

OKTA Integration with Workspace ONE Access

Scenario and Objectives of this Lab Module

We will come into to many existing environments and they will already have existing Federations in place. We will see what is required when the customer has **OKTA** Federated with existing Applications.

OKTA sees **Workspace ONE Access** as their go to market solution for cross-platform SSO solutions and have officially deprecated the MDM component in favour of using Workspace ONE

In this scenario **OKTA** could be the first point of call and we would use **Workspace ONE Access** to authenticate and provide SSO access to mobile devices and **Workspace ONE UEM** to manage compliance

Please note we will complete the testing of this lab in the latter part of this course once we have **Mobile SSO for Android** and **Mobile SSO for IOS** for **Workspace ONE Access**.

This lab is comprised of 5 parts

Part 1. Configuring an **OKTA** individual developer account.

Part 2. Federating **OKTA** with **Workspace ONE Access**.

Part 3. Federating **BambooHR** with **OKTA**.

Part 4. Configuring **Workspace ONE Access** to be an **OKTA** application source.

Note! After we have setup Single Sign On for Android and IOS. We will then Configure Conditional Access policies in Workspace One UEM, then we will test the integrations for SSO through **OKTA**, **VMware Identity Manger** and **Workspace ONE UEM**.

Just a reminder that when creating custom Accounts. Be sure to write down the exact details related to this account. One suggestion might be to standardize on passwords and keep the password as simple as possible, to ensure success of these labs. In the future if you have concerns related to accessing these accounts feel free to reset the passwords.

Failure to follow these guidelines could result in being locked out of your tenant and you would then have to take for responsibility for regaining access leading to a loss of time.

Part 1. Setting up an OKTA Overview free trial

1. Setting up an OKTA Overview free trial (PART 1)

- In this section we will register a 30 day free trial with OKTA account that we will use for this lab. It can be used beyond the scope of this lab as well and does not expire.

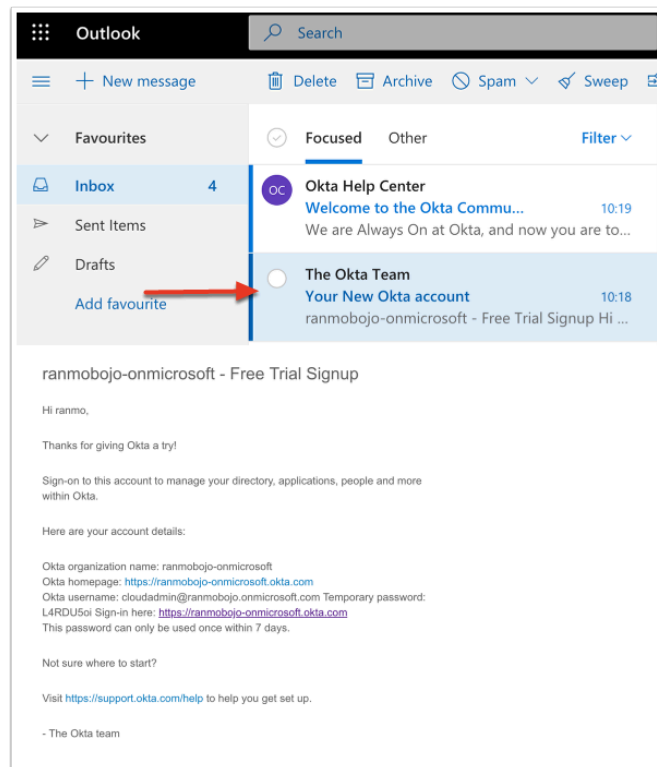
1. Open your **Chrome Browser** on the Control Center and browse to <https://www.okta.com/free-trial/#> On the **START YOUR 30 DAY FREE TRIAL WITH OKTA TODAY** page select **SIGN UP TODAY**
2. Fill in the **Free Trial** Form
 1. Using either a **work e-mail address** or your **custom office365 CloudAdmin email account** eg. **cloudadmin@ranmobojo.onmicrosoft.com**. Fill in your **first** and **last name**
 - **Do not use a EUC-Livefire.com email address.**
 2. In the drop down **Would you like more information about the trial?** select **Yes....**
 3. In the phone area type a valid phone number
 4. Under Employee count select a one the numbered check boxes
3. Select **Get Started**
4. Notice you have a **Thank You for registering. Welcome to the family.** NB! NOTE the url and save your unique URL to notepad e.g. [ranmobojo-onmicrosoft.okta.com](https://www.okta.com/ranmobojo-onmicrosoft.okta.com)

The screenshot displays the Okta Free Trial registration process in four numbered steps:

- Step 1: START YOUR 30 DAY FREE TRIAL WITH OKTA TODAY**. This section highlights benefits: 20 minutes to configure new applications, 90% of staff using Okta within two weeks, and \$3M+ of productivity. A red box highlights the **Sign Up Today** button.
- Step 2: Free Trial**. This is the registration form. It includes fields for email (cloudadmin@ranmobojo.onmicrosoft.com), first name (ranmo), last name (bojo), a dropdown for 'Would you like more information about the trial?' (set to 'Sure, let's talk now'), a phone number (+447943810331), and employee count checkboxes (0-50, 51-249, 250-749, 750-1999, 2,000+). A checkbox at the bottom indicates agreement to terms and conditions.
- Step 3: Get Started**. A confirmation message: 'We would like to keep you in our database in order to send you product updates, and email announcements from Okta, and to share your information with various service providers and partners, as described in detail here. You may unsubscribe from Okta's mailing list at any time, by following this process. Additional details about Okta's privacy practices are available in our Privacy Policy.'
- Step 4: Thank you for registering. Welcome to the family.**. A confirmation message stating a confirmation email has been sent. It provides a unique URL: <https://www.okta.com/ranmobojo-onmicrosoft.okta.com>.

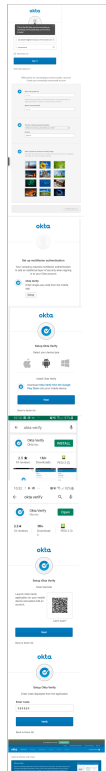
2. Setting up an OKTA Overview free trial (PART 1)

- Go to **Office 365**. Log-in to office.com with your **Cloud Admin account** and check your office 365 email. **Open** your email from the **The Okta Team**
- Click on the **sign in here** URL



3. Setting up an OKTA Overview free trial (PART 1)

- In the **Login console** use your **Okta username** the **temporary password**. Select **Sign In**. On the **Welcome** window ,
 1. **Enter** and **Confirm** your **new password**,
 2. Choose a **forgot password question** and **Answer**
 3. Click a picture to choose a **security image**
 4. Select **Create My Account**
 5. On the **Set up multifactor Authentication** page select **Setup**
 6. On the **Setup Okta Verify** page. Complete the following
 1. Choose your device type. (either windows, Android or IOS) In this setup we will demonstrate Android .
 2. **Download and install** the Okta Verify Application. When done open the Okta Verify application on your Device.
 3. Select **Next**
 7. On the **Scan Barcode**, page using your device **Scan your Barcode** and select **Next**
 8. On the **Enter Code** page, enter your **device Code** and select **Verify**
 9. On the **Getting Started with Okta** window notice you now have a 30 day trial of OKTA. Browse around to familiarize with the Console.

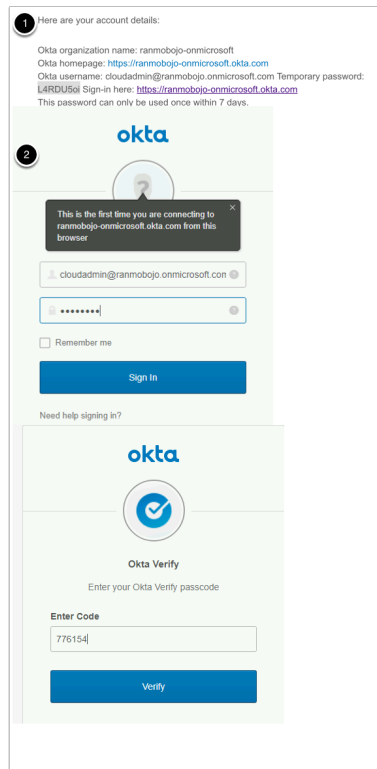


4. Setting up an OKTA Overview free trial (PART 1)

- To complete our setup we will setup Directory sync with your EUC-Livefire Active Directory Domain you and your OKTA environment.

Log into your **"on-prem" lab** environment as **euc-livefire.com\administrator** with the password **VMware1!**

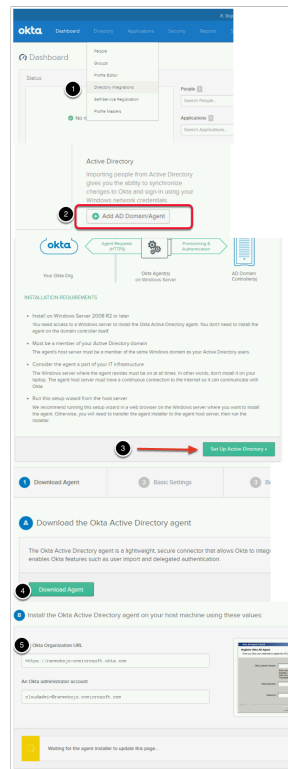
1. On the **ControlCenter2** server open your **chrome browser** and copy **OKTA url** on the ControlCenter server. e.g. <https://ranmobojo-onmicrosoft.okta.com/>
2. Sign in with your **OKTA admin console** with your OKTA **username** and **password** select **Sign In**
3. Use your Okta Verify Code to sign in



5. Setting up an OKTA Overview free trial (PART 1)

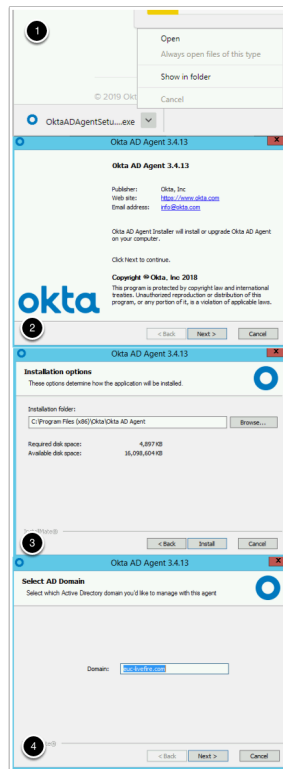
Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. In the Okta Admin console select **Directory** > **Directory Integrations**
2. In the **Directory Integrations** interface, bottom right-hand corner, select **Add AD Domain/Agent**
3. Select **Set Up Active Directory** in the bottom right-hand corner
4. Select **Download Agent**,
5. Note the **installation information** on your admin Console, you will use this information when installing the agent.



6. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. in your control center VM Select the downloaded **OktaADAgentSetup.exe** and select **Open** select **Run**
2. On the downloaded Okta AD Agent, select **Next**
3. On the **Installation options** window select **Install**
4. In the **Select AD Domain** window *accept your default Domain* and select **Next**



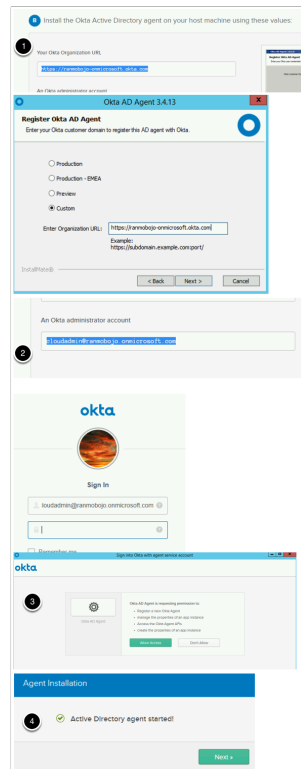
7. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. On the **Okta AD Agent Windows Service Account** window *accept the default*, select **Next**
2. On the **Okta AD Agent Windows Service User**, type and **confirm** the **password, VMware1!** select **Next**
3. On the **Okta AD Agent Proxy Configuration** window, select **Next**

The image displays three sequential screenshots of the Okta AD Agent 3.4.13 installation wizard. The first window, titled 'Okta AD Agent Windows Service Account', prompts the user to select a domain user for the agent to run as. It offers two options: 'Create or use the OktaService account (recommended)' (selected) and 'Use an alternate account that I specify'. The second window, titled 'Okta AD Agent Windows Service User', informs the user that a new domain user will be created and asks for a password. The third window, titled 'Okta AD Agent Proxy Configuration', asks the user to specify a proxy server for the agent to access Okta, with the 'Use proxy server' option currently unchecked.

8. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. On the **Register Okta AD Agent** window, select the Custom radio button, next to Enter Organizational URL: in the **Enter Organization URL:** box type *your Organization URL* Select **Next**
2. In the **Sign in** page under **Username**, type the *OKTA Administrator account* and *password* and select **Sign In**
3. Select **Allow Access**
4. On the Agent Installation window select **Next**



9. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. In the **Set Up Active Directory** window , In the **Connect an Organizational Units (OU) to Okta** interface ensure that only **corp ou** is selected in the **users** and **groups** interface. Select **Next**
2. In the **Import Ad Users and Groups** window select **Next**

1

Okta username format: User Principal Name (UPN)

Next >

Import AD Users and Groups

Active Directory agent configured!

2

Next >

10. Setting up Directory sync with our Active Domain and this OKTA environment continued....

1. On the **Select the attributes to build your Okta User profile** page select **Next**
2. On the **Agent Setup Complete** page select **Done**
3. Select the **Okta AD Agent** on your Taskbar and select **Finish**

1

2

3

4

5

Set Up Active Directory

1 Agent Started 2 Basic Settings Configured 3 Build User Profile 4 Agent Setup Complete 5 Done

3 Select the attributes to build your Okta User profile

Search...

Refresh Attribute List

Next >

Attribute Name	Type	Description	Imported Attributes
USNInterleave	integer	USN-Interleave	Base Schema (required)

2

1 Agent Started 2 Basic Settings Configured 3 User Profile Built 4 Done

4 Agent Setup Complete

Your Active Directory domain is now integrated with Okta.

You can now sync your AD users to Okta and turn on useful authentication features. We recommend installing multiple agents for high availability. Read Next Steps to learn more.

Done

Test Delegated Authentication

Okta AD Agent

Okta AD Agent 3.4.13

Installation completed

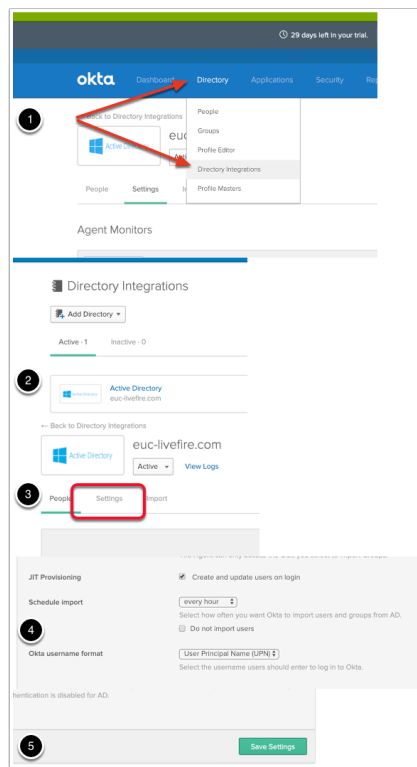
Okta AD Agent has been successfully installed on your computer.

Click Finish to close Okta AD Agent Installer.

Finish

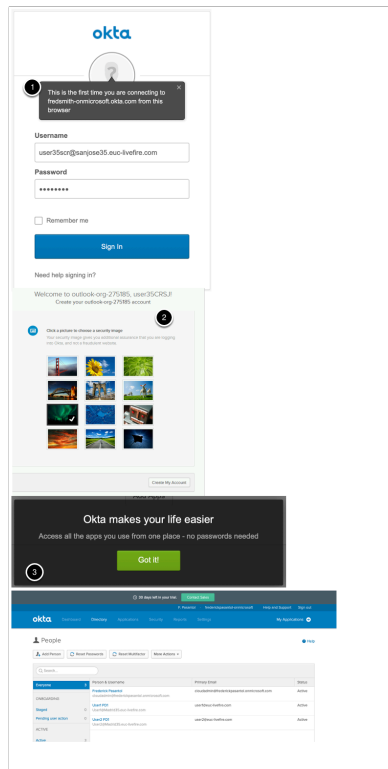
11. Setting up Directory sync with our Active Domain and this OKTA environment continued....

1. In the **Okta admin** console select **Directory > Directory Integrations**
2. Below the **Active** tab select **Active Directory**
3. In the **Active Directory** area next to **People** select **Settings**
4. In the **IMPORT AND ACCOUNT SETTINGS** console scroll down and select the following:
 1. Select the **check box** in line with **JIT Provisioning** called **Create and update users on login**
 2. Next to **Schedule import** change the **dropdown** from **never** to **every hour**
5. Scroll down to the bottom and select **Save Settings**



12. We will validate our provisioning of user provision now in OKTA

1. Open up an **Incognito window** in your browser and launch your **OKTA login URL**. Login with **your custom user account** user eg **user35SCR@sanjose35.euc-livewire.com** with password **VMware1!** select **Sign In**
2. On the **Welcome to your OKTA page**, click a **picture to choose a security image**, select **Create My Account**
3. Close the **OKTA IS THE IDENTITY STANDARD** page by selecting **Got it** on the bottom right hand corner.
4. If you go back to your **OKTA admin Console**, select **Directory > People**, you will now notice your provisioned users



Part 2. OKTA and Workspace ONE Access Federation Configuration

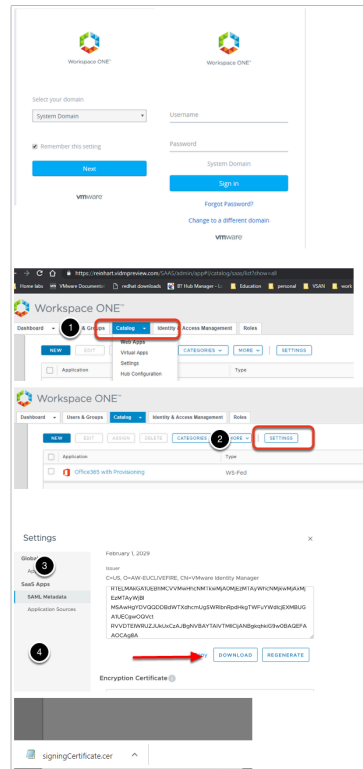
Summary

We have accomplished a few things in Part 1 . You have seen how well **Just In Time (JIT)** provisioning works with external applications and OKTA. OKTA supports a much broader ecosystem of applications than Workspace ONE Access. This part of the lab would represent what an organisation might already have in place or it might represent what we might have put in place first before using Workspace ONE Access. A very important concept to realize is if we are going to federate 3rd party solutions we have to have a basic understanding of the workings / capabilities of the solution we want to federate with to offer the best solution to the customer. Okta themselves realize that VMware have a very powerful Single-Sign On (SSO) solution using Workspace ONE. We will now federate with Workspace ONE Access.

In this section we will retrieve information required by Okta to setup an Identity Provider . In this scenario Workspace ONE Access will be the Identity Provider.

1. Login to the **Workspace ONE Administration Console** on the **System Domain** with **Admin** privileges to your New SaaS Workspace ONE Access Tenant.
 1. Select the **Catalog -> Web Apps** tab
 2. To the right select the **Settings** button from the sub-menu
 3. In the resulting dialog navigate to **SaaS Apps -> SAML Metadata**

4. Download the **Signing Certificate**. Note the location of the downloaded file **signingCertificate.cer**



2. Part 2. OKTA and Workspace ONE Access Federation Configuration

- In the right pane under **SAML Metadata**, click on **Identity Provider (Idp) Metadata** link and record and save the following 2 configurations using **Notepad**
 1. Next to **entityID** copy **your version** of the following url from the address bar :
e.g. <https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml>
 2. Search for **urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST** and next to **Location** copy **your version** of the following: **"<https://aw-livefirerplaston.vidmpreview.com/SAAS/auth/federation/sso>"**
 3. Select **X** in the right hand corner of the pane to close the window

SAML Metadata

Application Sources

logins from Identity Manager to relying applications, such as Web Apps. Copy and paste the certificate below and send it to the relying application so they can accept logins from Identity Manager. For integrating relying applications utilizing SAML 2.0, you can use the metadata:

SAML Metadata ⓘ

Identity Provider (IdP) metadata [Copy URL](#)

Service Provider (SP) metadata [Copy URL](#)

1 XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" cacheDuration="P0Y0M30DT0H0M0.000S" entityID="https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml" version="01T21:31:02.000Z">
  <md:NameIDFormat/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>
</md:EntityDescriptor>
```

2

```
</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>
</md:EntityDescriptor>
```

Entity ID "https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml"

Single sign on Service "https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>

Settings

Global

Approvals

Download SAML Metadata

Generate CSR

3. Part 2. OKTA and Workspace ONE Access Federation Configuration

- In this section we will create the Identity Provider (IdP) record in the **Okta admin UI** with Administrator login.

In the OKTA admin Console (on your Chrome browser)

- If required, In the top right hand corner. Select the **Admin** button
- Navigate to **Security** -> **Identity Providers**

1

Home

ranmo

+ Add Apps

Admin

2

okta

Dashboard

Directory

Application

Security

Reports

Settings

Dashboard

Status

6 users were imported from euc-livefire.com

General

Authentication

Multifactor

Identity Providers

Delegated Authentication

Networks

4. Part 2. OKTA and Workspace ONE Access Federation Configuration

- In the OKTA admin Console continued...

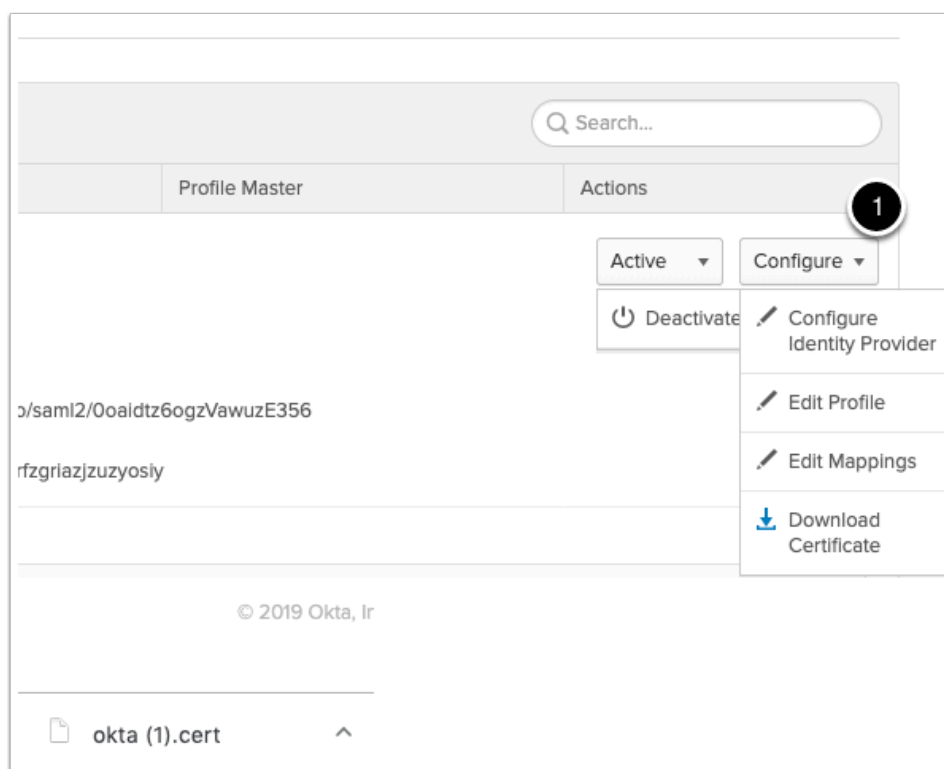
1. Select **Add Identity Provider** button window, select **Add SAML 2.0 IdP** :
2. Under **GENERAL SETTINGS** next to **Name**: type **WorkspaceONE**
3. Under **AUTHENTICATION SETTINGS**
 1. **Idp Username** : **idpuser.subjectNameid**
 2. **Filter**: **Unchecked**
 3. **Match Against**: **Okta Username**
 4. **If no match is found**: **Redirect to Okta sign-in page** radio button
4. Under **SAML PROTOCOL SETTINGS**
 1. **IdP Issuer URI**: e.g. <https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml>
Entity ID value value from the Workspace ONE Access IdP metadata file saved to Notepad
 2. **IdP Single Sign-On URL**: e.g. <https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso>
(Single Sign on Service value from IdP metadata file from the Workspace ONE Access Idp metadata file)
 3. **IdP Signature Certificate**. **Browse** , select **All files** next to filename and **select the Signing Certificate** from your SAAS Workspace ONE Access Tenant. *If your cer files is greyed out, make sure you are using **Chrome** as your browser.*
5. Select **Add Identity Provider**

The screenshot displays the 'Add Identity Provider' form in the Okta admin console. The form is divided into several sections: 'GENERAL SETTINGS', 'AUTHENTICATION SETTINGS', and 'SAML PROTOCOL SETTINGS'. In the 'GENERAL SETTINGS' section, the 'Name' field is set to 'WorkspaceONE'. The 'AUTHENTICATION SETTINGS' section shows 'Idp Username' as 'idpuser.subjectNameid', 'Filter' as 'Unchecked', 'Match against' as 'Okta Username', and 'If no match is found' as 'Redirect to Okta sign-in page'. The 'SAML PROTOCOL SETTINGS' section shows 'IdP Issuer URI' as 'https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml', 'IdP Single Sign-On URL' as 'https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso', and 'IdP Signature Certificate' as 'OKTA, OKTA EUCLIVEFIRE, Okta Workspace ONE Access, Certificate expires in 3650 days'. The 'Add Identity Provider' button is highlighted at the bottom.

5. Part 2. OKTA and Workspace ONE Access Federation Configuration

- In the **OKTA admin Console continued...**

- In the **Identity Providers** interface, to the right, select the **drop down arrow** next to **Configure** and select **Download Certificate**



Part 3: Federating BambooHR with OKTA

1. Federation of BambooHR with OKTA (Part 3)

- In this section we setup a Federation with BambooHR web application. You are entitled to a 7 day trial of the BambooHR SaaS software.
 1. We will start off by going to a **browser** and In google type **BambooHR free trial**.
 2. Where it says **Try it Free** select
 3. In the **Were Ready to you up page** aenter the following credentials
 - **First Name** (same First Name you registered with OKTA)
 - **Last Name** (same Last Name you registered with OKTA)
 - **Work email address**, (same email address you registered with OKTA)
 - **Select a Password** (VMware1!)
 4. Select **Get Started**
 5. On the **Congratulations page** type your
 - **work phone number**, your phone number
 - **company Name**, eg. Euclivfire
 - **custom domain name** eg. Madrid34.bamboohr.com
 6. Select **Create Account**
 7. On the **Account is ready page** select **Login**
 8. On the login page , login with your email and password

Google bambooHR New User

To 4 Free - BambooHR
 BambooHR is a leading provider of HR software. We're ready to help you get started with BambooHR. Start today. It takes less than a minute and is 100% confidential.

We're ready to set up your free trial of BambooHR
 Start today. It takes less than a minute and is 100% confidential.

Step 1 of 2

First Name
 Hendrik

Last Name
 Manwell

Work Email
 Hendrik.Manwell@gmail.com

Password
 [REDACTED]

I agree to the terms and conditions

Get Started

Account is ready **Log In**

Congratulations, we're setting up your free trial
 While it's loading we need a few more facts to get you started.

Step 2 of 2

Company Name
 eucioefive

Number of Employees
 10-25 employees

Country
 United States

Consent (URL)
 Liberal15_bamboo.hr.com

I agree to the terms and conditions

Create Account

COMPANY LOGO HERE

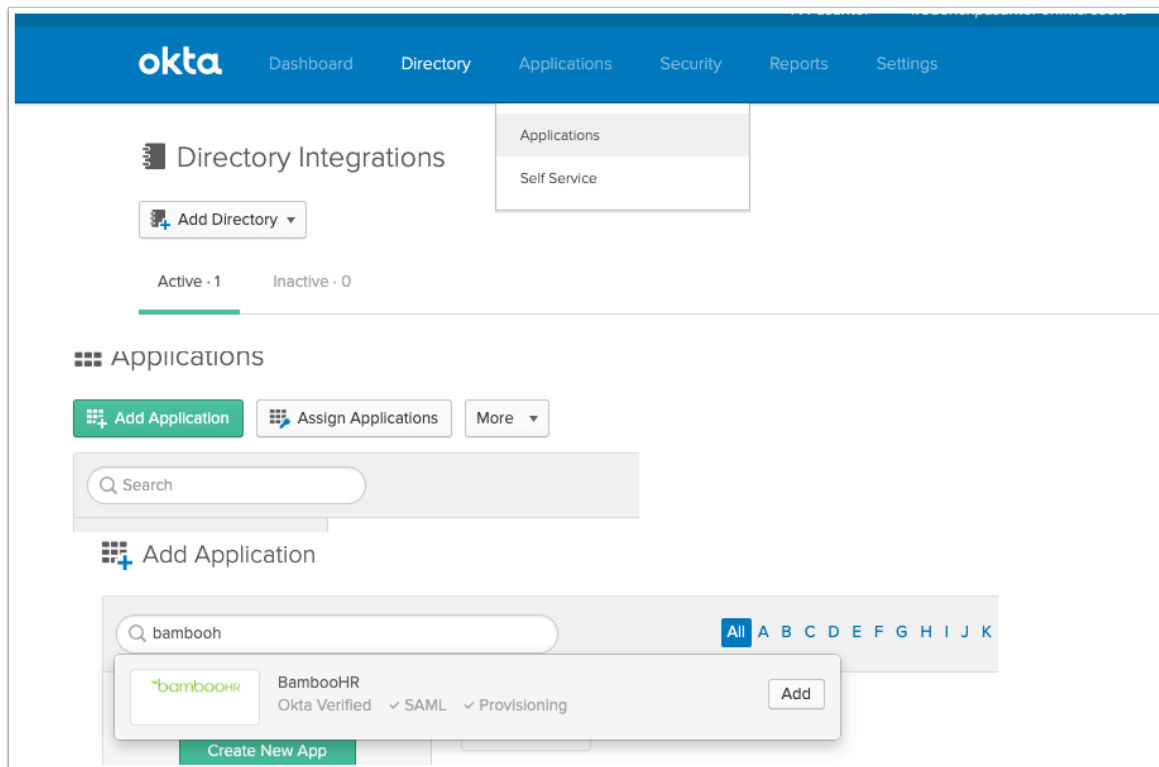
Hendrik.Manwell@gmail.com

[REDACTED]

Log In [Forgot Password?](#)

2. Federation BambooHR with OKTA (Part 3)

- Switch to your OKTA admin console to complete the next step of the configuration
 - In the **Okta Admin Console** select **Applications** > **Applications**
 - Under **Applications** select **Add Application**
 - In the **Search** type **BambooHR** and select **Add**



3. Federation BambooHR with OKTA (Part 3)

- In the **Add BambooHR** interface under **General Settings** type the following
 - Next to **Application Label**, type **BambooHR(customdomain) BambooHR Madrid 34**
 - Next **Subdomain** type your **custom domain** e.g **Madrid34** select **Next**

The screenshot shows the 'Add BambooHR' interface with the 'General Settings' tab selected. The 'Application label' is set to 'BambooHR Madrid 34' and the 'Subdomain' is set to 'Madrid34'. The 'Browser plugin auto-submit' checkbox is checked. The 'Next' button is highlighted in green.

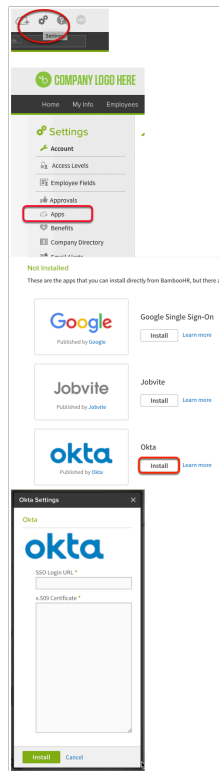
4. Federation BambooHR with OKTA (Part 3)

- In the **OKTA Add BambooHR** interface under **Sign-On Options** select the following
 1. Next to **SAML 2.0** select the **radio button**
 2. At the bottom of the window select **Done**

The screenshot shows the 'Add BambooHR' configuration window in the OKTA admin console. The 'Sign-On Options' tab is selected, indicated by a blue circle with the number '2'. The 'Sign-On Options · Required' section is active. Under 'SIGN ON METHODS', 'SAML 2.0' is selected with a blue radio button. Below this, there is a 'Default Relay State' field and a 'Create and update' dropdown. A checkbox for 'Allow users to securely see their password (Recommended)' is unchecked. A blue information box states: 'Password reveal is disabled, since this app is using SAML with no password.' At the bottom right, there is a green 'Done' button. A circular callout with the number '2' is positioned over the 'Done' button.

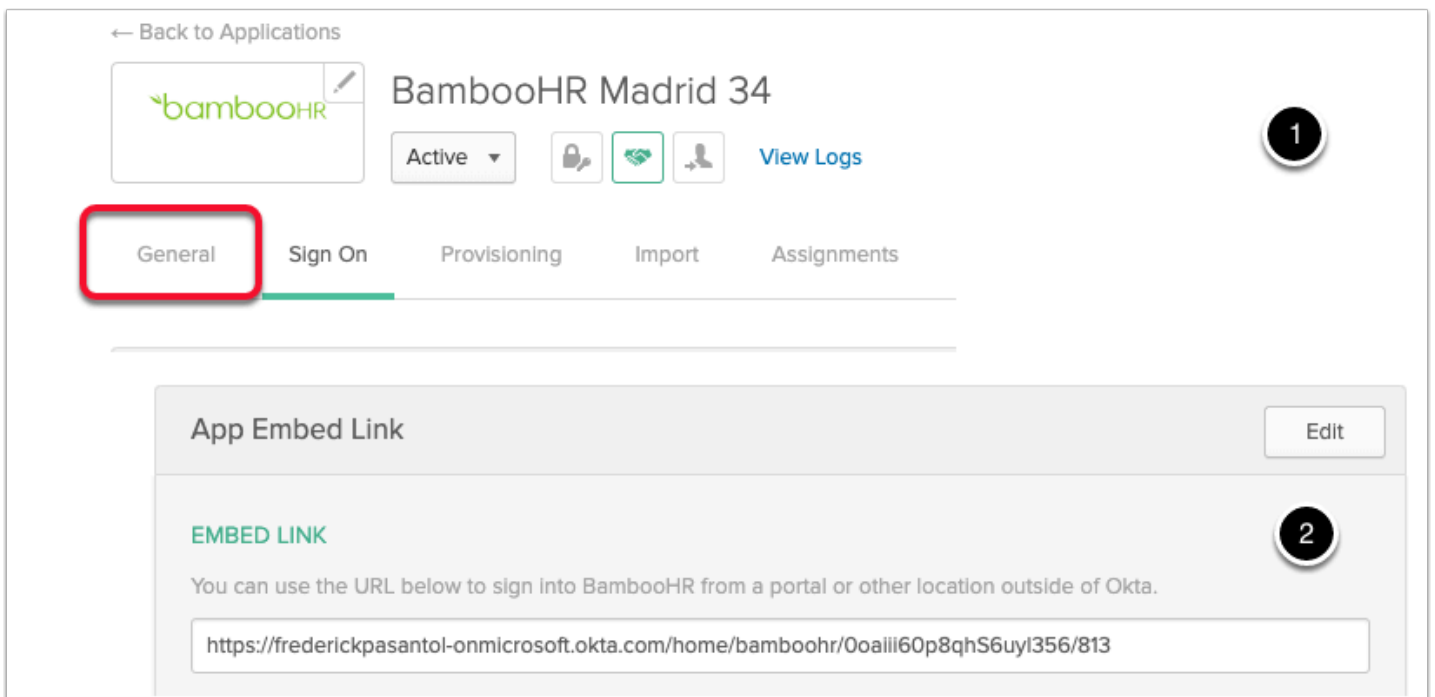
5. Federation BambooHR with OKTA (Part 3)

- Switch back to your custom **BambooHR** SaaS AP
 1. In top right-hand select **Settings**, this is a wheel-cog icon
 2. In the left-hand pane select **Apps**
 3. Under **Apps** select **Single Sign-On**
 4. In the **Single Sign-On** window select **OKTA**
 5. Scroll down and select **Install**



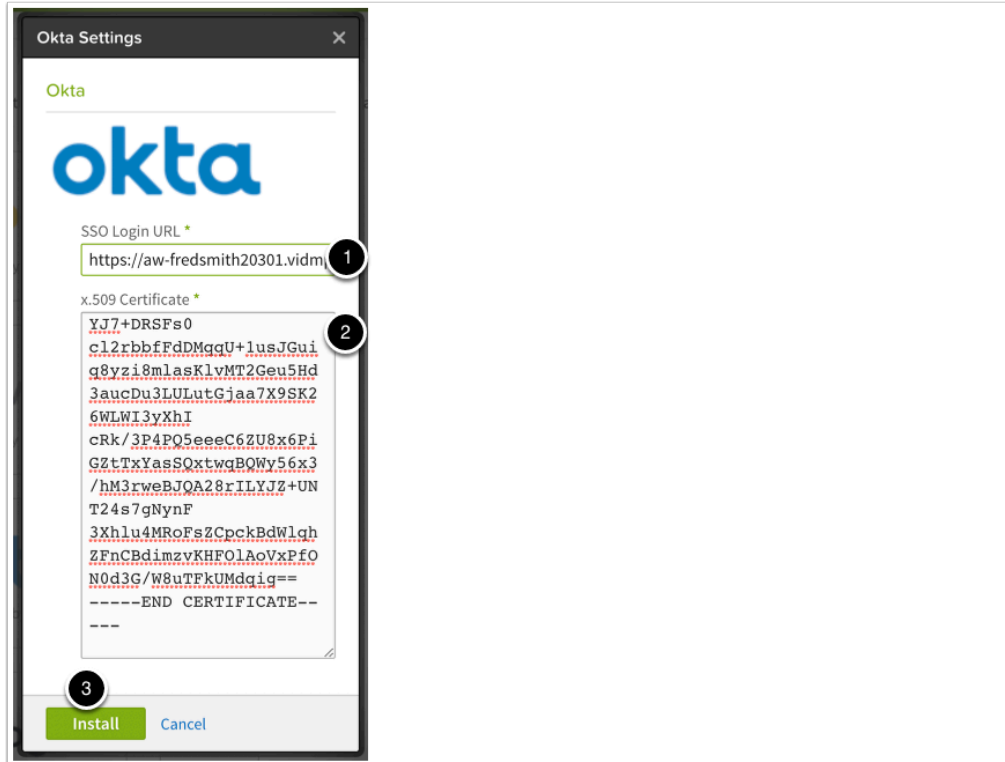
6. Federation BambooHR with OKTA (Part 3)

- Switch back to your **Okta Console**
 - In the **Applications** interface next to **Sign On** select **General**
 - Scroll down to **App Embed Link** and under **EMBED LINK** copy **the entire URL** and save in **Notepad**



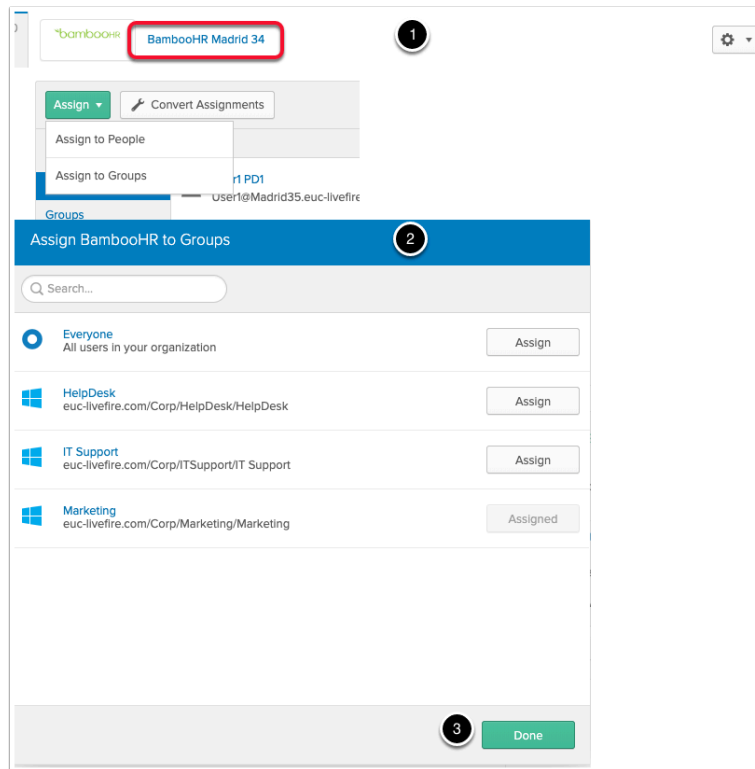
7. Federation BambooHR with OKTA (Part 3)

- Switch back to your **BambooHR Admin Console**
 - From your Notepad file copy the **SSO Login URL** and under **SSO Login URL** paste the copied link from OKTA
 - Next open the **Okta.cert** file with a text editor and **copy** the entire certificate, this includes **---begin certificate xxx --- END CERTIFICATE---** and paste into the **x.509 Certificate box**
 - Scroll to the bottom of the page and select **Install**



8. Federation BambooHR with OKTA (Part 3)

- Switch back to your **OKTA Admin Console**
 - Go back to **Applications > Applications** and select your **BambooHR application**
 - Select **Assign > Assign to Groups**
 - In the **Assign BambooHR to Groups** next to **Marketing** select **Assign** and select **Done**
 - Select **Assign > assign to people**
 - Assign to your administrator user.



9. Federation BambooHR with OKTA (Part 3)

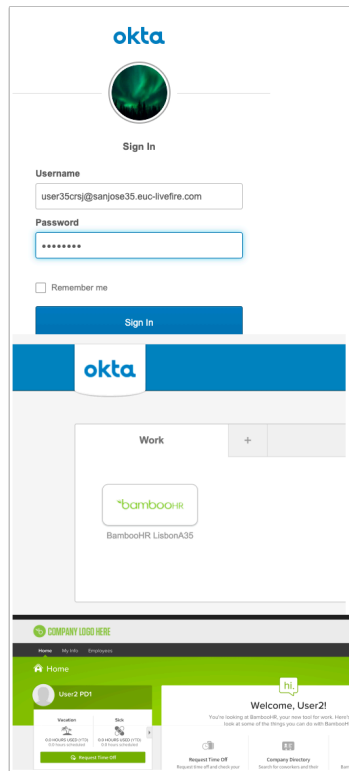
- Switch back to your **BAMBOOHR Admin Console**
 1. In the Bamboo HR application select the **Home tab**
 2. To right of the page select the **drop down arrow** next **New...** and select **New Employee**
 3. In the **Add Employee** interface , use the following information, type next to:
 1. **Name:** **Unique User from AD** (the one you created in the SFDC lab)
 2. **Last:** Last name of the unique User
 3. **Email address:** **XXXXX@euc-livewire.com** (unique username + @euc-livewire.com)
 4. **Self Service Access:** ON
 4. When done select **Save**.

The screenshot shows the BambooHR 'Add Employee' form on the left and a 'user35CRSJ Properties' pop-up window on the right. Red arrows indicate the mapping of data from the form to the pop-up:

- First name:** user35CRSJ (from 'Name' field)
- Last name:** CRJ (from 'Middle' field)
- Display name:** user35CRSJ (from 'Name' field)
- Description:** (empty, from 'Description' field)
- Office:** (empty, from 'Office' field)
- Telephone number:** (empty, from 'Telephone number' field)
- Email:** user35crj@earpae35.euc-livfire.com (from 'Email' field)
- Web page:** (empty, from 'Web page' field)

10. Federation BambooHR with OKTA (Part 3)

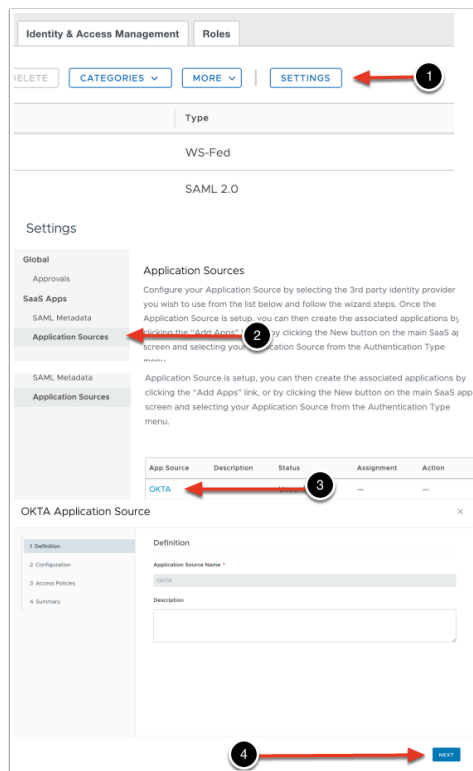
- We will now validate the single sign-on process with OKTA and BambooHR
 - Open an **Incognito session** of your browser and copy **your custom login url** for OKTA in the address bar. Login with XXXXuniqueuser@customsuffix.euc-livfire.com (example user35buk@auckland35.euc-livfire.com) and password **VMware1!** select Sign In
 - If this is the first time you login you will be prompted to choose a custom icon and you will have to close default pop ups
 - Under the **Work** tab you should see your **BambooHR entitlement**. Select your **BambooHR** entitlement.
 - You should see the single sign on between **OKTA** and **BambooHR**.



Part 4. Configuring An OKTA Application Source in Workspace ONE Access.

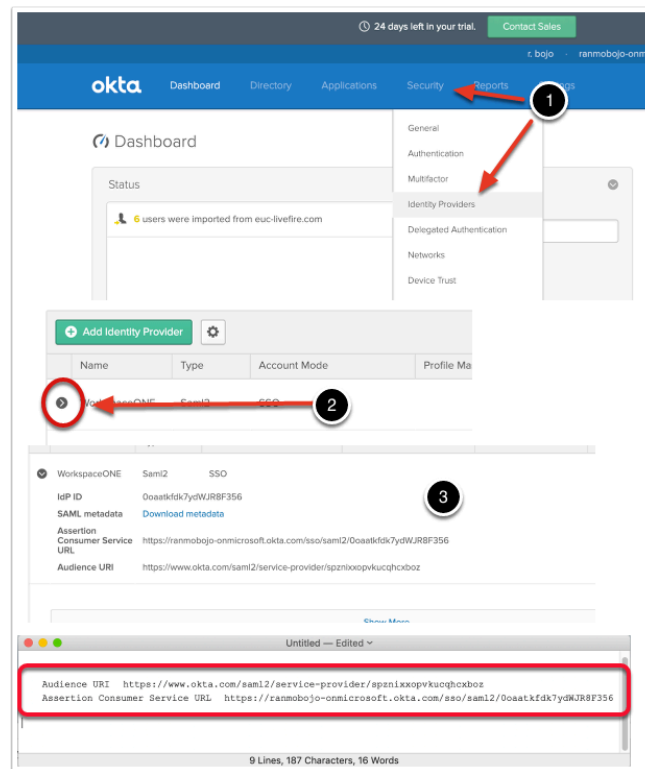
1. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- Ensure you are logged into your Workspace ONE Access Session
 1. Under **Catalog > Web Apps** to the right select **SETTINGS**
 2. In the Inventory pane under **SaaSApps** select **Application Sources**
 3. In the **Application Sources** section under **App Source** select **OKTA**
 4. On the **OKTA Application Source** window select **NEXT**



2. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- Switch back to your **OKTA admin Console**
 - Select **Security > Identity Providers**
- 1. Expand your **arrow >** next to your existing **WorkspaceONE** configuration to face down.
- 2. Notice under WorkspaceONE you have 4 rows of information.
 - Save your **Assertion Consumer Service URL** and your **Audience URI** to Notepad



3. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- Switch back to your **Workspace ONE admin console**
 1. In the **OKTA Application Source** under **Configuration** change the **radio button** to **Manual**
 2. In section **2. Configuration** of the **OKTA Application Source** page add the following:-
 1. In the **Single Sign-On URL** section **copy and paste** your **Assertion Consumer URL**
 2. In the **Recipient URL** section **copy and paste** your **Assertion Consumer URL**
 3. Next to **Application ID:** **copy and paste** your **Audience URI**

OKTA Application Source

1 Definition

2 Configuration

3 Access Policies

4 Summary

Single Sign-On

Authentication Type ⓘ

SAML 2.0

Configuration ⓘ

☐ URL/XML ☒ Manual

OKTA Application Source

1 Definition

2 Configuration

3 Access Policies

4 Summary

Configuration ⓘ

☐ URL/XML ☒ Manual

Single Sign-On URL * ⓘ

https://ranmobojo-onmicrosoft.okta.com/sso/saml2/00aatkfdk7ydWJR8F356

Recipient URL * ⓘ

https://ranmobojo-onmicrosoft.okta.com/sso/saml2/00aatkfdk7ydWJR8F356

Application ID * ⓘ

https://www.okta.com/saml2/service-provider/spznixxopvkucqhcxbz

4. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the **OKTA Application Source** wizard
 1. Under **Configuration** **Scroll** down, next to:
 1. **Username Format:** Unspecified, (default)
 2. Under the **Username Value:** **`${user.userPrincipalName}`**
 2. **Scroll down** until **Advanced Properties**, and **expand** configure the following Next to:
 1. **Sign Response:** Yes (default)
 2. **Sign Assertion:** No (default)
 3. **Encrypted Assertion:** No (default)
 4. **Include Assertion Signature:** No (default)
 5. **Signature Algorithm:** SHA256 with RSA (default)
 6. **Digest Algorithm:** **SHA256**
 7. **Assertion Time:** 200 (default)

The image displays two screenshots of the 'OKTA Application Source' configuration window. The first screenshot, labeled with a circled '1', shows the 'Configuration' tab. In the 'Username Value' field, the value '\$(user.userPrincipalName)' is selected and highlighted with a red rectangle. The second screenshot, labeled with a circled '2', shows the 'Request Signature' section. The 'Sign Assertion', 'Encrypt Assertion', and 'Include Assertion Signature' options are all set to 'No'. The 'Signature Algorithm' is set to 'SHA256 with RSA'. A circled '3' is placed near the bottom of the second screenshot.

5. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the **OKTA Application Source** under **Configuration** continue scrolling down
 1. Under **Request Signature:** **open** the contents of the **Okta.cert** file previously downloaded from Okta. **Copy** and **paste** the contents including the "**-----BEGIN CERTIFICATE-----**" and "**-----END CERTIFICATE-----**"
 2. Select **Next**

OKTA Application Source

1 Definition
2 Configuration
3 Access Policies
4 Summary

Request Signature

```
nREMgUvPvT/EmOAIXOw+YYDZuhUF+Ng7zGZf4QaaMxVWLAIZ43YW5//ezleueIPVqpoebQIDPX
q5aS/VJJC8pRoxNXHwI37VkGOAnOBem+yM3yA4Zo4WtLzZ82/kRNeRIKrhgw==
-----END CERTIFICATE-----
```

Encryption Certificate

Enable Authentication Failure Notification

No ☐

Application Login URL

Proxy Count

1

2

CANCEL BACK NEXT

6. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- **OKTA Application Source** under **Configuration** continued

1. On the **Access policies** page select **NEXT**
2. On the **Summary** page select **SAVE**

OKTA Application Source

1 Definition
2 Configuration
3 Access Policies
4 Summary

Access Policies

Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below.

default_access_policy_set

1

CANCEL BACK NEXT

OKTA Application Source

1 Definition
2 Configuration
3 Access Policies
4 Summary

Definition

Name
OKTA

Description
--

Configuration

Authentication Type
SAML 2.0

Configuration
Manual

Single Sign-On URL
https://rammobajo-onmicrosoft.okta.com/app/zendesks/exkammz8GToggCMK356/sso/saml

Recipient URL
https://rammobajo-onmicrosoft.okta.com/sso/saml2/0aaatkhd7ydwJ8PF356

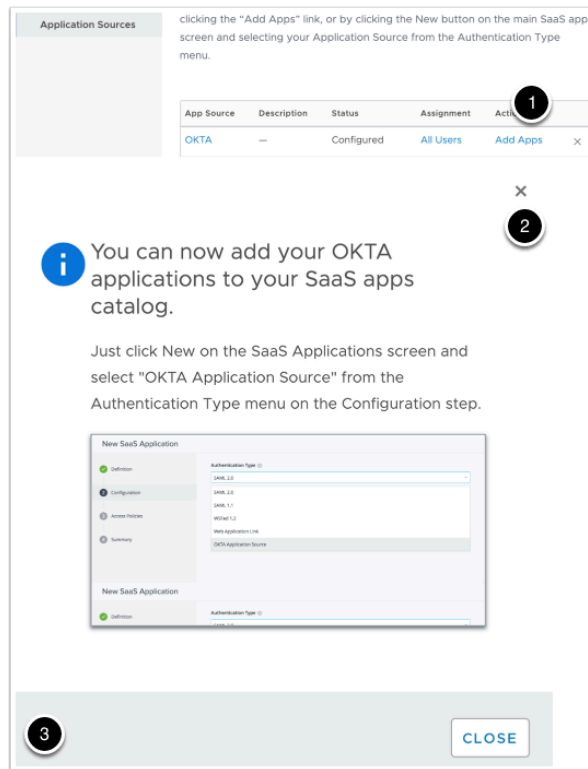
Application ID

2

CANCEL BACK SAVE

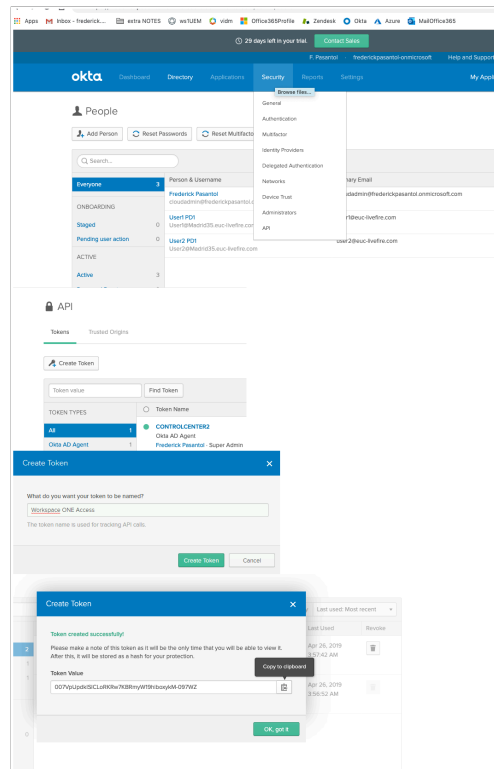
7. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- **OKTA Application Source** under **Configuration** continued
 1. Under **Settings** notice that your **OKTA Source** is now configured. Under **Action** select **Add Apps**
 2. Read the message: When done, select **Close** and select **X** to close the **Settings** page.



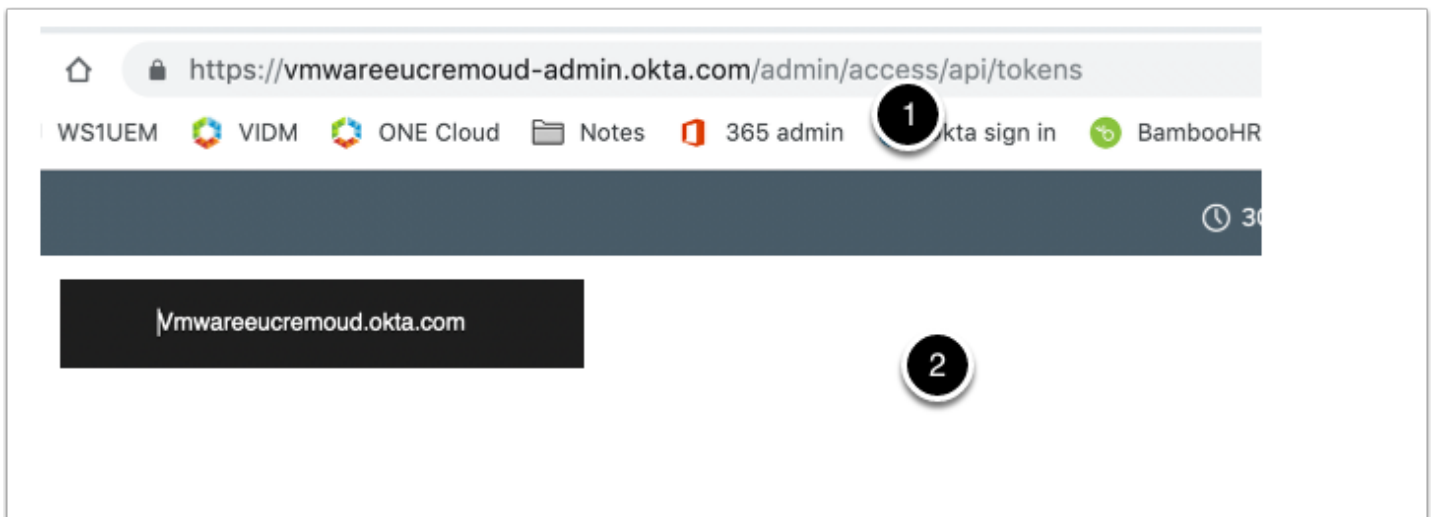
8. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- We will now configure the automatic sync of OKTA applications into the **User Catalog**
 1. Go back to your **OKTA admin Console** and select **Security** > **API**
 - **Very IMPORTANT! We are now going to create a TOKEN, we will only get ONE CHANCE to save this Token. Open a copy of Notepad or Word to document this**
 2. In the **API** console under **Tokens** select **Create Token**
 3. In the **Create Token** window under **What do you want your token to be named?** type **Workspace ONE Access** and select **Create Token**
 4. On the **Create Token** window under **Token Value** select the **Copy to Clipboard** option and **save** and **paste** to Notepad . Then select **OK, got it.**



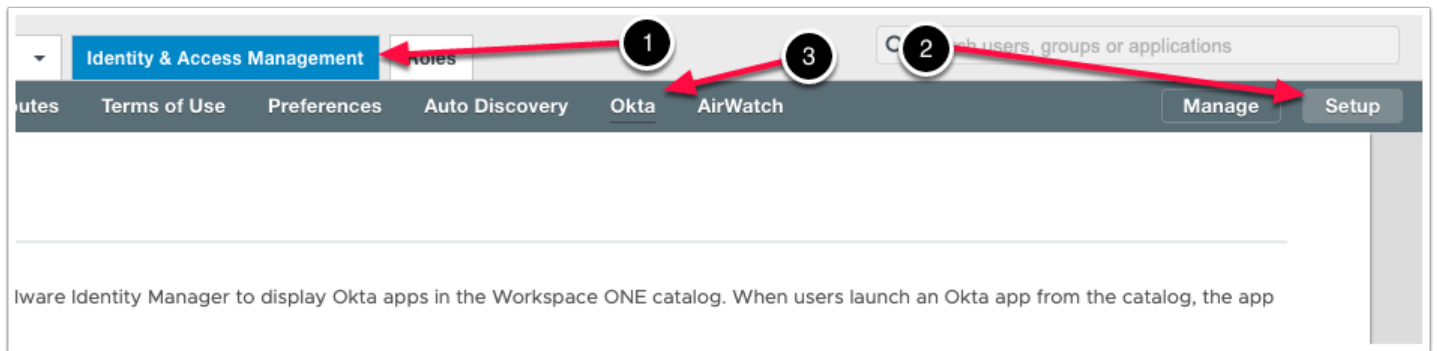
1. 9. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the Okta Console configure the following:
 - Copy your **OKTA ADMIN URL** and save to **NOTEPAD**
 - In **Notepad REMOVE** anything after **.com** and the **-admin** part of the hostname portion from the URL, then **copy the URL**



10. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- Switch back to your Workspace ONE Access Console
 - Select the **Identity & Access Management** tab and select **Setup**
 - Select **Okta**



11. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the Workspace ONE Access Console under **Setup > Okta**
 - Under **Okta Cloud URL** paste your **edited OKTA URL** from Notepad
 - Under **Okta API** token paste your **OKTA access token** from Notepad
 - Under **Search Param** select **\$(user.userName)** in the dropdown
 - Select **SAVE**

Okta Configuration

Configure your Okta tenant with VMware Identity Manager to display Okta apps in the Workspace ONE catalog. W entitlement is confirmed with Okta.

Next, go to the Catalog > Web Apps > Settings page and add Okta as an Application Source app. You do not need dynamically appears in the catalog.

Okta Cloud URL * ⓘ

Okta API Token * ⓘ

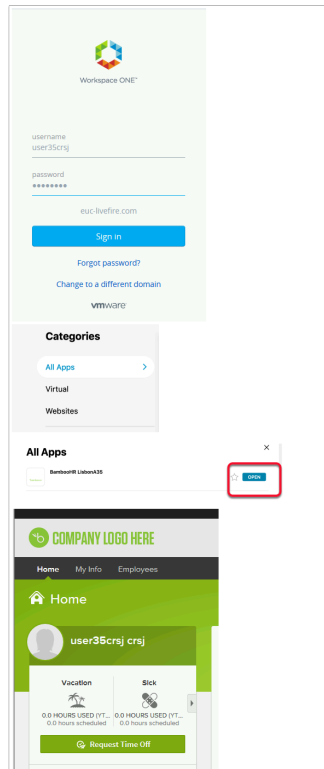
User Search Param * ⓘ

SAVE

12. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- We will now validate the Single Sign On process from Workspace ONE Access to OKTA to BambooHR
 - Open a new browser or Incognito session. Make sure all cookies are deleted from previous sessions.
 - Use your **Workspace ONE Access Url** and login as your **unique user** from the **euc-livefire.com** domain with the password **VMware1!**
 - Under **Categories** select **All Apps**

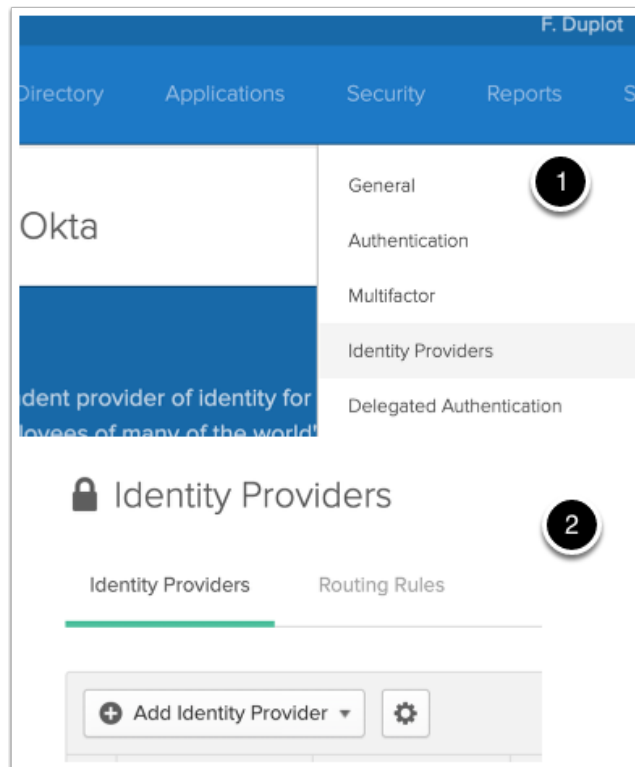
4. Under **All Apps** next to **BambooHR** select **OPEN**, you should now be redirected and signed into **BambooHR**



Part 5. Configuring An OKTA Routing rules for Workspace ONE Access.

5.1

- Ensure you logged into your trial OKTA Admin console with your Custom admin account
 1. Select **Security > Identity Providers**
 2. Next to **Identity Providers** select **Routing Rules**



5.2

- In the Routing Rules section
 1. Select **Add Routing Rule**
 2. In the Add Rule Box select and add the following:
 - **Rule Name:** **Workspace ONE**
 - **AND User's device platform is :**
 - **Any of these devices:** **radio button**
 - **Mobile:** **IOS** and **Android** **checkboxes**
 - **THEN Use this identity provider :****WorkspaceONE**
 3. Select **Create Rule**
 4. On the **Activate Rule?** Window select **Activate**
- When we complete the Mobile SSO IOS and Android labs we can test BambooHR authentication using Workspace ONE Access

Identity Providers

Routing Rules

Add Routing Rule

1 Default Rule

Default R

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

Anything

THEN

Use this identity provider

WorkspaceONE

Manage configuration for Identity Providers

Manage configuration for IWA

Activate Rule?

Activated rules will be applied immediately and change how users are routed to identity providers when logging into your organization.

Activate

Don't Activate