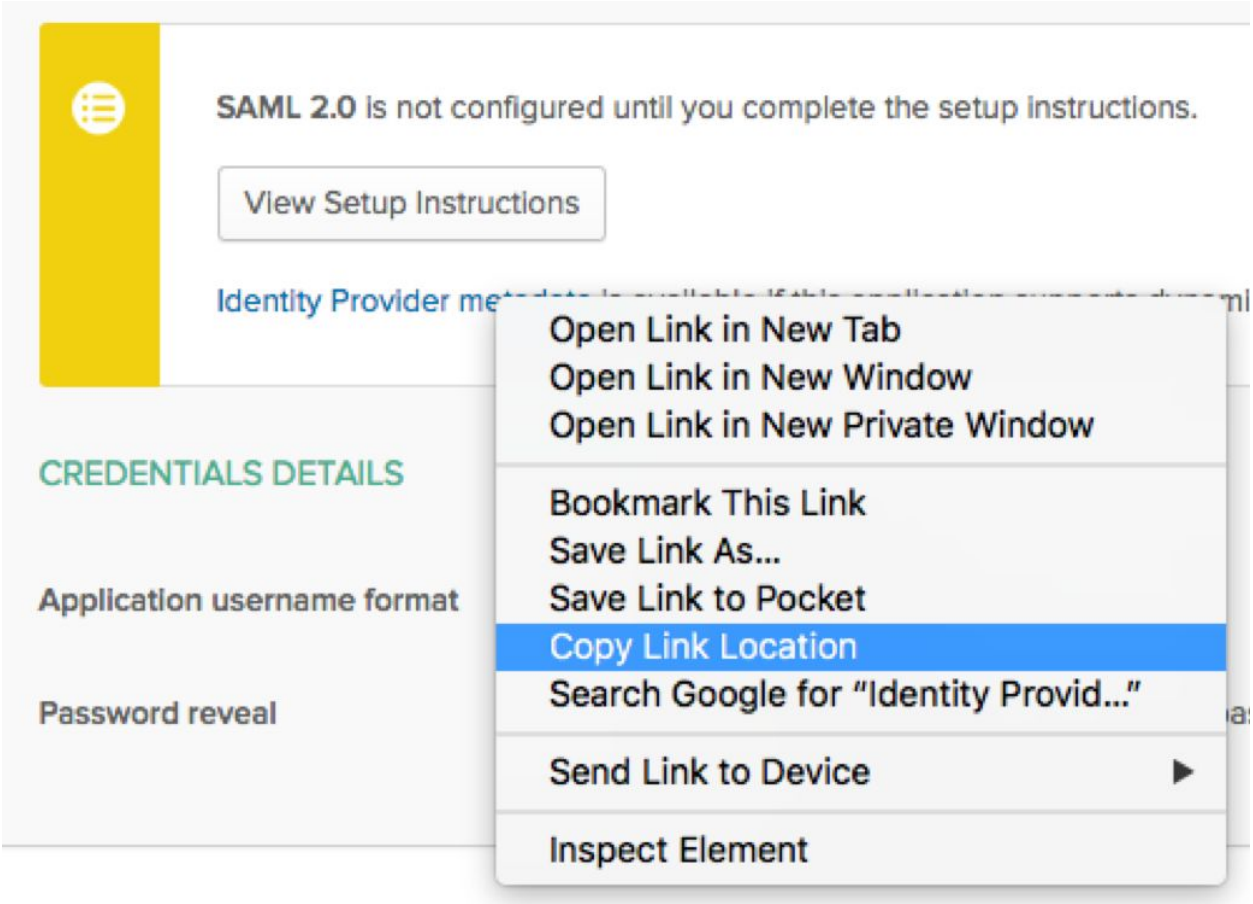
i. e.g. *https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/sp.xml*

10. Name ID format: **Unspecified**
11. Application username: **Okta username**
    a. The application username mapping is defined in the next section, consider the directory sources and mapping to ensure the correct values are sent.



12. Click **Next**
13. Select the **I'm an Okta customer adding an internal app** button

14. Check the **This is an internal app that we have created** box
15. Click **Finish**
16. From the **Settings** section of the **Sign On** sub-menu for the new application locate and copy the URL for the **Identity Provider metadata**

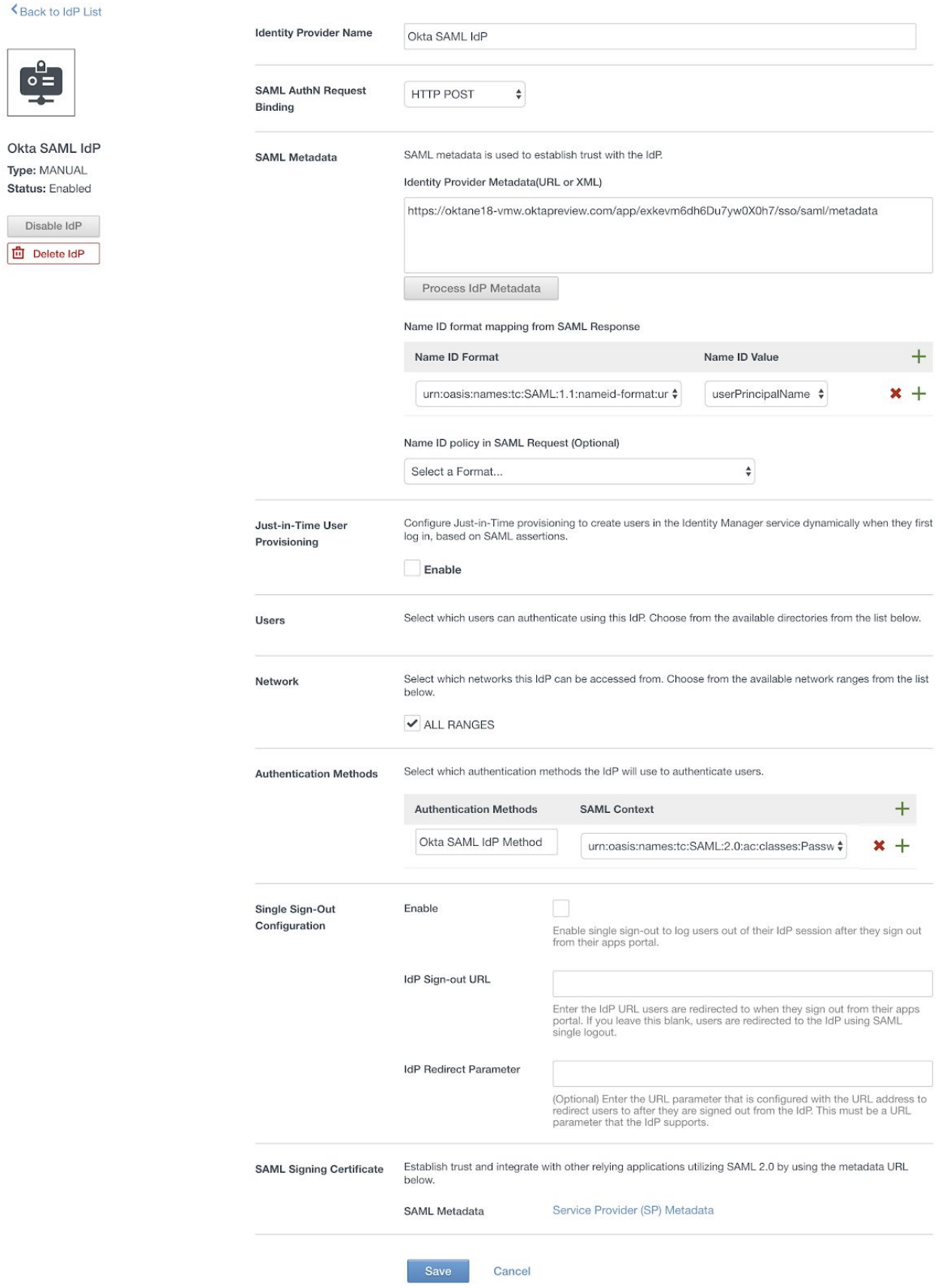


Complete Create New Identity Provider in Workspace ONE

Returning to the Workspace ONE to complete the creation of the new identity provider.

1. Identity Provider Name: ***Okta SAML IdP***
2. SAML AuthN Request Binding: **HTTP Post**
3. SAML Metadata: metadata URL copied from Okta
    a. e.g. *https://yourOktaTenant/app/appId/sso/saml/metadata*
4. After pasting the metadata URL from Okta click the **Process IdP Metadata** button
5. In the Name ID format mapping from SAML Response section
    a. Name ID Format: **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**
    b. Name ID Value: ***userPrincipalName***
        i. Select the User Attribute that the application username value defined in Okta will match
6. Users: *Select the directories you want to be able to authenticate using this IdP*
7. Network: *Select the networks which can access this IdP*
8. Authentication Methods
    a. Authentication Methods: ***Okta SAML IdP Method***

b. SAML Context: **urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport**



9. Click **Add**

JIT users in Workspace ONE from Okta

If you require support to populate a JIT directory in Workspace ONE from Okta in the SAML assertions you'll need to modify the SAML 2.0 application in Okta to send the following attributes.

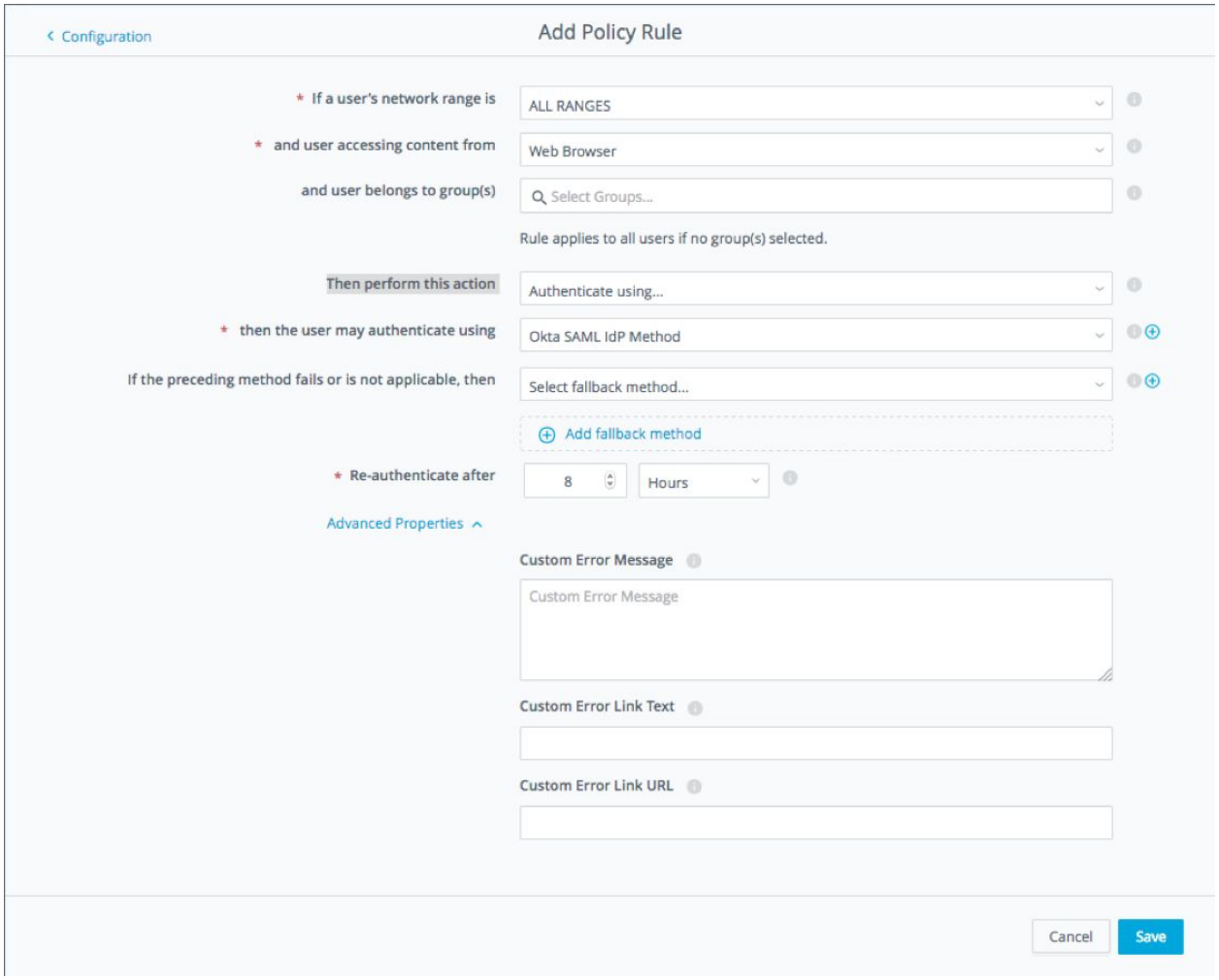
Refer to the Directory Alignment and User Provisioning and lifecycle managment sections for additional context.

Okta UD attribute value source	SAML attribute name	Workspace ONE directory attribute

Add newly created Authentication method to an Access Policy in Workspace ONE

This example will make Okta the default IdP for a configured policy

1. Click the **Identity & Access Management** tab
2. Navigate to the **Policies** sub menu
3. Edit an existing policy (or create a new policy)
    a. If creating a new policy define a policy Name and Description
4. Add or Configure a policy rule to match your criteria
5. Example:
    a. If a user's network range is: ***ALL RANGES***
    b. and user accessing content from: ***Web Browser***
    c. and user belongs to group(s): **Empty** *(all users)*
    d. Then Perform this action: ***Authenticate User…***
    e. then the user may authenticate using: *Okta SAML IdP Method*
        i. Authentication method for the IdP created in the previous step



6. Click **Save**

Assign the app to user in Okta

This completes the setup, assign the application to users in Okta and perform tests. You should see x, y and z
Return to your Okta org and assign the newly created Workspace ONE app to users and perform tests.

Workspace ONE as Identity Provider in Okta

This Guide describes the process of configuring Workspace ONE as an Identity Provider in Okta. When configured this can be used to provide Mobile SSO (passwordless authentication) for users on enrolled devices as well as conditional access based on Device compliance as configured and managed by AirWatch and enforced by Workspace ONE.

For General information review the **Configure Inbound SAML** section of our Identity Providers documentation

Note: If WS1 is not the default and only IdP device trust could be circumvented by a user accessing okta through a username/password, to add ongoing enforcement of "device trust" in Okta you can add app tunneling and network rules as described in Configure App Tunneling and Per-App VPN Profiles and Network Zones and Sign on Policies in Okta

In this document we will configure Workspace ONE as an Identity Provider in Okta.

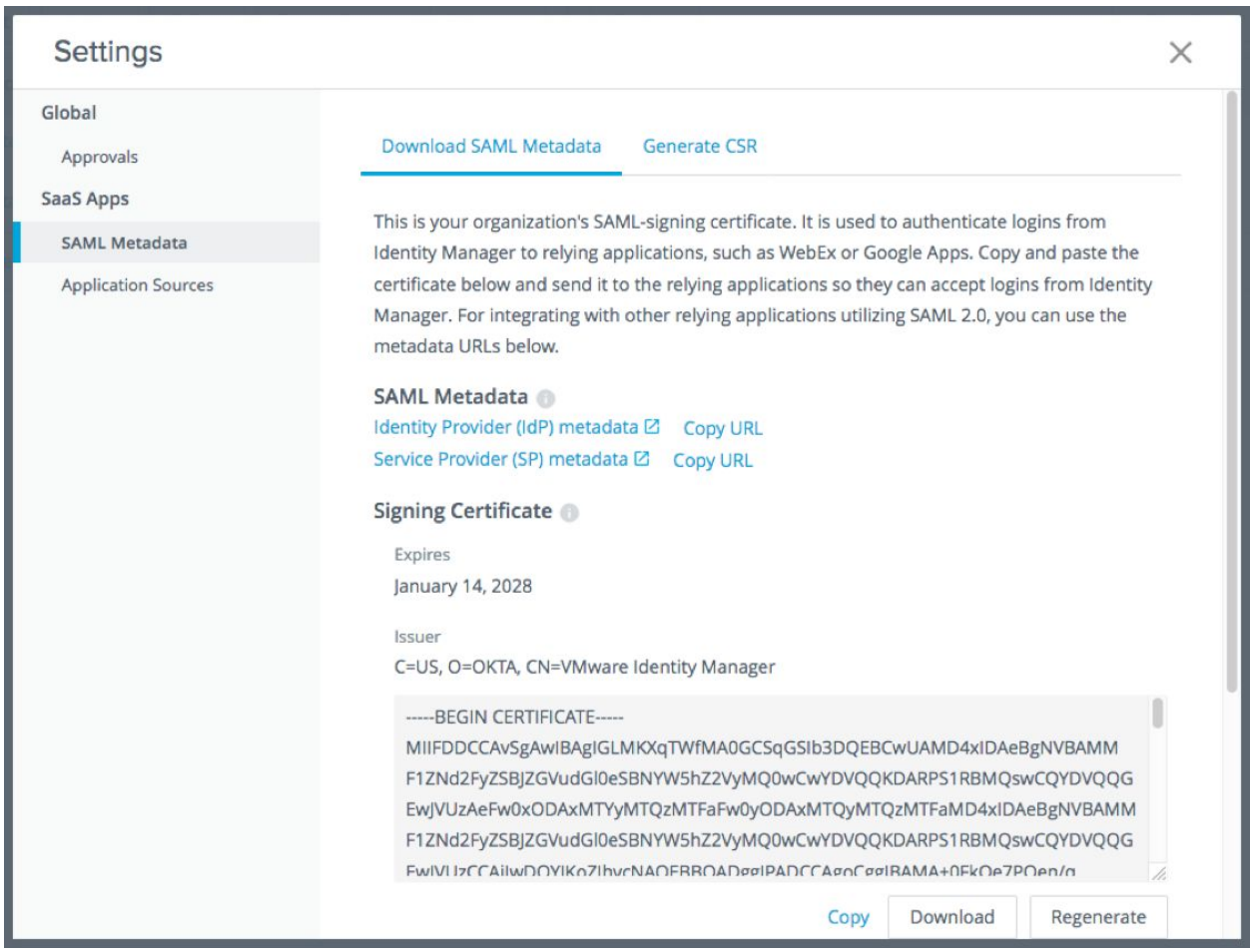
Also documented here:
https://communities.vmware.com/blogs/identityville/2017/01/03/configuring-vmware-identity-manager-as-idp-for-okta

Get Workspace ONE Identity Provider details

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

Login to the Workspace ONE Administration Console with Administrator privileges or any other role entitled to add a New SaaS Application

1. Click the **Catalog -> Web Apps** tab
2. Click **Settings** from the sub-menu
3. In the resulting dialog navigate to **SaaS Apps -> SAML Metadata**
4. Download the **Signing Certificate**
    a. Note the location of the downloaded file ***signgingCertificate.cer***
5. Open the **Identity Provider (IdP) metadata** link in a new window
6. In the IdP Metadata file locate and record the
    a. entityID
        i. e.g. *https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml*
    b. **SingleSignOnService** with Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        i. e.g. *https://tenant.vmwareidentity.com/SAAS/auth/federation/sso*



Add Identity Provider in Okta

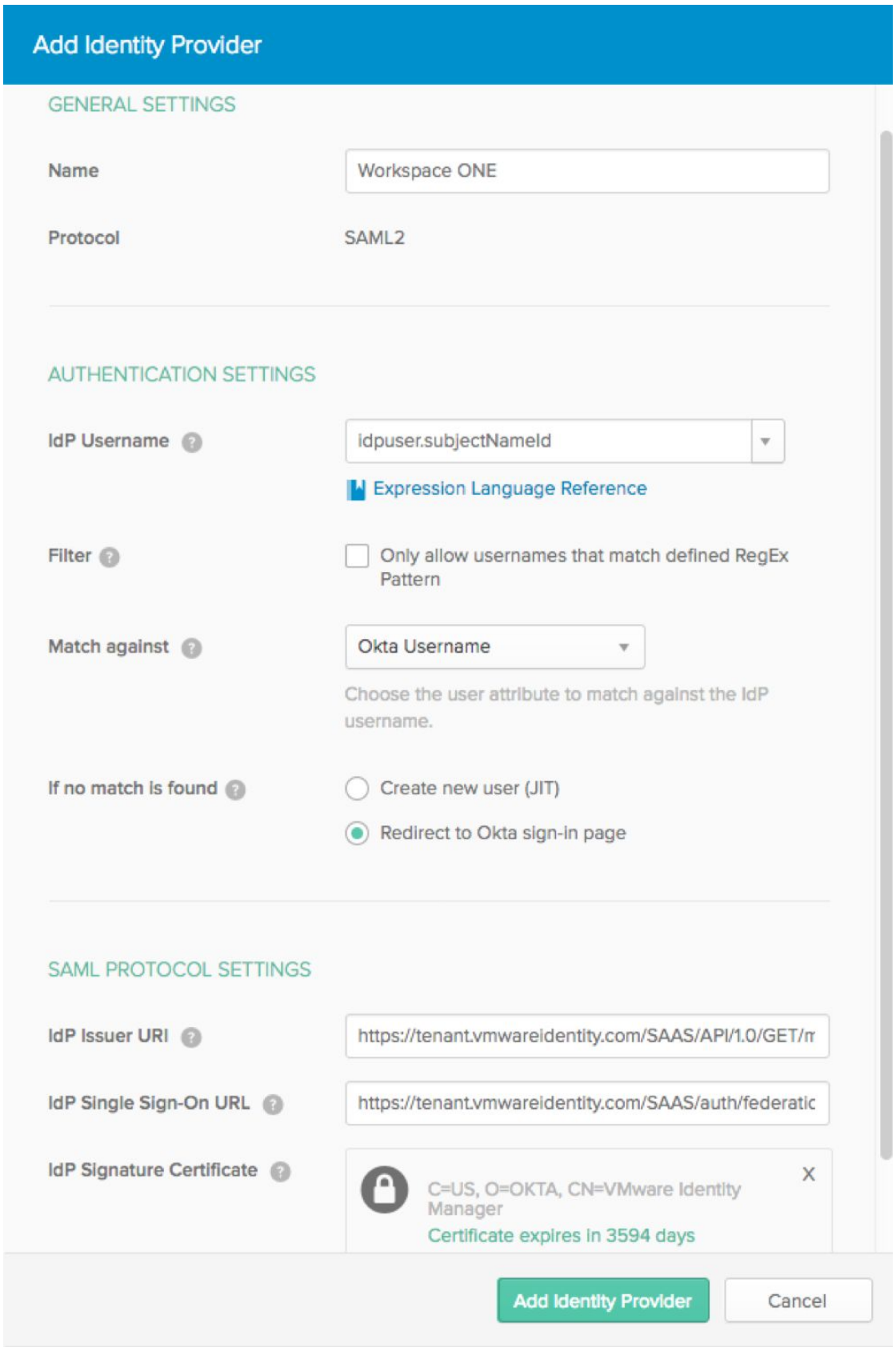
In this section we will create the Identity Provider (IdP) record in Okta

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

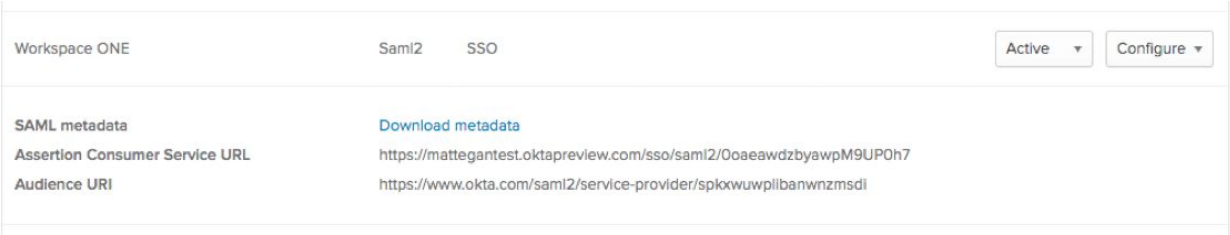
For additional information about how Okta deals with external identity providers review our product help guide on Identity Providers

1. Navigate to **Security -> Identity Providers**
2. Click **Add Identity Provider**
3. Provide a Name: ***Workspace ONE***
4. IdP Username: ***idpuser.subjectNameId***
    a. If you will be sending the username in a custom SAML attribute define an appropriate expression, refer to *https://developer.okta.com/reference/okta_expression_language/index#idp-user-profile*
5. Filter: ***Unchecked***
6. Match Against: ***Okta Username***
    a. Adjust as required for your environment and the values you'll be sending
    b. Refer to the Directory Alignment chapter for information

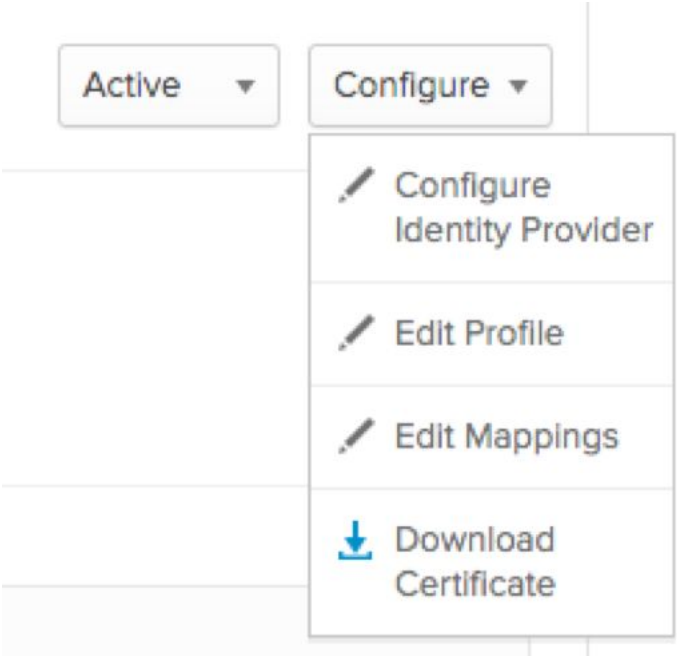
7. If no match is found: ***Redirect to Okta sign-in page***
8. IdP Issuer URI: ***entityID***
    a. value from IdP metadata file from Workspace ONE
    b. e.g. *https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml*
9. IdP Single Sign-On URL: ***SingSignOnService Location***
    a. value from IdP metadata file from Workspace ONE
    b. e.g. *https://tenant.vmwareidentity.com/SAAS/auth/federation/sso*
10. IdP Signature Certificate
    a. Browse and select the Signing Certificate from Workspace ONE
        *i. Hint: you may need to change the file extension or default browser filter looking for *.crt and *.pem files*
11. Click **Add Identity Provider**



12. Observe the following
    a. Assertion Consumer Service URL
    b. Audience URI



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*

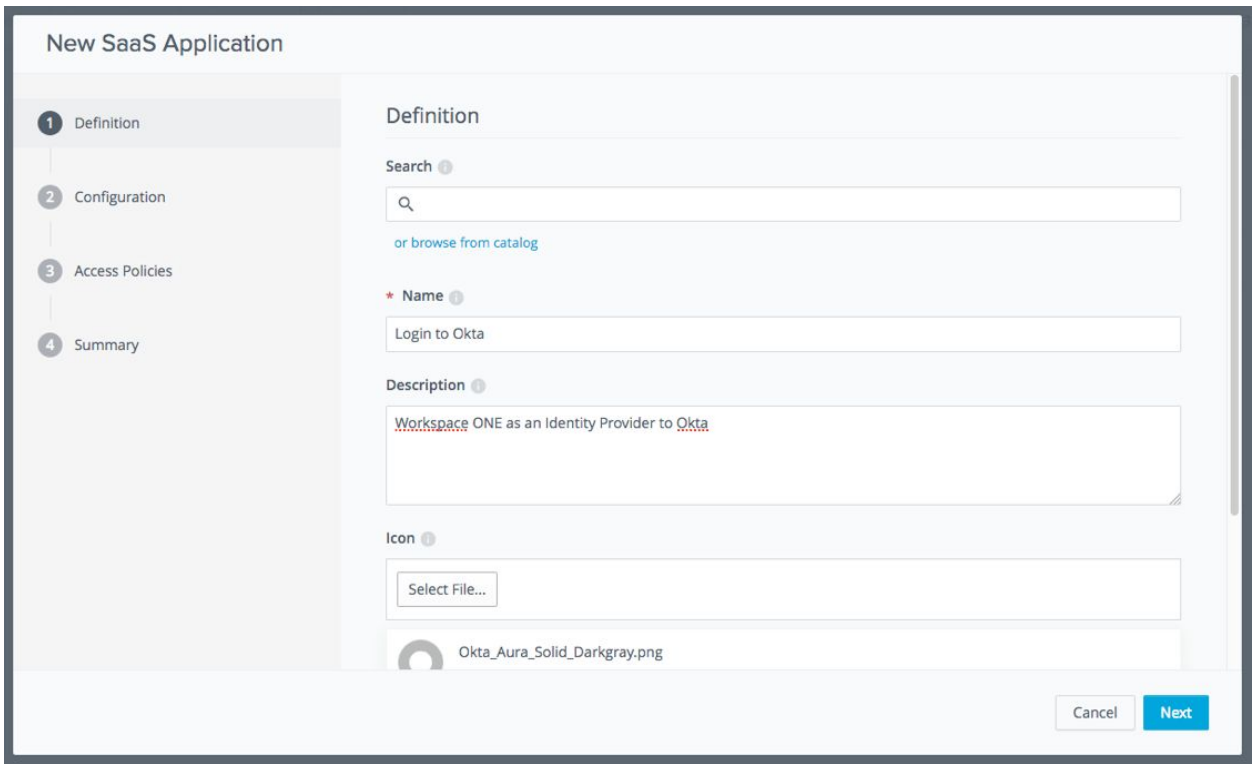


Create New SaaS Application in Workspace ONE

Login to the Workspace ONE Administration Console with Administrator privileges or any other role entitled to add a New SaaS Application

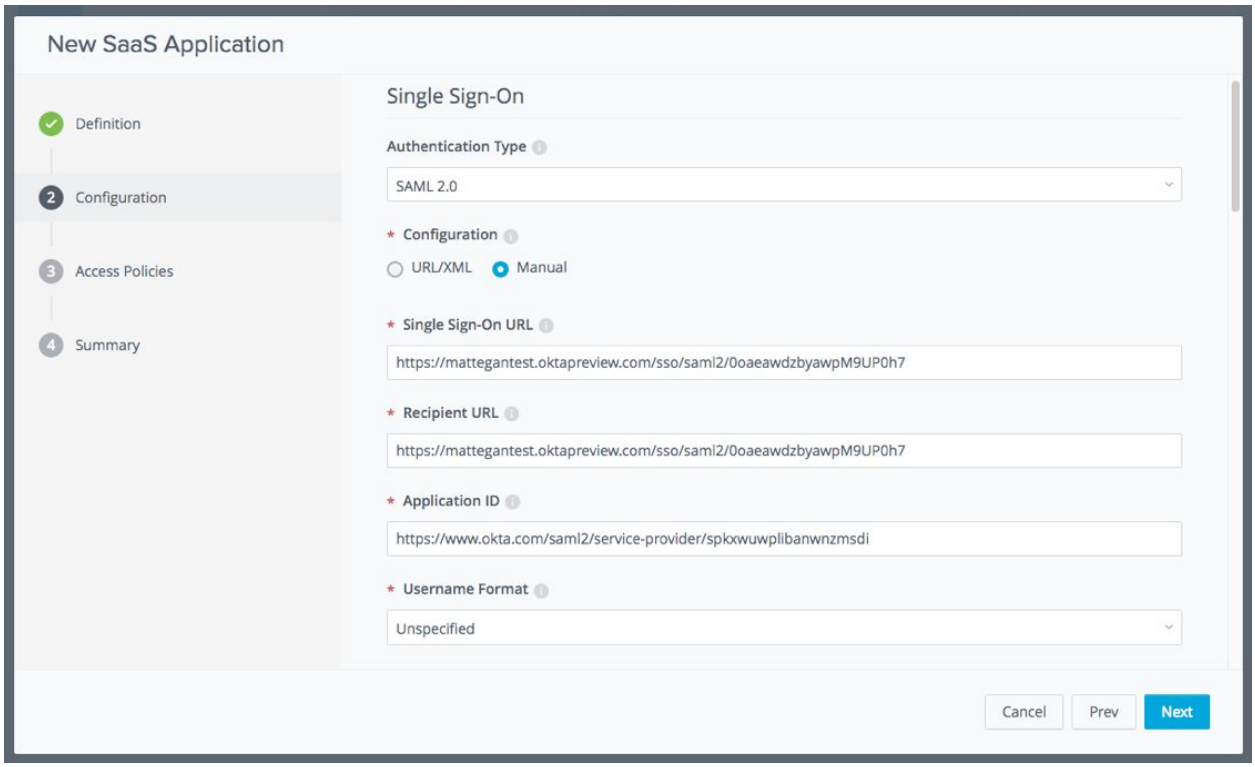
This process is nearly identical to the Configure OKTA Application Source in Workspace ONE process.

1. Click the **Catalog -> Web Apps** tab
2. Click **New**
3. Provide a Name: ***Login to Okta***
4. Description: ***as you see fit***
5. Optionally *select an Icon*
6. Optional *select a Category*



7. Click **Next**
8. Authentication Type: **SAML 2.0**
9. Configuration: **Manual**
10. Single Sign-On URL: ***Assertion Consumer Service URL from Okta IdP***
    a. e.g. *https://yourOktaOrg/sso/saml2/0oaeawdzbyawpM9UP0h*
11. Recipient URL: ***Assertion Consumer Service URL from Okta IdP***
    a. *e.g. https://yourOktaOrg/sso/saml2/0oaeawdzbyawpM9UP0h*
12. Application ID: ***Audience URI from Okta IdP***
    a. e.g. *https://www.okta.com/saml2/service-provider/spkxwuwplibbnwnamsdi*
13. Username Format: **Unspecified**
14. Username Value: ***${user.userPrincipalName}***
    a. Choose an appropriate attribute source from Workspace ONE
    b. Refer to the Directory Alignment chapter for information
15. Expand **Advanced Properties**
16. Sign Response: ***Yes***
17. Sign Assertion: ***No***
18. Encrypted Assertion: ***No***
19. Include Assertion Signature: ***No***
20. Signature Algorithm: ***SHA256 with RSA***
21. Digest Algorithm: ***SHA256***
22. Assertion Time: ***200***
23. Request Signature: contents of Okta.cert file previously downloaded from Okta
    a. open file with text editor and paste the contents including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
24. Encryption Certificate: ***Blank***
25. Application Login URL: ***Blank***
26. Proxy Count: ***Blank***
27. API Access: ***No***

28. Custom Attribute Mapping: ***None***
    a. If you need to do SAML JIT (just in time) provisioning you'll need to configure your Okta
29. Open in VMware Browser: ***No***



30. Click **Next**
31. Assign an Access Policy
32. Click **Next**
33. Click **Save**
34. *Optionally assign the new SaaS application to users and groups as required*

JIT users in Okta from Workspace ONE

If you require support to perform JIT creation of users in Okta from Workspace ONE you'll need to modify the SAML 2.0 application in Workspace ONE to include **Custom Attribute Mappings** that align with the JIT provisioning settings in Okta

Refer to the Directory Alignment and User Provisioning and lifecycle managment sections for additional context.

Refer to the JIT Settings section of Okta's Identity Provider documentation

Workspace ONE directory source attribute	**SAML attribute name**	**Okta UD Mapping**

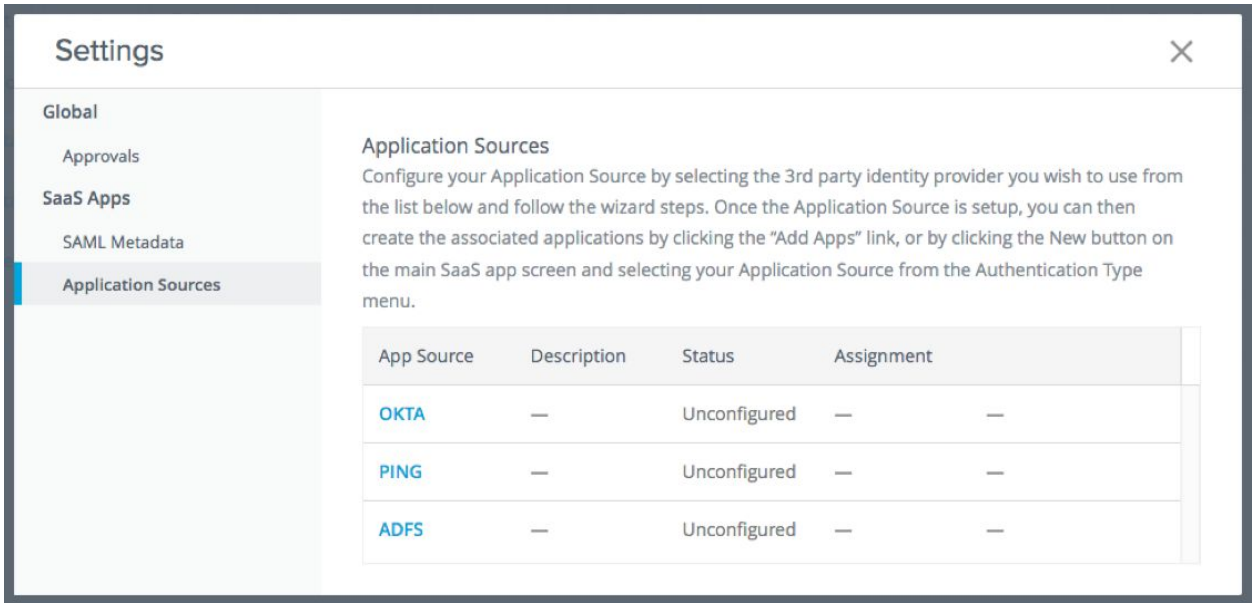
Configure OKTA Application Source in Workspace ONE

Follow this step if you wish to display Okta application links in your Workspace ONE user Portal. Once configured you'll be able to add Okta applications in Workspace ONE

This process is nearly identical to the Create New SaaS Application in Workspace ONE process.

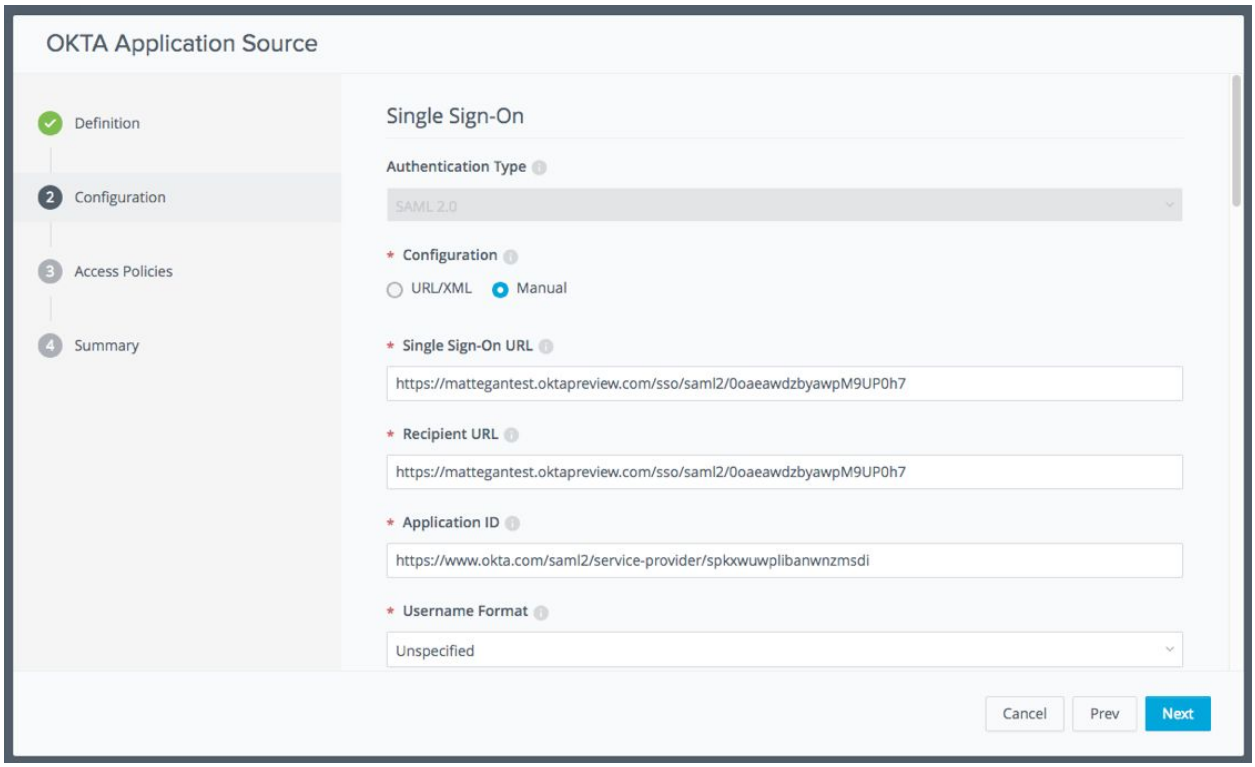
Login to the Workspace ONE Administration Console with Administrator privileges or any other role entitled to add a New SaaS Application

1. Click the **Catalog -> Web Apps** tab
2. Click **Settings** from the sub Menu bar
3. In the resulting dialog navigate to **SaaS Apps** and select **Application Sources**



4. Click **OKTA**
5. Optionally provide a description and click **Next**
6. Authentication Type: **SAML 2.0**
7. Configuration: **Manual**
8. Single Sign-On URL: Assertion Consumer Service URL from Okta IdP
   a. *https://yourOktaOrg/sso/saml2/0oaeawdzbyawpM9UP0h*
9. Recipient URL: Assertion Consumer Service URL from Okta IdP
   a. *https://yourOktaOrg/sso/saml2/0oaeawdzbyawpM9UP0h*
10. Application ID: Audience URI from Okta IdP
    a. *https://www.okta.com/saml2/service-provider/spkxwuwplibbnwnamsdi*
11. Username Format: **Unspecified**
12. Username Value: ***${user.userPrincipalName}***
    a. Choose an appropriate attribute source from Workspace ONE
13. Expand **Advanced Properties**
14. Sign Response: ***Yes***
15. Sign Assertion: ***No***
16. Encrypted Assertion: ***No***
17. Include Assertion Signature: ***No***
18. Signature Algorithm: ***SHA256 with RSA***

19. Digest Algorithm: ***SHA256***
20. Assertion Time: ***200***
21. Request Signature: contents of Okta.cert file previously downloaded from Okta
    a. open file with text editor and paste the contents including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
22. Encryption Certificate: ***Blank***
23. Application Login URL: ***Blank***
24. Proxy Count: ***Blank***
25. API Access: ***No***
26. Custom Attribute Mapping: ***None***
    a. If you need to do SAML JIT (just in time) provisioning refer to **JIT Settings** in our Identity Providers documentation
27. Open in VMware Browser: ***No***



28. Click **Next**
29. Assign an Access Policy
30. Click **Next**
31. Review the summary and click **Save**

JIT users in Okta from Workspace ONE

If you require support to perform JIT creation of users in Okta from Workspace ONE you'll need to modify the SAML 2.0 application in Workspace ONE to include **Custom Attribute Mappings** that align with the JIT provisioning settings in Okta

Refer to the Directory Alignment and User Provisioning and lifecycle management sections for additional context.

Refer to the JIT Settings section of Okta's Identity Provider documentation

Workspace ONE directory source attribute	SAML attribute name	Okta UD Mapping

---

Configure Default Identity Provider in Okta

When integrating Okta and Workspace ONE to achieve Mobile SSO or enforce device compliance policies you may choose to configure Workspace ONE as the default Identity Provider to Okta. Use the steps below to achieve this.

See Configure Inbound SAML -> Workflow -> **Part 5 (optional) – Specify a default IdP and configure an error page URL** in our Identity Providers documentation.

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

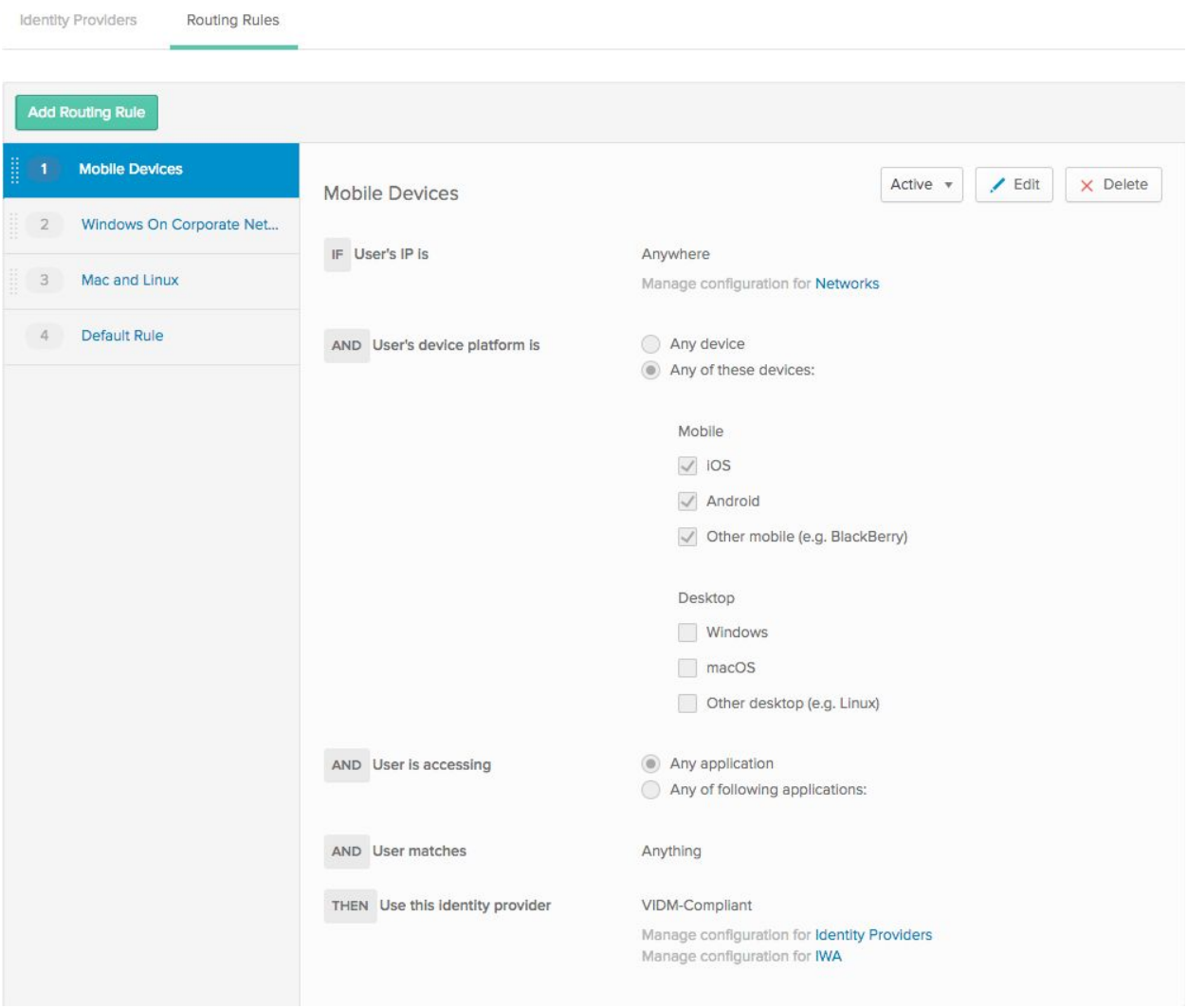
Identity Provider Routing rules is a feature provided by Identity Provider (IdP) Discovery in Okta. This feature allows an Okta admin to route users to different authentication sources based on the user, user property, target application, source network or device type.

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

Sign into Okta as an administrator with privileges sufficient to create or modify Identity Provider Routing Rules

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
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 ● SAML IdP ○ Redirect the user to a specific federated IdP

Edit Rule

Rule Name

Mobile Devices

IF User's IP is — In zone

Manage configuration for Networks

All Zones

Zones

AND User's device platform is

Any device

Any of these devices:

Mobile

iOS

Android

Other mobile (e.g. BlackBerry)

Desktop

Windows

macOS

Other desktop (e.g. Linux)

AND User is accessing

Any application

Any of following applications:

AND User matches — User attribute

login — Starts...

THEN Use this identity provider — VIDM-Compliant

Manage configuration for Identity Providers

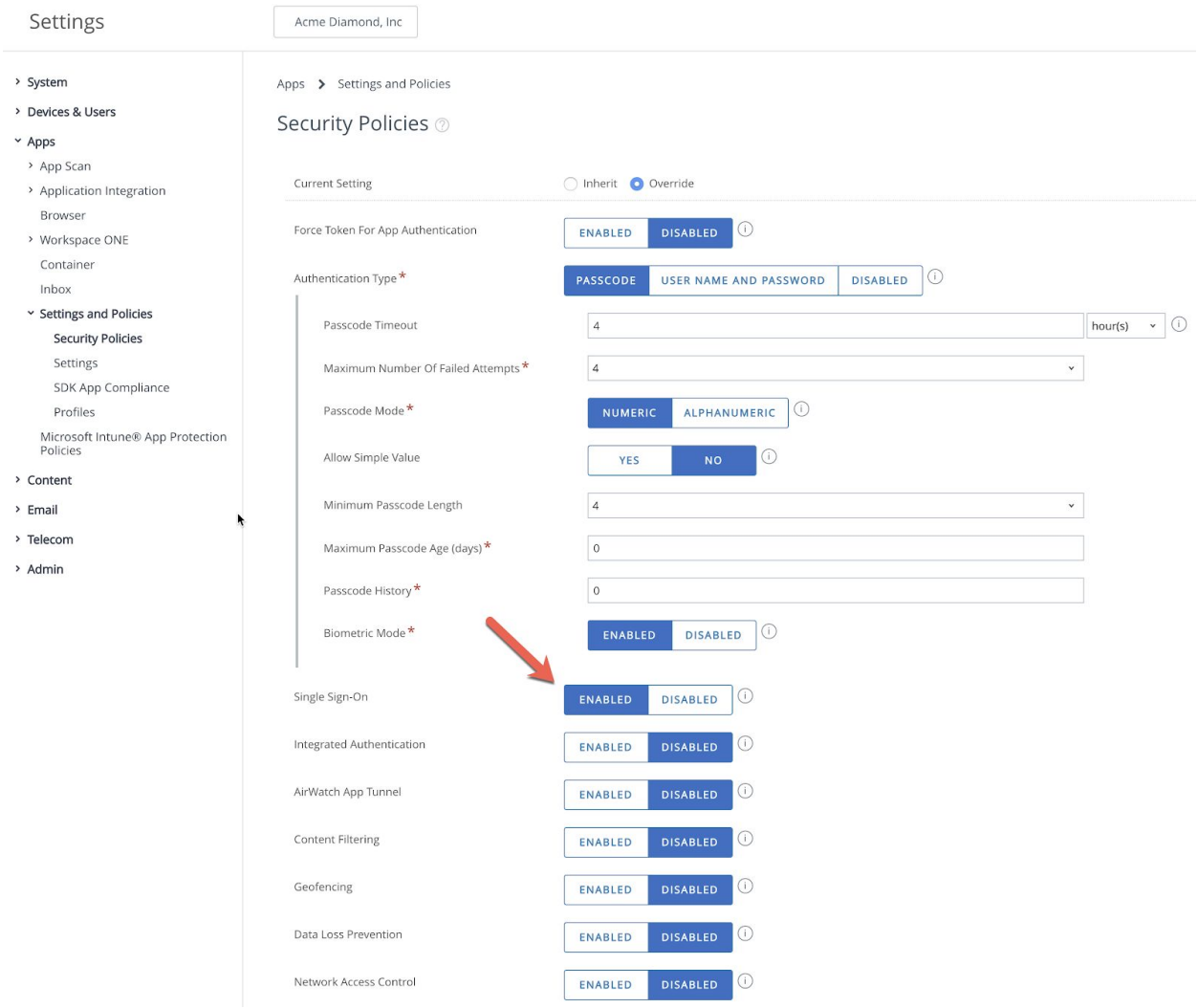
Manage configuration for IWA

Update Rule | Cancel

Configure Workspace ONE Seamless Hand-Off

When Workspace ONE is presented as the point of enrollment, a SSO setting inside Workspace ONE UEM (AirWatch) must be enabled. This allows a seamless hand-off from Workspace ONE on the user's behalf into AirWatch so that a second authentication prompt is not received. This can also eliminates any user activity directly into AirWatch portals (as it is all handled from Workspace ONE). From the AirWatch administrative portal:

1. Navigate to **GROUPS & SETTINGS -> All Settings**
2. Navigate to **APPS**
3. Navigate to **SETTINGS AND POLICIES -> Security Policies**
4. Update ***Current Setting*** to **Override**
5. Set the **Single Sign-On** flag to **Enabled**
6. **Save** the setting at the bottom of the page



Configure App Tunneling and Per-App VPN Profiles

When configured in conjunction with Network Zones and Sign on Policies in Okta this feature provides a sort of continuous authentication and the ability for Okta to granularly enforce what is essentially "arms length" device trust.

This document will describe the configuration using VMware Tunnel but it could also be implemented using a variety of VPN endpoints.

Prepare VMware Tunnel and configure Per-App VPN policies

The VMware Tunnel provides a secure and effective method for individual applications to access corporate resources. The VMware Tunnel authenticates and encrypts traffic from individual applications on compliant devices to the back-end system they are trying to reach.

The Per App Tunnel component and VMware Tunnel apps for iOS, Android, Windows Desktop, and macOS allow both internal and public applications to access corporate resources that reside in your secure internal network. They allow this functionality using per app tunneling capabilities. Per app tunneling lets certain applications access internal resources on an app-by-app basis. This means that you can enable some apps to access internal resources while you leave others unable to communicate with your back end systems.

In this guide we will setup VMware Tunnel in such a way that it directs all traffic bound for Okta through the tunnel. As a result, Okta will be able to infer device and application compliance and trust based on the fact that the traffic is originating from a secure and trusted network.

Deploy VMware Tunnel

For the purposes of this guide we will assume you have deployed VMware Tunnel is a single-tier model and we are only configuring that Tunnel to support Per-App Tunneling. This guide will not cover the Installation of the VMware Tunnel Server and will assume that a VMware Tunnel server is deployed, and externally accessible with firewall rules to allow traffic and DNS entries for name resolution. Refer to this document for a detailed installation guide.

Further this guide will detail, at a high level, the steps required when using a manual installation of a the VMware Tunnel Server on a supported Linux Server (RHEL).

Before starting the next step, you must know the Hostname (or IP Address) and Port of the VMware Tunnel Server.

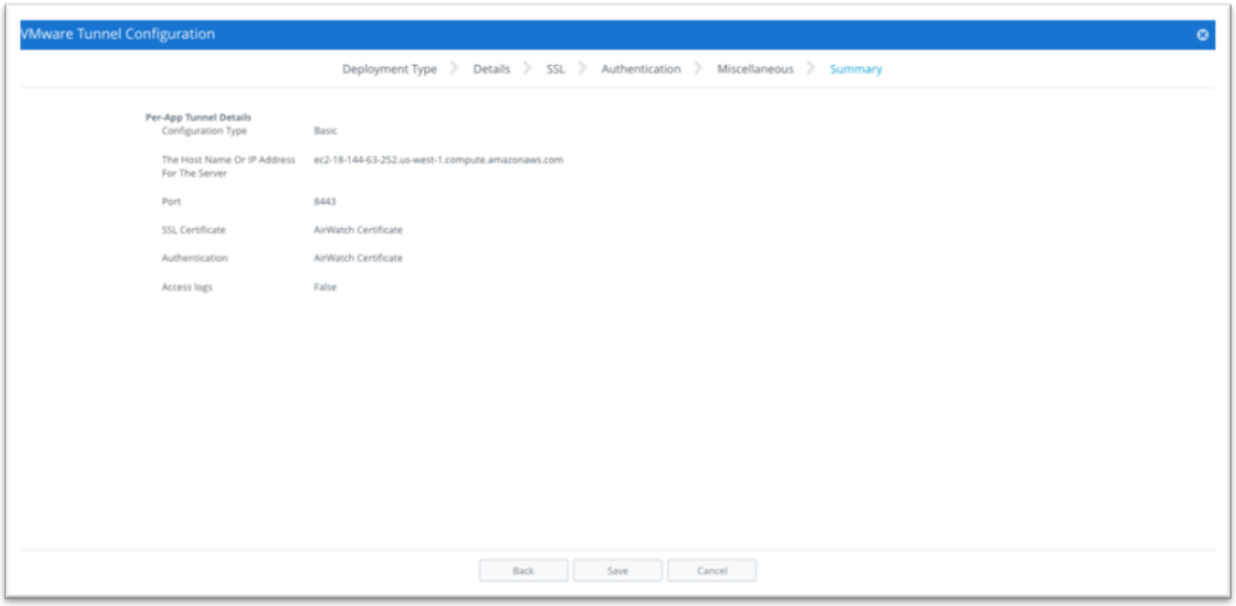
Refer to this documentation to learn more about about VMware Tunnel

Generate Configuration in AirWatch

Login to the AirWatch Console with Console Administrator privileges or other role with the ability to edit the VMware Tunnel page under System.

1. Navigate to **GROUPS & SETTINGS -> All Settings**
2. Expand **System -> Enterprise Integration -> VMware Tunnel**
3. At the bottom of the page click **Configure**
4. Use this table to complete the wizard

Deployment Type	Proxy (Windows & Linux): **Disabled** Per-App Tunnel (Linux Only): **Enabled** Architecture: **Basic**
Details	Hostname: **hostname or ip address of your VMware Tunnel** Port: **Port you wish to use**
SSL	Use Public SSL Certificate: **Unchecked**
Authentication	Per-App Tunnel Authentication: **Default**
Miscellaneous	Access logs: ***Disabled*** ● note: you should turn this on if you have a syslog server available NSX Communication: **Disabled**



5. Click **Save**
6. Click the **Download Configuration XML**
7. Provide a password to protect the certificate (private key) that is a part of the export
   a. Remember this password, it is required to complete the Tunnel Setup later
   b. Save the resulting **vpn_config.xml** file locally
   c. It is uploaded to the VMware Tunnel server in the next step
8. Click **Save**

Upload Configuration to VMware Tunnel Server

Using a file transfer tool upload the **vpn_config.xml** and **VMwareTunnel.bin** files you downloaded to the server which will become the VMware Tunnel server
Example:

scp vpn_config.xml username@hostname:.
scp VMwareTunnel.bin username@hostname:.

Apply Configuration to VMware Tunnel Server

Using an SSH client, connect to the VMware Tunnel Server with a user with root/sudo rights.

Navigate to the directory you uploaded the files to in the previous step and issue the following commands to make the installer file executable and subsequently execute the the installer.

sudo chmod +x VMwareTunnel.bin
sudo ./VMwareTunnel.bin

1. Read and Accept the License agreement
2. Choose the installation type: **2**

```
==============================================================================
Tunnel Installation Setup
-------------------------

    1- Provide API Server Information
    2- Import Config.xml file

Select the installation type: 2
```

3. Choose the features to be installed: **1**

```
==============================================================================
Choose Product Features
-----------------------

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:

    1- [ ] VMware Per-App Tunnel
    2- [ ] VMware Proxy

Please choose the Features to be installed by this installer.: 1
```

4. Provide the **vpn_config.xml** file path

a. Uploaded in the previous step

```
==========================================================================
Per-App Tunnel Config File Path
-------------------------------


  Please provide complete vpn_config.xml file path.

  For Ex: /opt/vmware/vpn_config.xml: /home/ec2-user/download/vpn_config.xml

  You entered /home/ec2-user/download/vpn_config.xml as configurations file

  Is this correct? (Y/N): Y
```

5. Accept the Feature Selection Summary

```
==========================================================================
Feature Selection Summary
-------------------------

Please Review the Following Before Continuing:

Product Name:
    VMware Tunnel

Product Features:
    VMware Per-App Tunnel



PRESS <ENTER> TO CONTINUE:
```

6. Provide the Tunnel Certificate Password
   a. Defined before downloading the **vpn_config.xml** file from AirWatch

```
==========================================================================
Per-App Tunnel Certificate Password
-----------------------------------


  Please provide your Per-App Tunnel Certificate Password:
```

7. Confirm the Firewall Settings

```
==============================================================================
Firewall Settings
-----------------

The Installer detected Firewall is OFF.

   The following ports will be used by VMware Tunnel.

   ( 8443 )

    Press <ENTER> to continue:
```

8. Confirm the Pre-Installation Summary

```
==============================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
    VMware Tunnel

Install Folder:
    /opt/vmware/tunnel

Product Features:
    VMware Per-App Tunnel

Disk Space Information (for Installation Target):
    Required:   67.14 MegaBytes
    Available: 9,620.73 MegaBytes

PRESS <ENTER> TO CONTINUE:
```

9. Begin the Installation

```
==============================================================================
Ready To Install
----------------

InstallAnywhere is now ready to install VMware Tunnel onto your system at the
following location:

   /opt/vmware/tunnel

PRESS <ENTER> TO INSTALL:


==============================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]
```

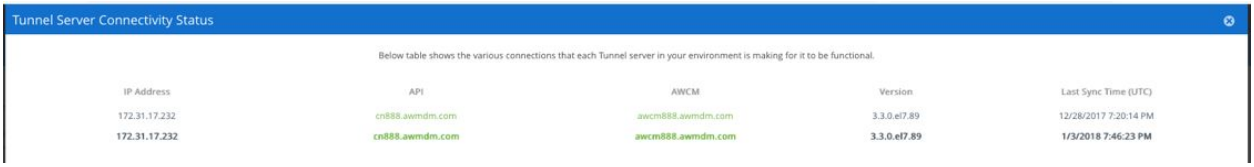
10. Complete the Installation

```
==============================================================================
Installation Complete
---------------------

Congratulations. VMware Tunnel has been successfully installed to:

/opt/vmware/tunnel

Installer logs have been installed to:

/opt/vmware/tunnel/_tunnel_installation/Logs

PRESS <ENTER> TO EXIT THE INSTALLER:
```

Confirm VMware Tunnel Function

After completing the installation, you can return to the AirWatch console to verify connectivity with the
VMware Tunnel Server.

1. Navigate to **GROUPS & SETTINGS -> All Settings**
2. Expand **System -> Enterprise Integration -> VMware Tunnel -> Configuration**
3. Click the **Test Connect** button
4. The Tunnel Server Connectivity Status screen will display the current status and details



Configure Device Policy

The following subsections will configure AirWatch so it will direct traffic destined for Okta through the newly deployed tunnel, Deploy the required VMware Tunnel app and then apply an assignment policy to a sample application to enforce the traffic rules.

Refer to this documentation to learn more about about Per-App Tunneling

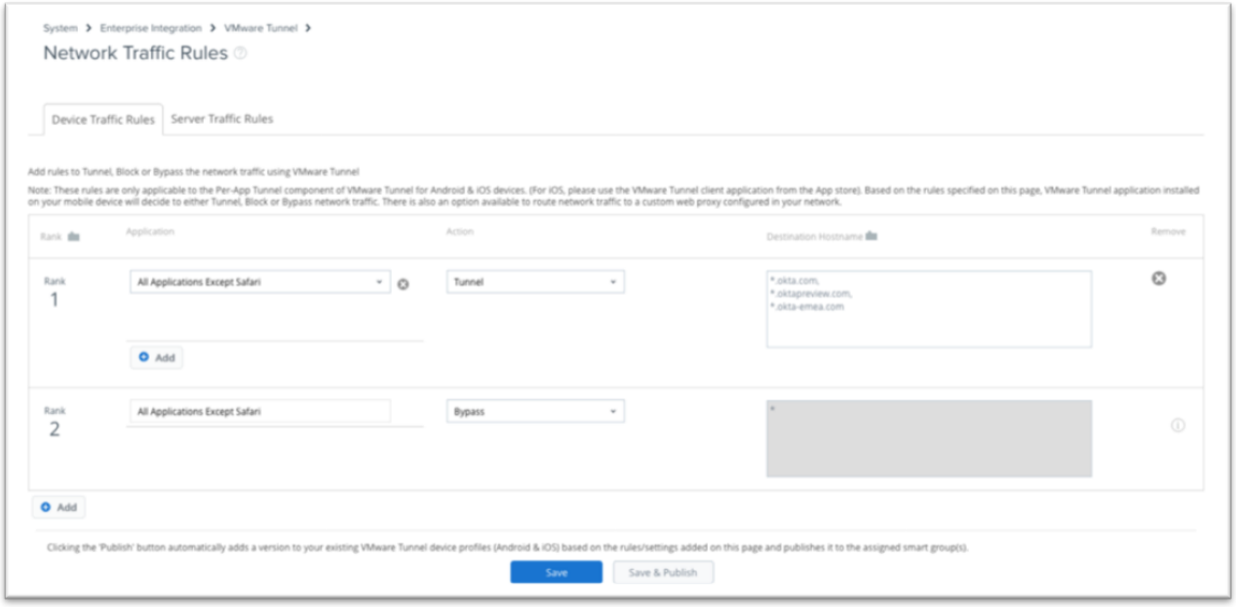
Configure Tunnel Network Traffic Rules

This section will discuss the process of configuring AirWatch to direct traffic for selected applications.

With the VMware tunnel server now functional we will create a Device Traffic Rule to direct traffic bound for Okta through the tunnel.

To complete these steps login to the AirWatch Console with Console Administrator privileges or other role with the ability to edit the VMware Tunnel page under System.

1. Navigate to **GROUPS & SETTINGS -> All Settings**
2. Expand **System -> Enterprise Integration -> VMware Tunnel -> Network Traffic Rules**
3. Add a new rule in the Device Traffic Rules tab
    a. Application: **All Applications Except Safari**
    b. Action: **Tunnel**
    c. Destination Hostname: ***.okta.com, *.oktapreview.com, *.okta-emea.com**



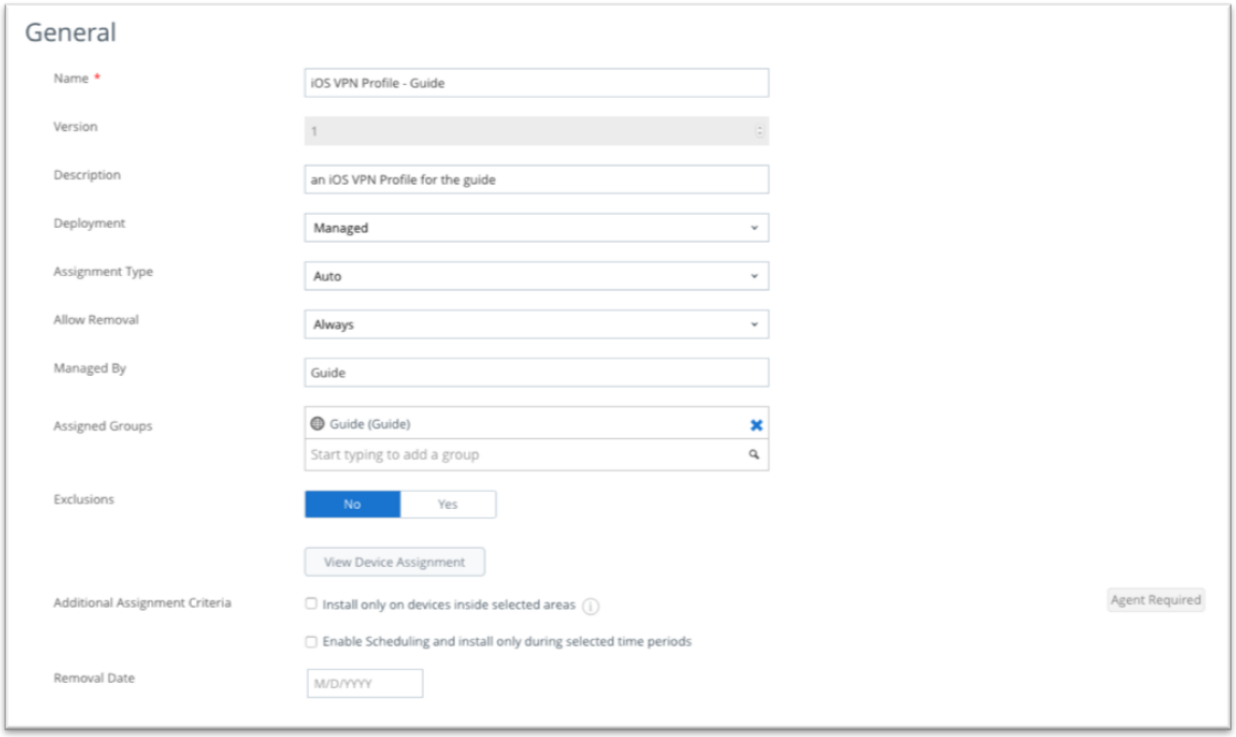
4. Click Save & Publish

Note: If you have other policies or want to have different destination rules on a per application by application basis you can define more granular rules.

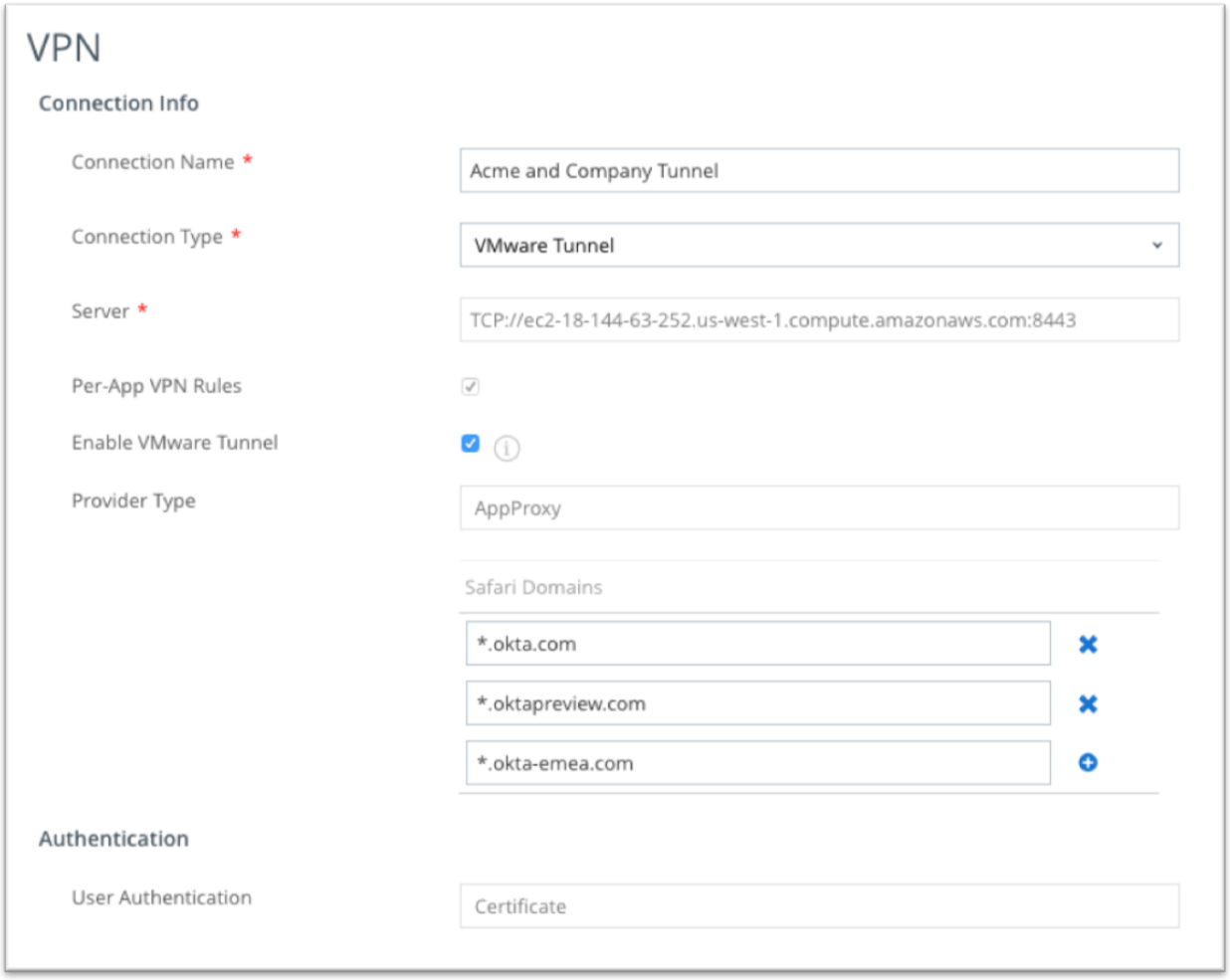
Create a iOS VPN Profile

In this next step we will create a device profile that configures a VPN for iOS pointing to the VMware Tunnel Server we have previously configured.

1. Navigate to **Devices -> Profiles & Resources -> Profiles**
2. Click the **Add** button and select **Add Profile**
    a. Select a platform to start: **iOS**
        - *Repeat for additional platforms as required*
3. General
    a. Name: ***iOS VPN Profile***
    b. Assigned Groups: ***Guide (Guide)***
        - Select the assignment group you desire to target
    c. Other settings as required by your environment



4. VPN
    a. Select **VPN** from the left navigation menu
    b. Click **Configure**
    c. Connection Name: ***provide a distinct and appropriate name***
    d. Connection Type: **VMware Tunnel**
    e. Server: ***Select the Server previously configured***
    f. Per-App VPN Rules: **Checked**
    g. Enable VMware Tunnel: **Checked**
    h. Provider Type: **AppProxy**
    i. Safari Domains: (optional but causes Safari to send traffic for Okta through this Tunnel)
        - *.okta.com
        - *.oktapreview.com
        - *.okta-emea.com
    j. User Authentication: **Certificate**



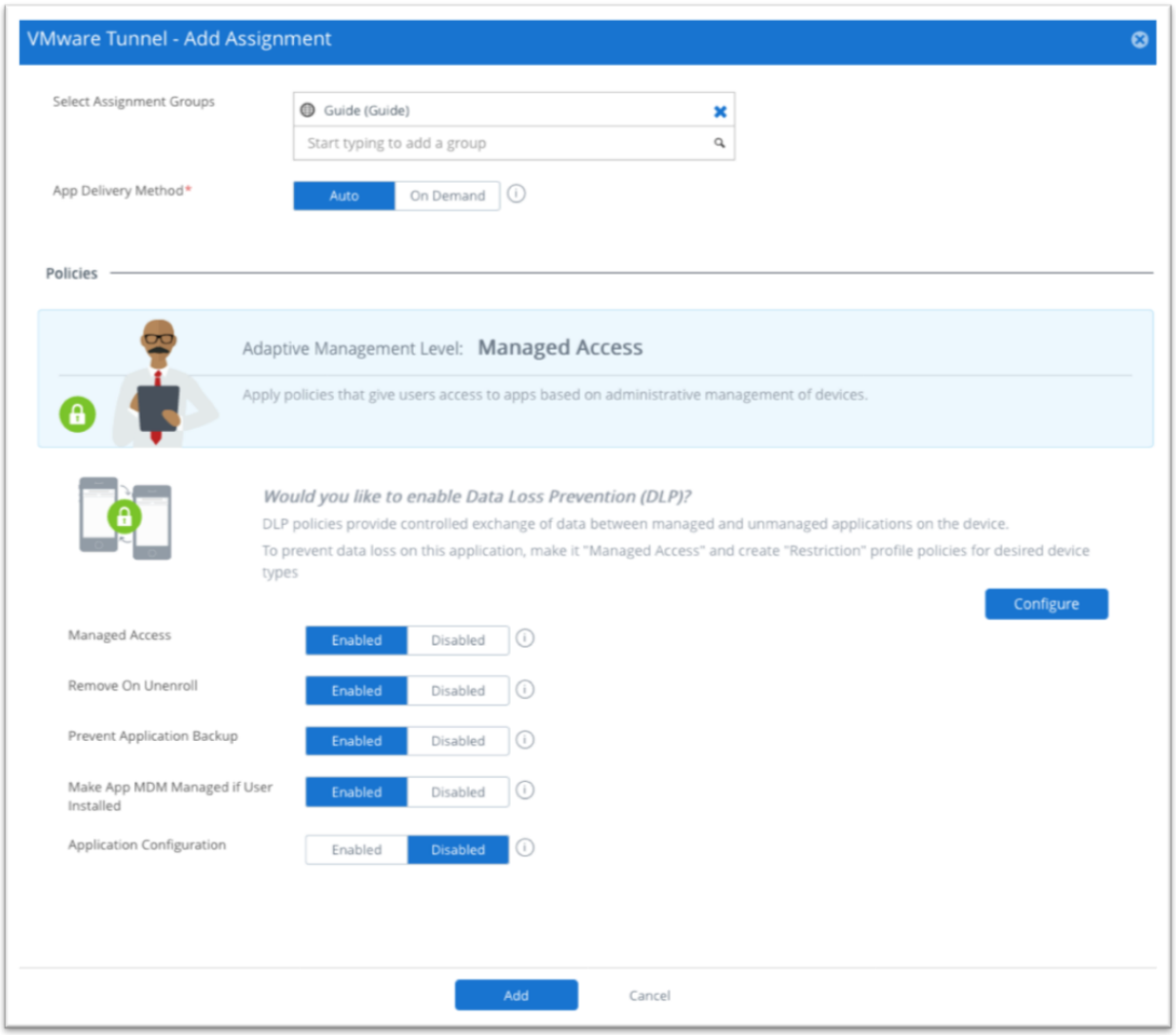
5. Click **Save & Publish**
6. Confirm the Device Assignment Summary and click **Publish**

Create app Assignment to deploy VMware Tunnel App

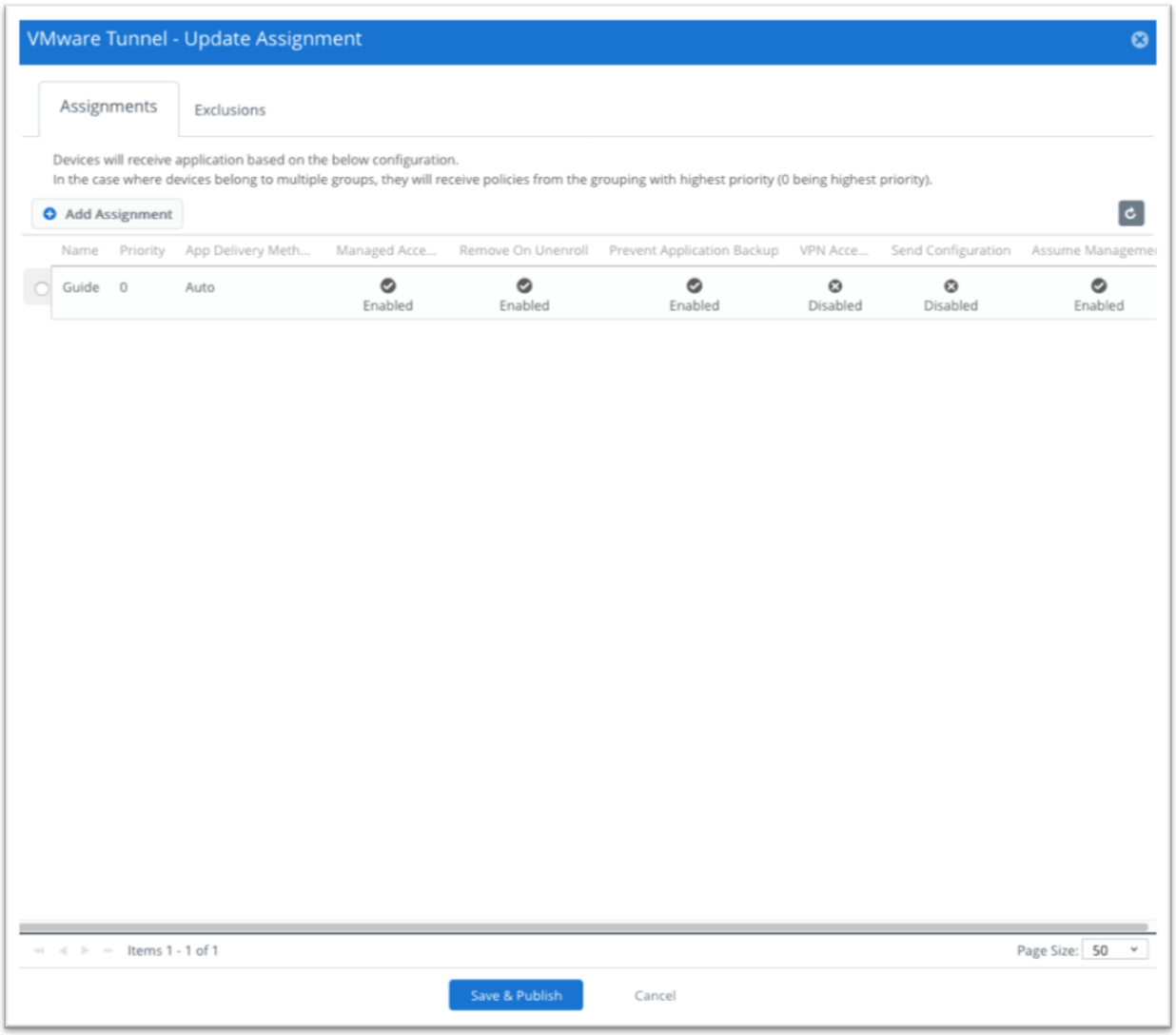
In this step we will deploy the required VMware Tunnel App to our desired users/devices

1. Navigate to **Apps & Books -> Applications -> Native -> Public**
2. Click the **Add Application** button
    a. Platform: ***Apple iOS*** (repeat for additional platforms)
    b. Source: **Search App Store**
    c. Name: **VMware Tunnel**
    d. Click **Next**
    e. Click **Select** for the **VMware Tunnel** from the search results
    f. Click **Save & Assign**
3. In the Assignments window click on **Add Assignment**
    a. Select Assignment Groups: **Guide**
    b. App Deliver Method: ***Auto***
    c. Managed Access: ***Enabled***
    d. Remove on Unenroll: ***Enabled***
    e. Prevent Application Backup: ***Enabled***

f. Make App MDM Managed if User Installed: ***Enabled***



4. Click **Add**
5. *Repeat as required*



6. Click **Save & Publish**
7. Confirm the Assigned Devices and click **Publish**

Create or Modify app Assignment to use our VPN Profile

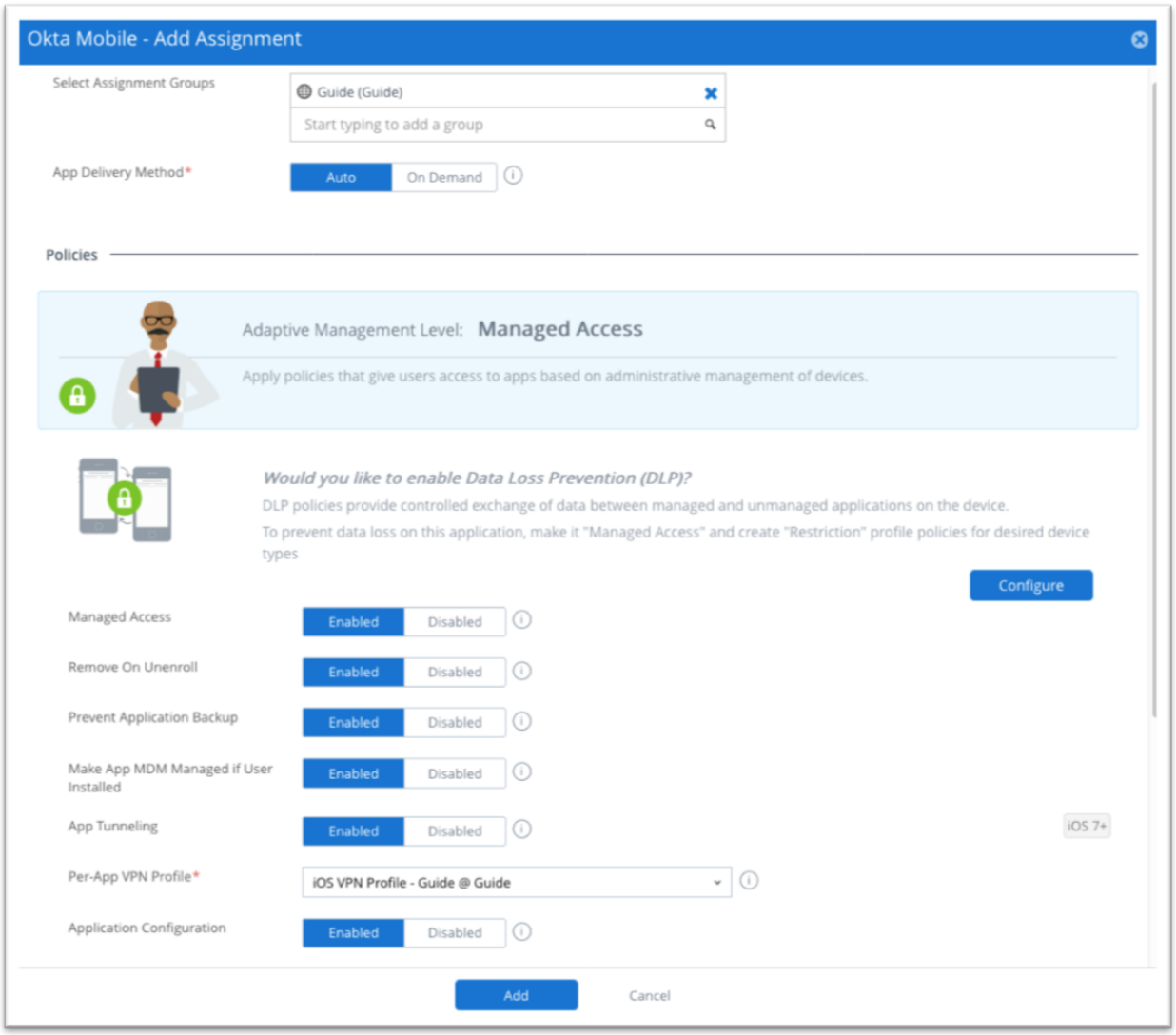
In this final step we will assign a managed application and configure VPN Access for that the assignment of that app.

This step ties together the *application assignment -> VPN Profile -> Tunnel Traffic Rules* and VMware Tunnel Server configuration.

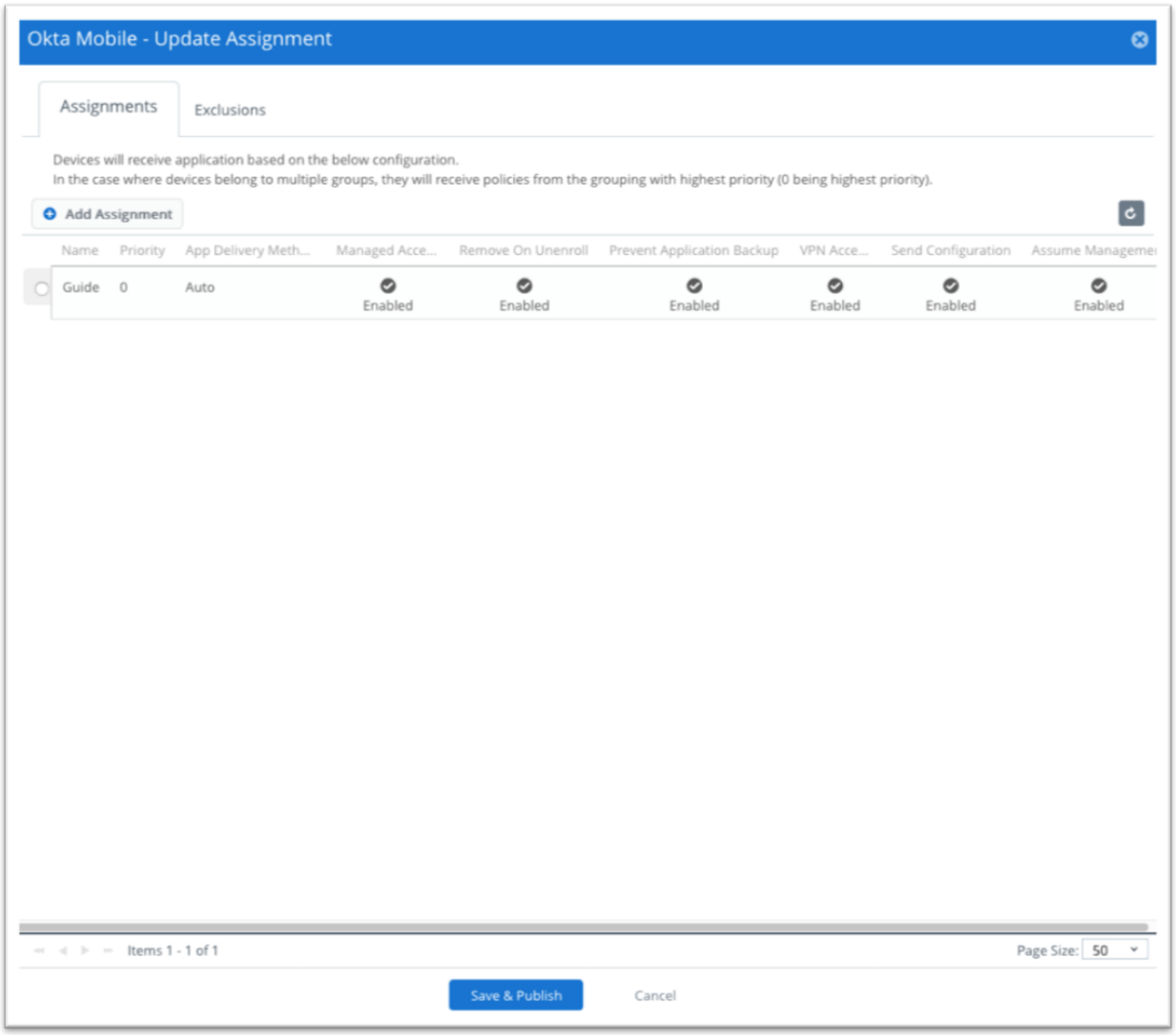
1. Navigate to **Apps & Books -> Applications -> Native -> Public**
2. Locate and click on the desired application (this guide will use ***Okta Mobile***)
3. Click on the **Assign** button in the top right-hand corner
4. In the Assignments window click on **Add Assignment**
    a. Select Assignment Groups: **Guide**
    b. App Deliver Method: ***Auto***

c. Managed Access: ***Enabled***
d. Remove on Unenroll: ***Enabled***
e. Prevent Application Backup: ***Enabled***
f. Make App MDM Managed if User Installed: ***Enabled***
g. Per-App VPN Profile: **Enabled**
h. Application Configuration: ***optional***
i. Settings specific to Okta Mobile

name	**type**	**value**
managementHint	String	YES
siteName	String	*youOktaOrg.com*
Username	String	*{UserPrincipalName}*



j. Click **Add**
k. Repeat as required



5. Click **Save & Publish**
6. Confirm the Assigned Devices and click **Publish**

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 VMware Tunnel appliance is authenticated using a device certificate that is issued by AirWatch and revoked by AirWatch 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 VMware Tunnel is using a trusted device.

See IP Zones to create a new network zone with the egress IP address of your VMware 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 VMware Tunnel or other trusted VPN traffic.

Custom Login Pages in Okta

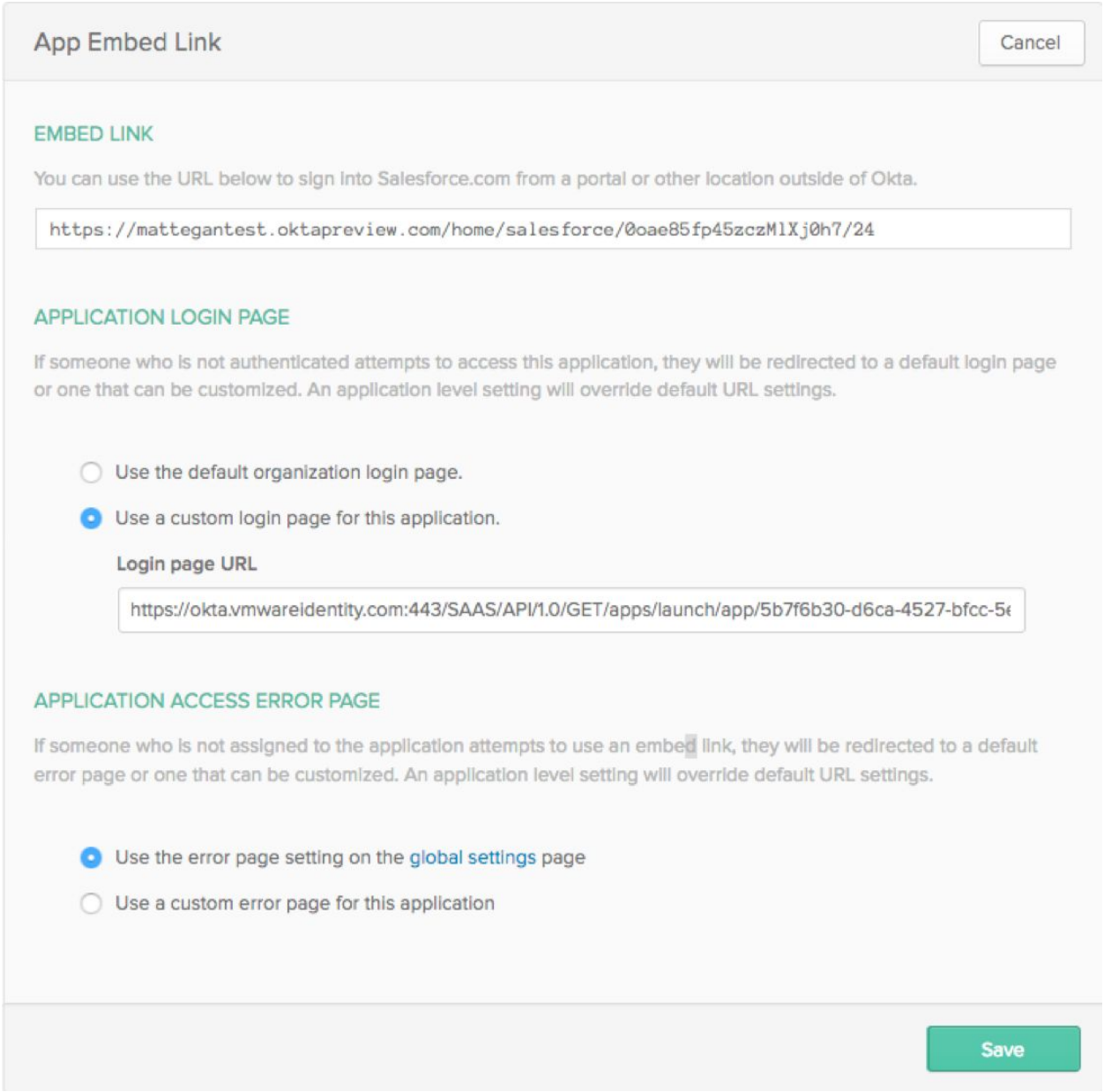
To provide customers a solution that is generally available the use of custom login pages for applications can be used to direct all authentication for a specific application in Okta to Workspace ONE, for this to work correctly you must also Modify the relaystate for Workspace ONE to allow it to retrieve details about the application a user is trying to access so it can return the user.

For generalized instructions review the **Redirect unauthenticated users to a custom login page** in our The Applications Page product guide

In this section we will describe how to configure an Okta application to use a custom login page. When integrating with Workspace ONE this is a creative way to selectively direct logins for a specific application to Workspace ONE. Until IdP discovery is Generally Available, consider this a viable solution.

Login to the Okta admin UI with Administrator privileges or any other role entitled to modify an application.

1. Navigate to **Applications -> Applications**
2. Locate and click on the application of interest
3. Navigate to the **General** tab of the application sub menu
4. Scroll to the **App Embed Link** section and click **Edit**
5. In the **Application Login Page** section Select **Use a custom login page for this application**
6. Enter the URL in the **Login Page URL** box
    a. Note: see Retrieve Launch URL from Workspace ONE to identify the IdP Launch URL



7. Click **Save**

Modify the relaystate for Workspace ONE

When leveraging Custom Login Pages in Okta to direct authentication for an application to Workspace ONE an administrator will also need to modify the configuration of **SAML 2.0 Web Application** you've created in Workspace ONE for Okta.

These steps will guide you through changing the relay state parameter name used by Workspace ONE from relaystate to fromURI.

See Configure Workspace ONE to use a custom RelayState Param in Okta in Workspace ONE as IdP to Okta

When you configure a custom login page in Okta and direct it to Workspace ONE use these steps to extract the appropriate artifacts from the login request to allow Workspace ONE to return the user to the originally requested application in Okta.

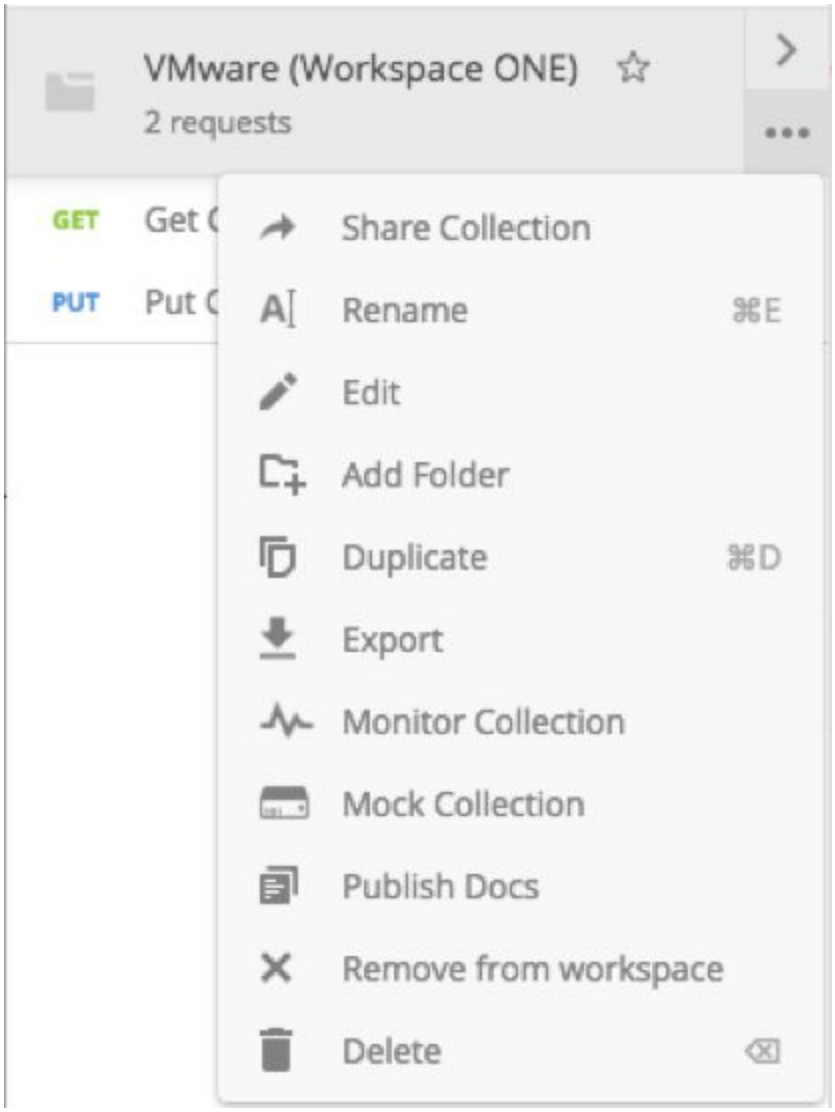
The steps make use of a tool called postman, they could equally be performed with tools like Powershell's Invoke-Webrequest cmdlet or curl.

Download and Install postman from https://www.getpostman.com

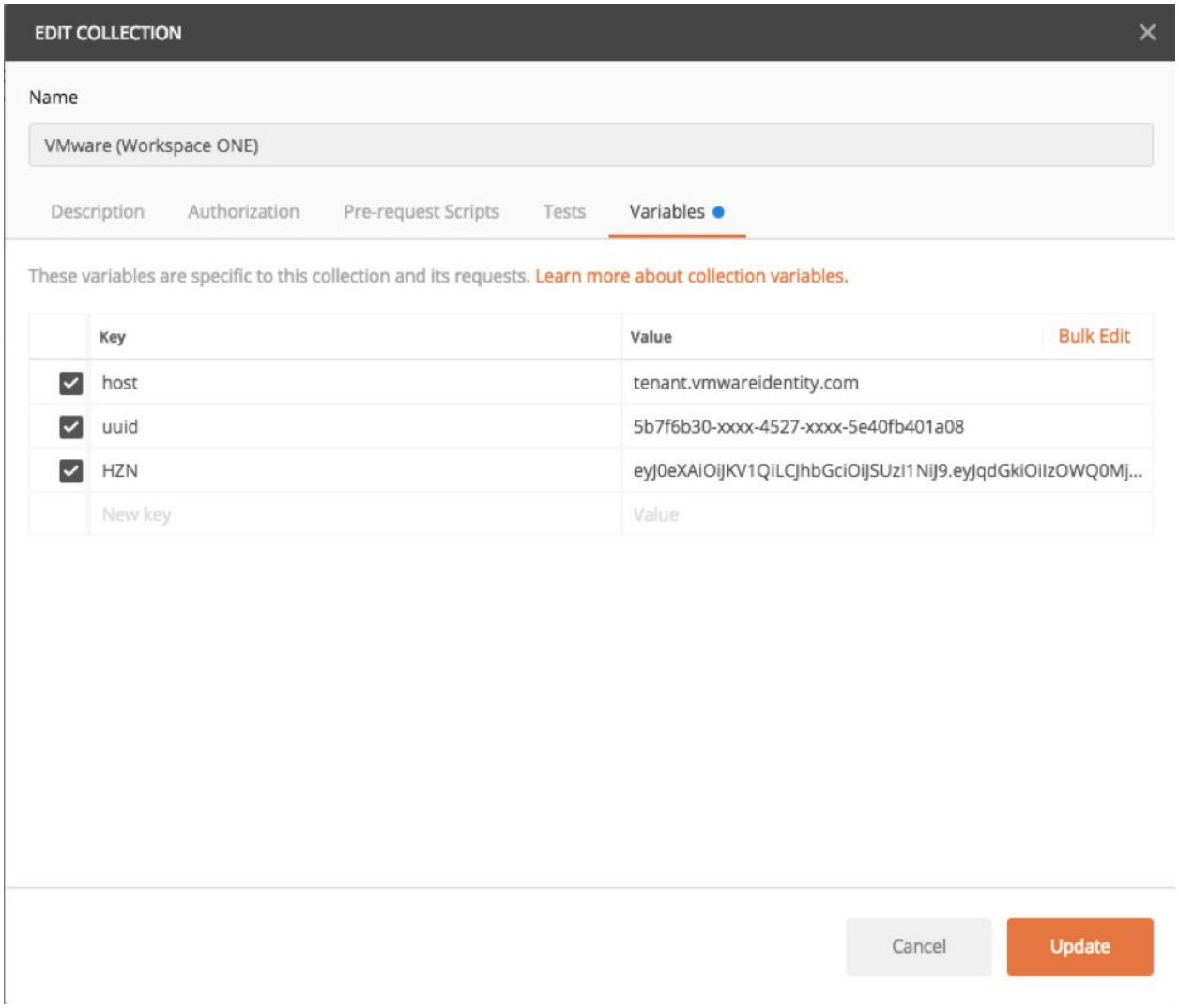
Download and install this custom postman collection

Perform updates using Postman

1. Open **Postman**
2. Click the **Import** button
3. Click **Choose Files** and navigate to the custom postman collection file you downloaded
4. Click on the **…** on the bottom right hand corner of the imported collection



5. Click **Edit**
    a. Click on the **Variables** tab
    b. Provide values for the variables
        - **host**: the hostname of your Workspace ONE server
        - **uuid**: the UUID from the launch URL for the Workspace ONE app you want to modify
            - Refer to Retrieve Launch URL from Workspace ONE for more info
        - **HZN**: Get a session cookie value from Firefox
            - Using Firefox login to Workspace ONE as an administrator
            - Right click -> View Page Info
            - Select Security Tab
            - Click View Cookies button
            - Locate the HZN cookie
            - Copy the Content
                a. Triple click, this is a long string value ~1500 char



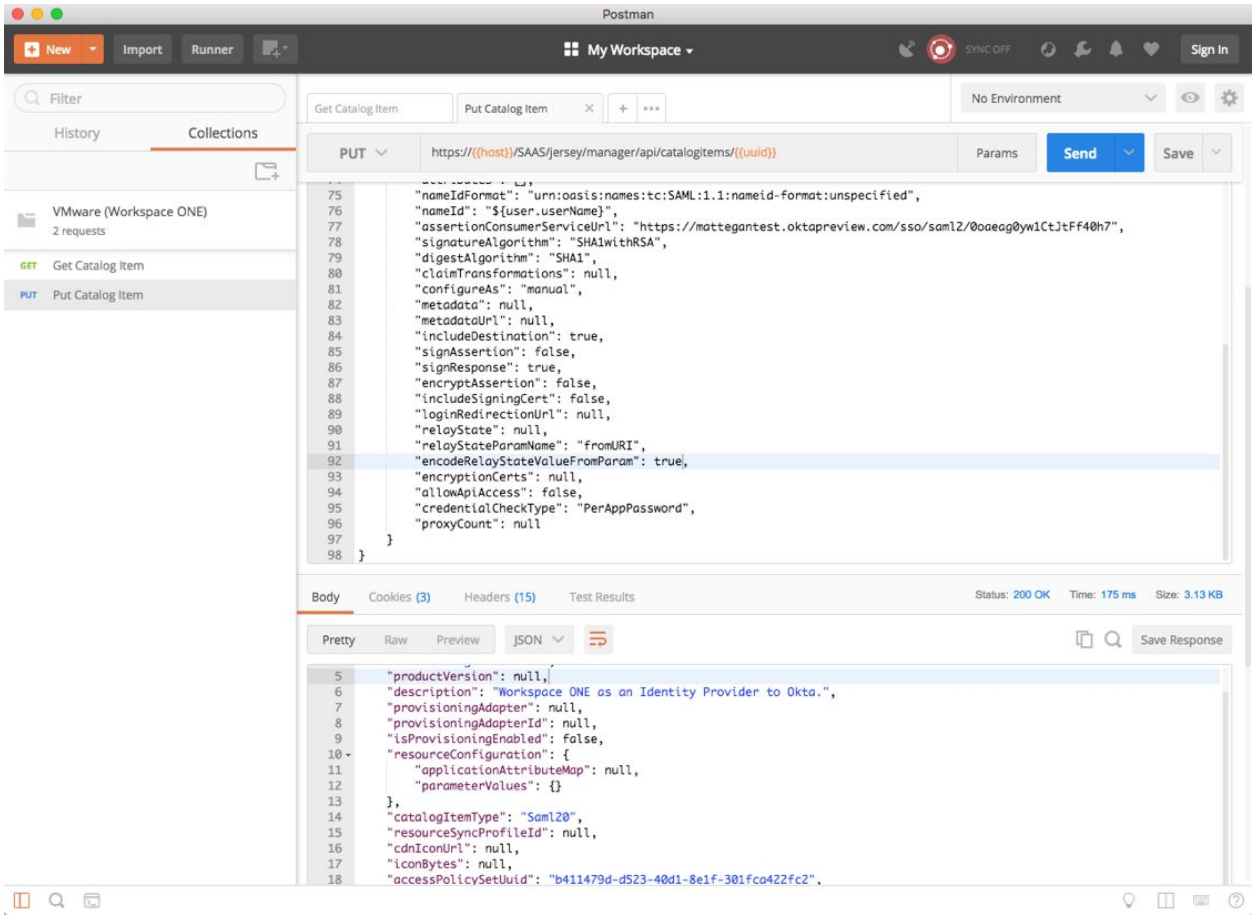
   c. Click Update
6. Select the **Get Catalog** Item from within the collection
7. Click **Send**
8. Review the response
   a. You should see the name and description matching what you see in the Workspace ONE admin UI for this application
9. Copy the response body
10. Select the **Put Catalog Item** from within the collection
11. Select **Body** from the sub menu
12. Select **Raw**
13. Paste the content from the previous step
14. Scroll through the json payload and locate the **relayStateParamName** and **encodeRelayStateValueFromParam**
15. Change the values from **null** and **false** to **fromURI** and **true** respectively

Before	After

```
"loginRedirectionURL": null,
"relayState": null,
"relayStateParamName": null,
"encodedRelayStateValueFromParam": false,
"encryptionCerts": null,
"allowApiAccess": false,
```

```
"loginRedirectionURL": null,
"relayState": null,
"relayStateParamName": "fromURI",
"encodedRelayStateValueFromParam": true,
"encryptionCerts": null,
"allowApiAccess": false,
```

16. Click **Send**
17. Confirm the Response **Status** is 200 OK

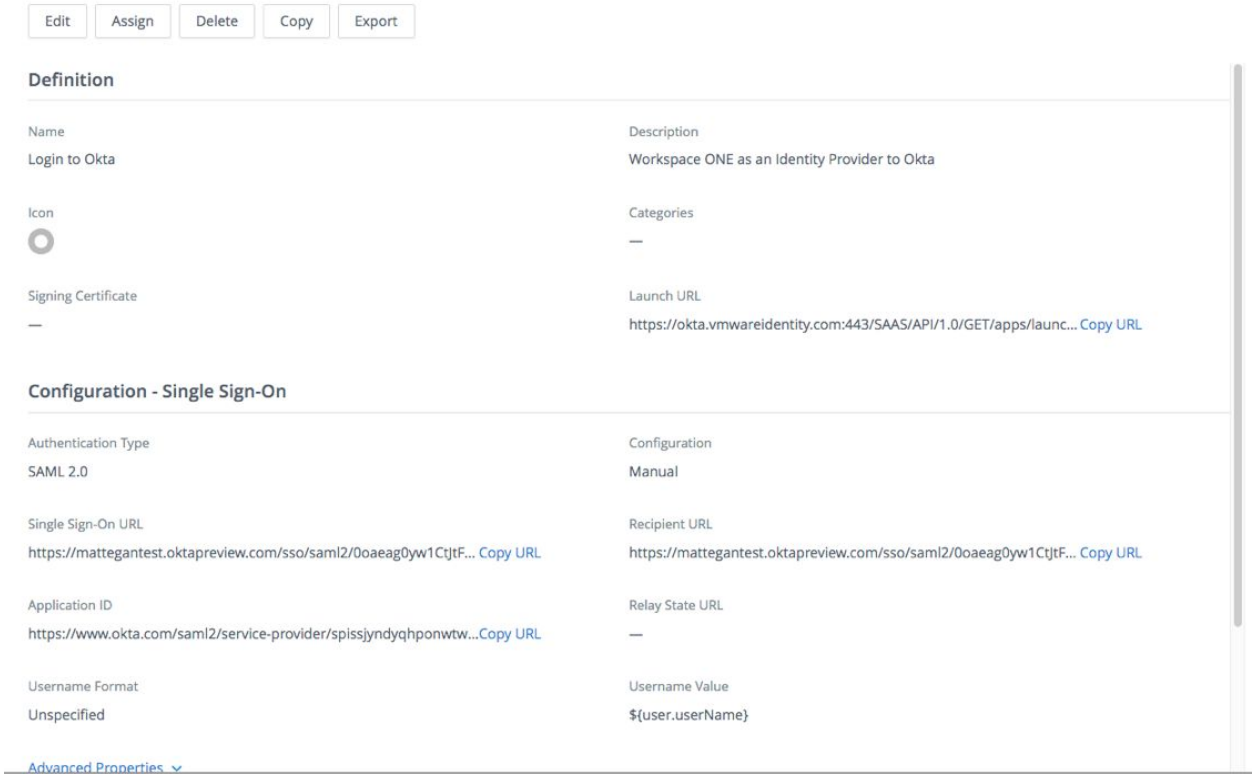


Retrieve Launch URL from Workspace ONE

In this section we'll detail the steps required to retrieve the Launch URL for an application in Workspace ONE. This step will be used if you need to Modify the relaystate for Workspace ONE or want to Access a Workspace ONE application from Okta.

Login to the Workspace ONE Administration Console with Administrator privileges or any other role entitled to add a New SaaS Application.

1. Click the **Catalog -> Web Apps** tab
2. Locate your application of interest and click on its title
3. Locate the **Launch URL**



4. Click the **Copy URL**

5. The **Launch URL** is now copied to your clipboard

Create Bookmark applications in Okta

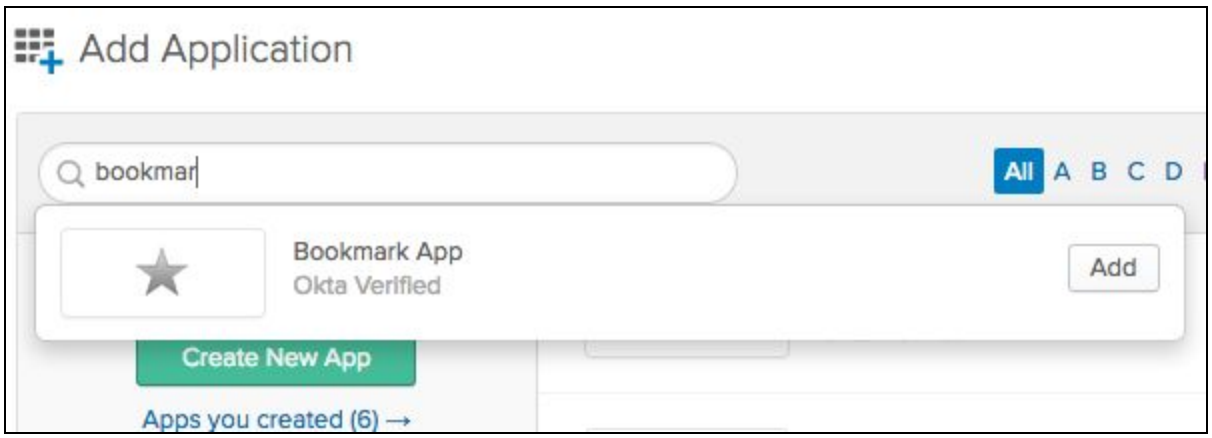
Follow these steps to create a bookmark application in Okta.

A bookmark application is an application that serves to simply direct users to a URL without any sort of authentication. Beyond the obvious value of sharing bookmarks, these apps can be used to trigger service provider (SP) initiated SAML authentication flows. In this guide we will use bookmarks when we setup Okta as Federation Provider to Airwatch as well as when we want to Access a Workspace ONE application from Okta.

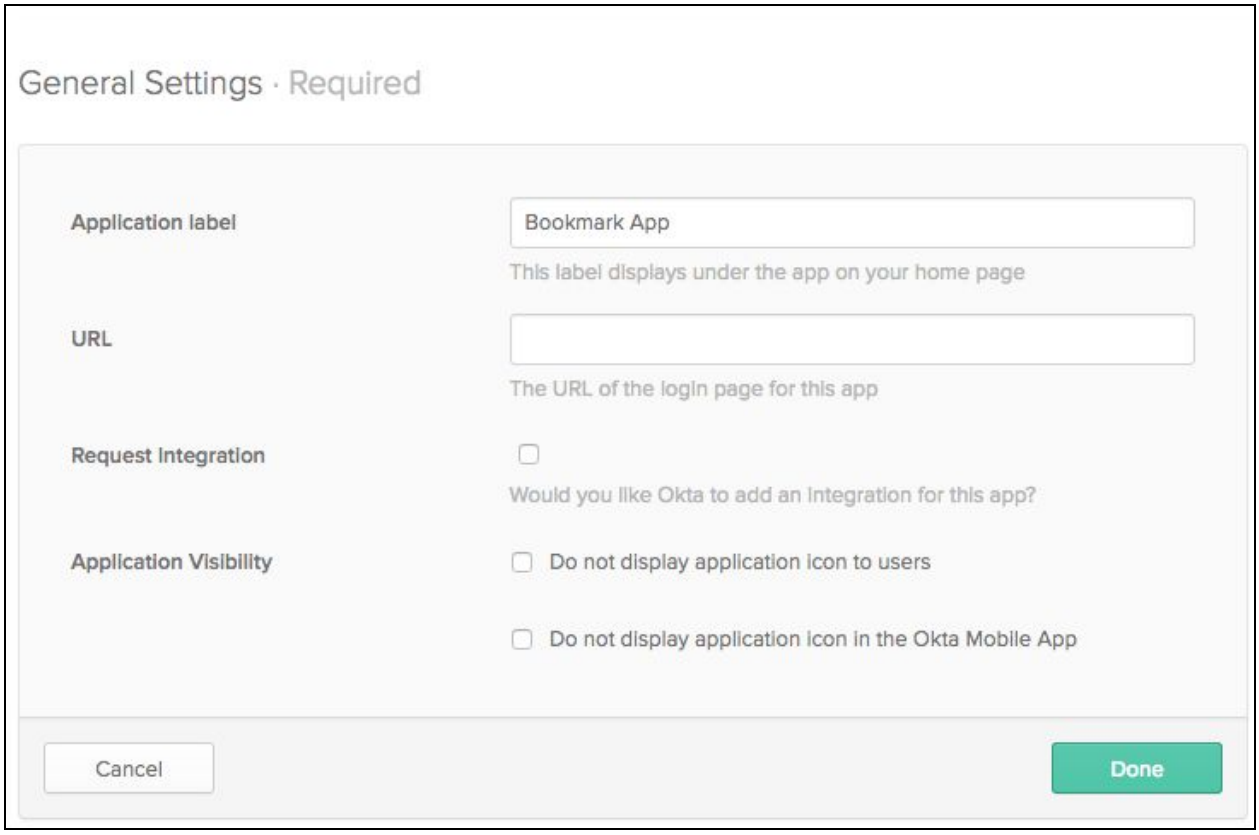
Sign into Okta as an administrator with privileges sufficient to create new applications.

1. Navigate to **Applications -> Applications**
2. Click **Add Application**

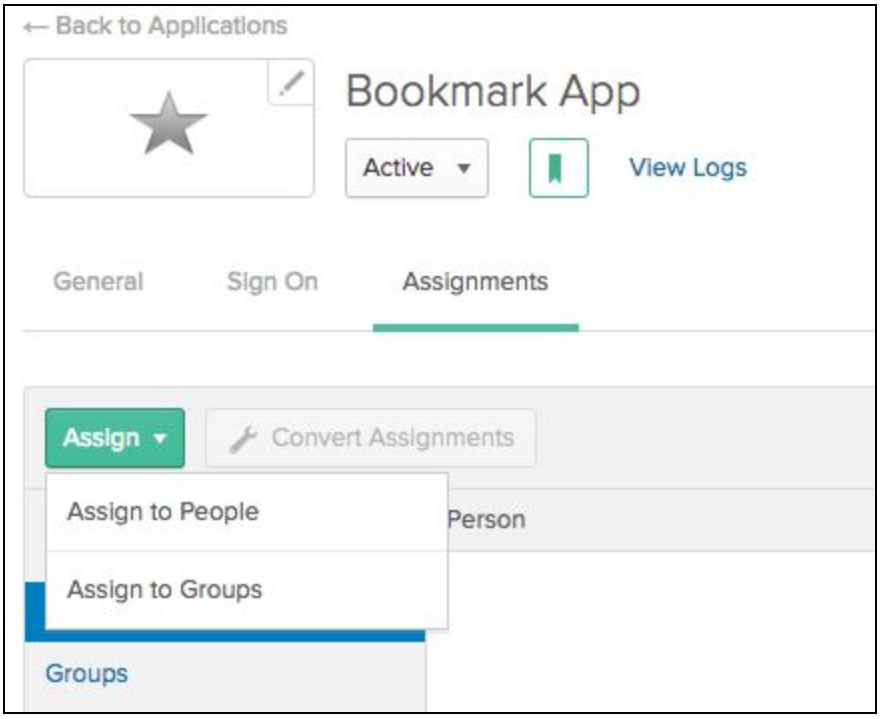
3. Search for **Bookmark App**
4. Click **Add**



5. Provide an appropriate **Application Label**
6. Provide the target **URL**



7. Click **Done**
8. Click on the **Assignments** sub-menu
9. Click the **Assign** button
10. Assign the app to the appropriate **People** or **Groups**



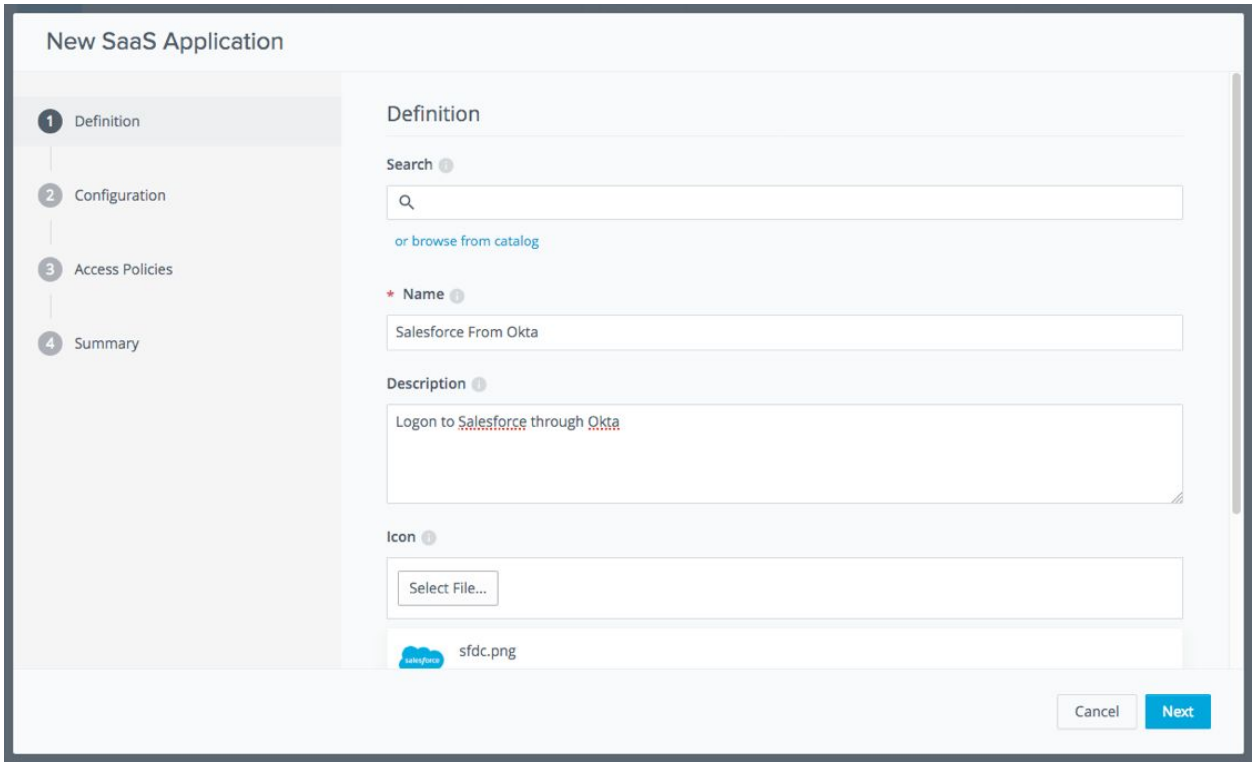
Access an Okta application from Workspace ONE

In order to provide consistent access experiences for users while still leveraging the appropriate platform to suit your technical requirements you can use the instructions in this section to surface Okta applications to your users in their Workspace ONE portal.

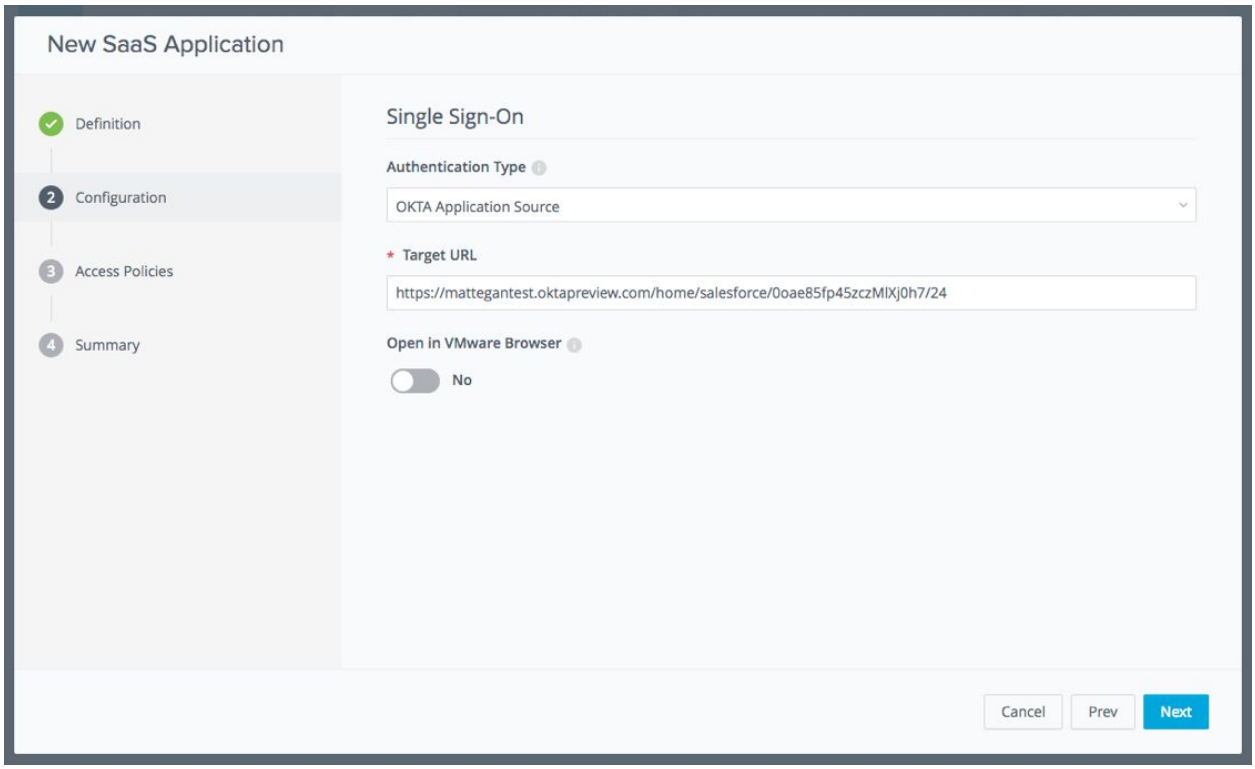
If you've configured the OKTA Application Source in Workspace ONE you can follow these steps to add an application from Okta to your users Workspace ONE portal.

Login to the Workspace ONE Administration Console with Administrator privileges or any other role entitled to add a New SaaS Application

1. Click the **Catalog -> Web Apps** tab
2. Click **New**
3. Provide a Name
4. Optionally provide a Description
5. Optionally select an Icon
6. Optional select a Category



7. Click **Next**
8. Authentication Type: **OKTA Application Source**
9. Target URL: **Okta App Embed link**
    a. Example: *https://yourOktaOrg/home/salesforce/0oae85fp45zczNlYa0h7/24*
    b. See **Show application embed links** from Okta's [The Applications Page]() documentation
10. Open in VMware Browser: **No**



11. Click **Next**
12. Assign an Access Policy

13. Click **Next**
14. Click **Save**
15. Optionally assign the new SaaS application to users and groups as required

When a user clicks on one of these applications in Workspace ONE it will send an Identity Provider (IdP) Initiated SAML Authentication Response to Okta with a RelayState value of the Okta Embed link causing Okta to inturn send an IdP initiated SAML Authentication Response to the target Service Provider.

Access a Workspace ONE application from Okta

In order to provide consistent access experiences for users while still leveraging the appropriate platform to suit your technical requirements you can use the instructions in this section to surface Workspace ONE applications in Okta.

1. Retrieve the Launch URL of the Workspace ONE application
2. Get the SAML URL of the Workspace ONE application in Okta
3. Do some stuff to combine the 2 URLs (okta app url + launch url)
4. Create a bookmark Application in Okta using the result of step 3
5. Assign the bookmark Application to the intended audience

When a user clicks this it will cause Okta to send a SAML Authentication Response to the Workspace ONE SAML ACS with a RelayState containing the Launch URL for the Workspace ONE application

---

Conditional Access Policies in Workspace ONE

Assumes existing integration of Workspace ONE and AirWatch, review x y z guide from VMware to configure

High level notes about what is possible and how we might suggest they do this and send them to VMware docs

---

References

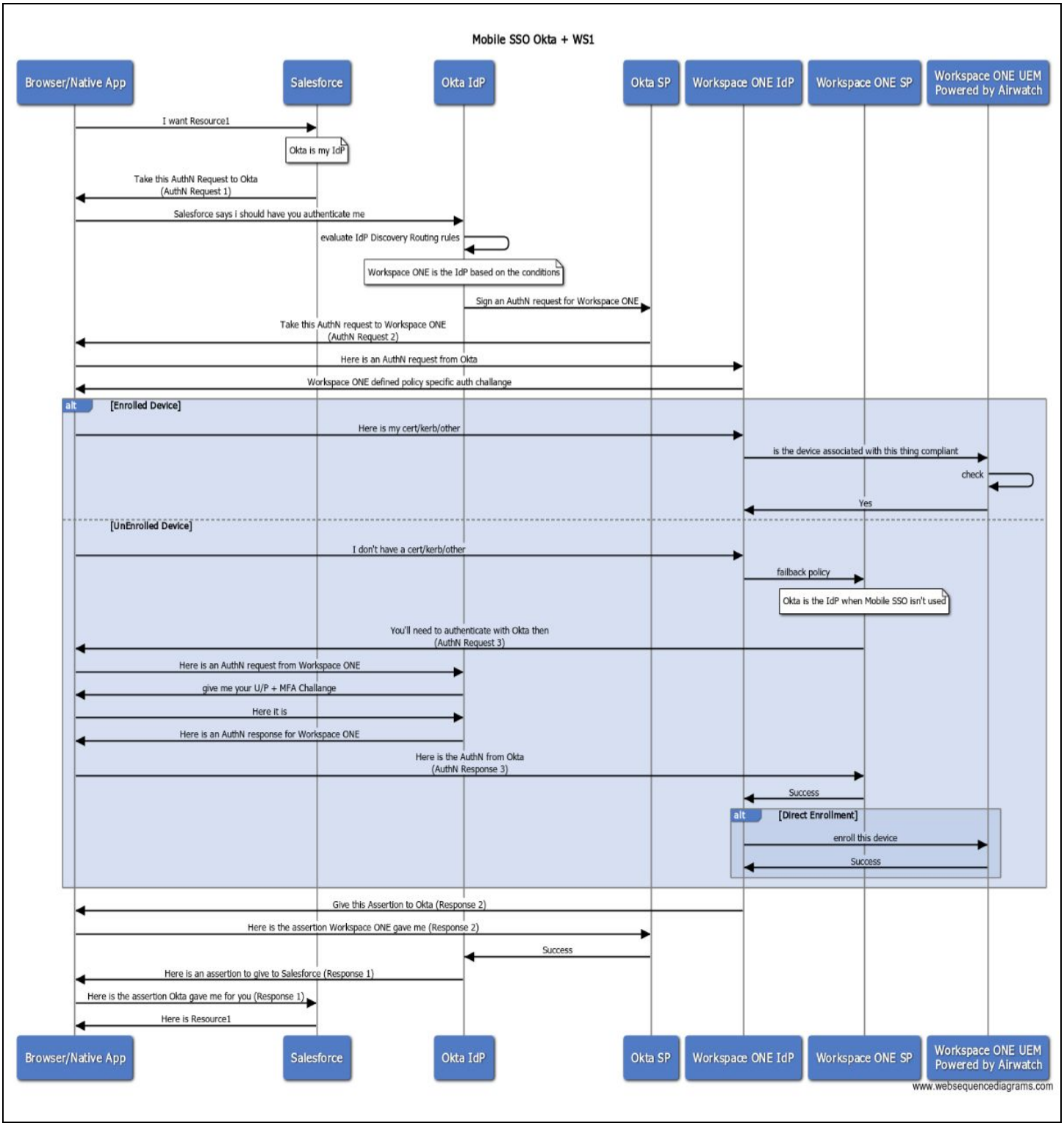
Links to relevant material from Okta where appropriate but most probably links to good VMware docs

Owner	Details	Link
VMware	REVIEWERS GUIDE – NOVEMBER 2017 REVIEWER'S GUIDE FOR CLOUD-BASED VMWARE WORKSPACE ONE: MOBILE SINGLE SIGN-ON	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-workspace-one-airwatch-reviewers-guide-mobile-SSO.pdf
VMware	Product Documentation for AirWatch v9.2	https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm
VMware	Implementing Mobile Single Sign-in Authentication for AirWatch-Managed iOS Devices	https://docs.vmware.com/en/VMware-Identity-Manager/3.1/aw-vidm-ws1integration-/GUID-3EC86F69-6F6E-4C48-A5D9-F319562B6B9C.html
VMware	Implementing Mobile Single Sign-On Authentication for AirWatch-Managed Android Devices	https://docs.vmware.com/en/VMware-Identity-Manager/3.1/aw-vidm-ws1integration-/GUID-1E5128A5-1394-4A50-8098-947780E38166.html
VMware	Datasheet - VMware Workspace ONE Consumer Simple. Enterprise Secure	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/workspace-one/vmware-workspace-one-datasheet.pdf

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



IdP Initiated - User accessing SaaS application from Workspace ONE app