MyWorkDrive SAML v2.0 Okta Integration Guide

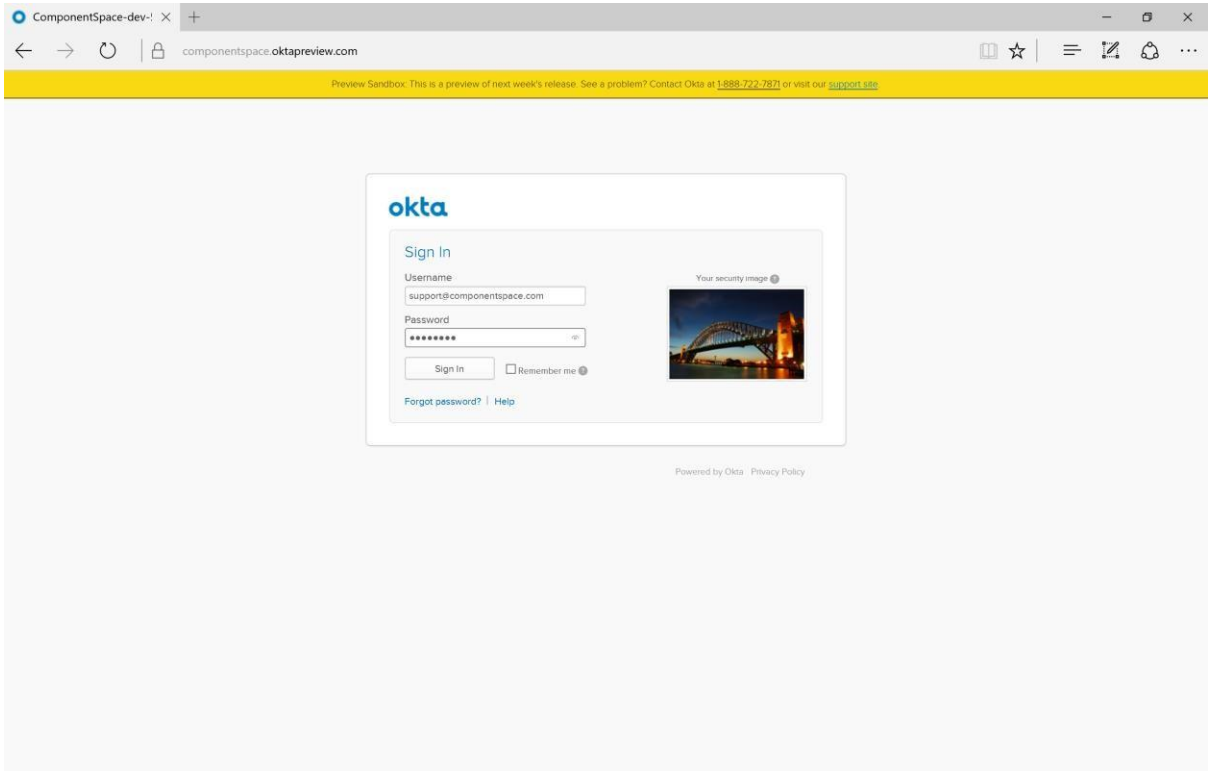
Introduction

In this integration, Okta is acting as the identity provider (IdP) and the MyWorkDrive Server is acting as the service provider (SP).

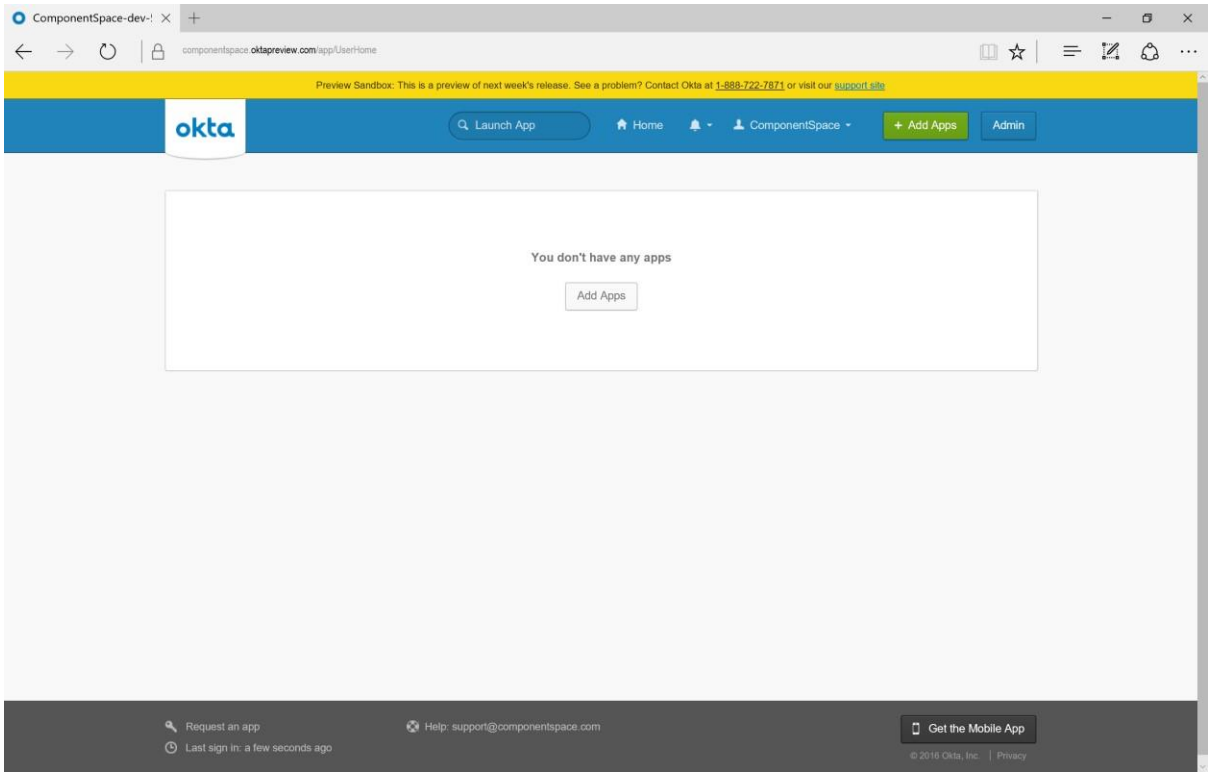
It is assumed all users are logging in to Okta using their UPN Suffix (eg @yourdomain.com) and it matches their Active Directory username UPN.

Identity Provider Configuration

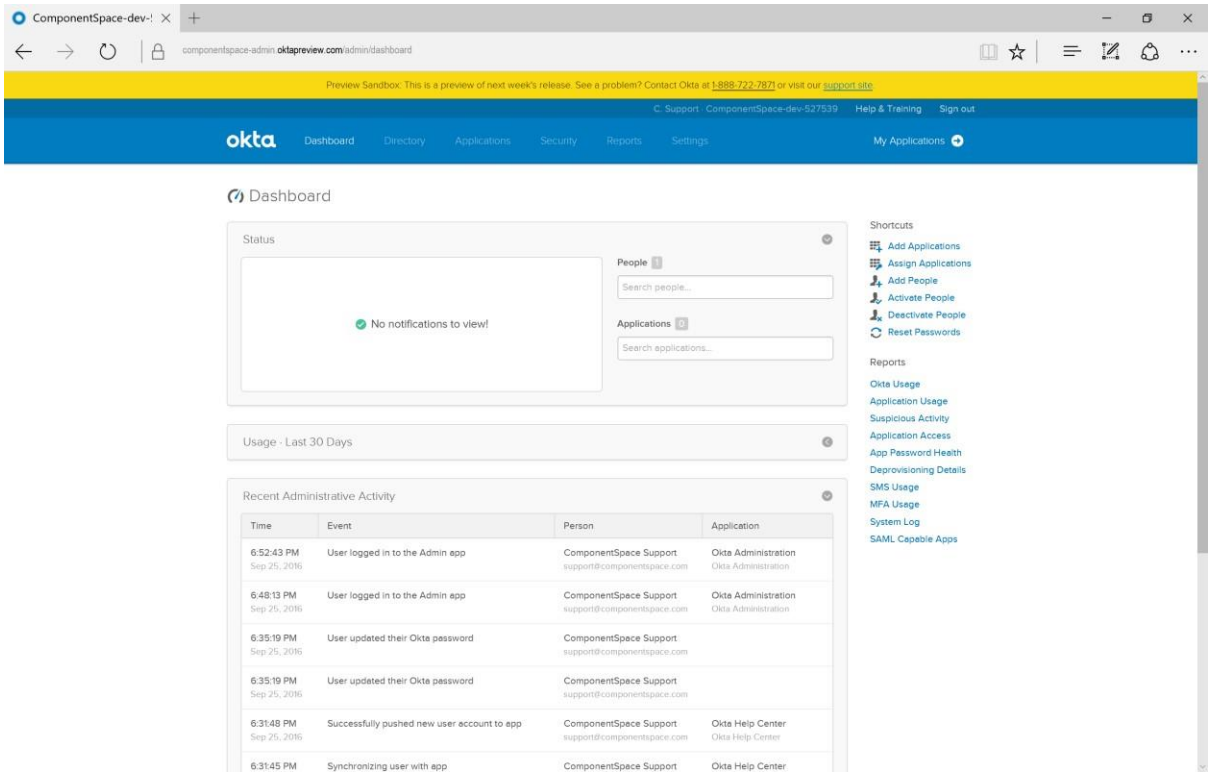
1. Login into Okta.



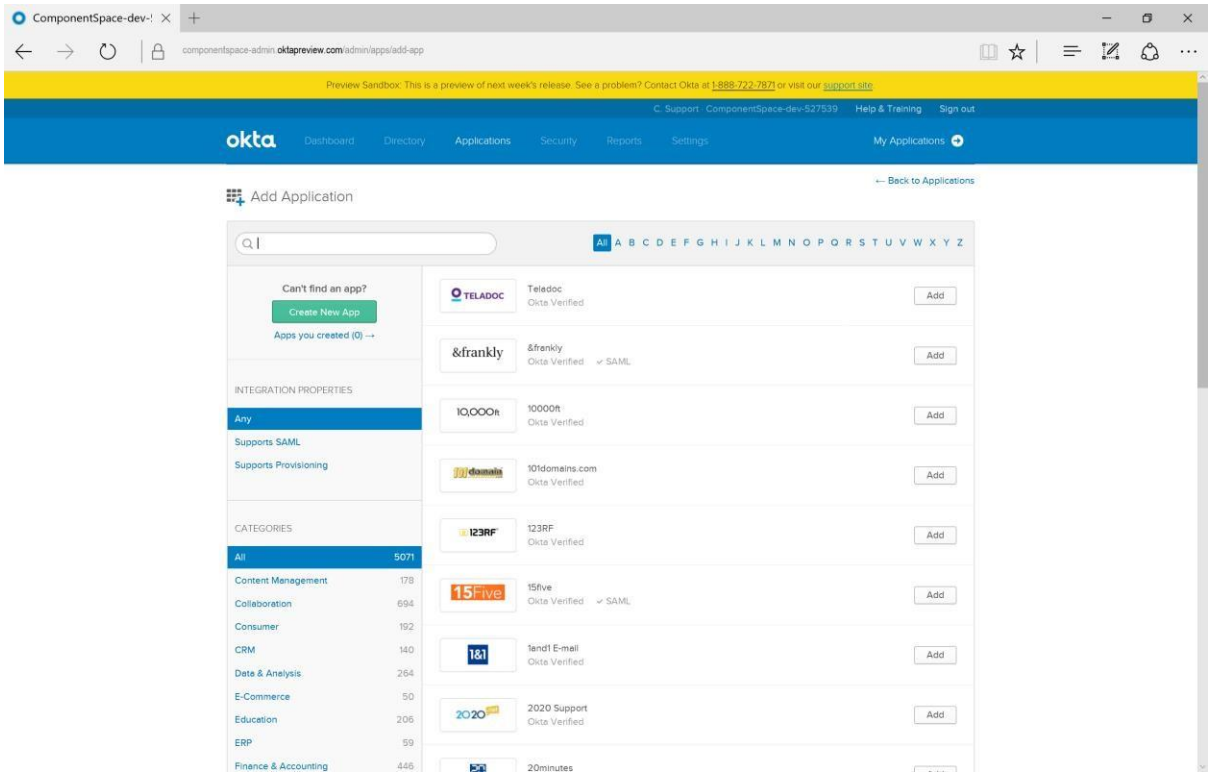
2. Click the Admin button.



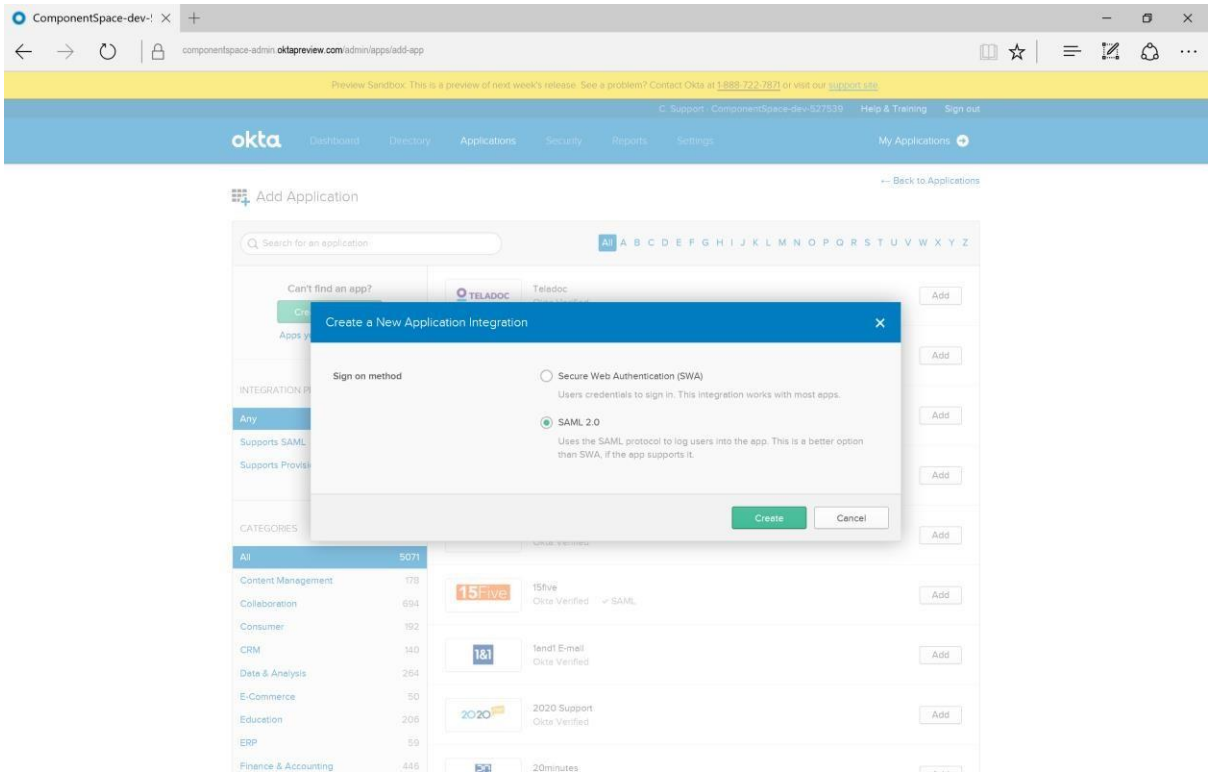
3. Click the Add Applications shortcut.



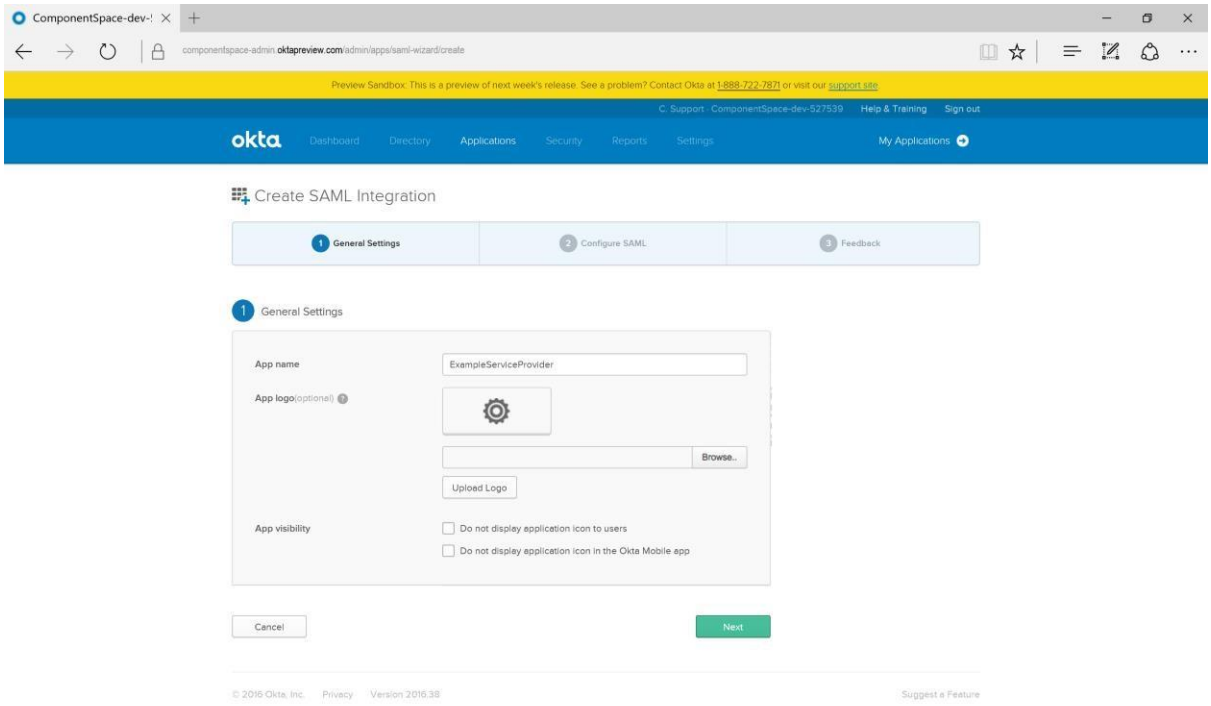
4. Click the Create New App button.



5. Select SAML 2.0 as the sign on method.



6. Specify an application name.



7. Specify the assertion consumer service URL (eg. https://YourMWDserver.yourdomain.com/SAML/AssertionConsumerService.aspx) as the single sign-on URL.

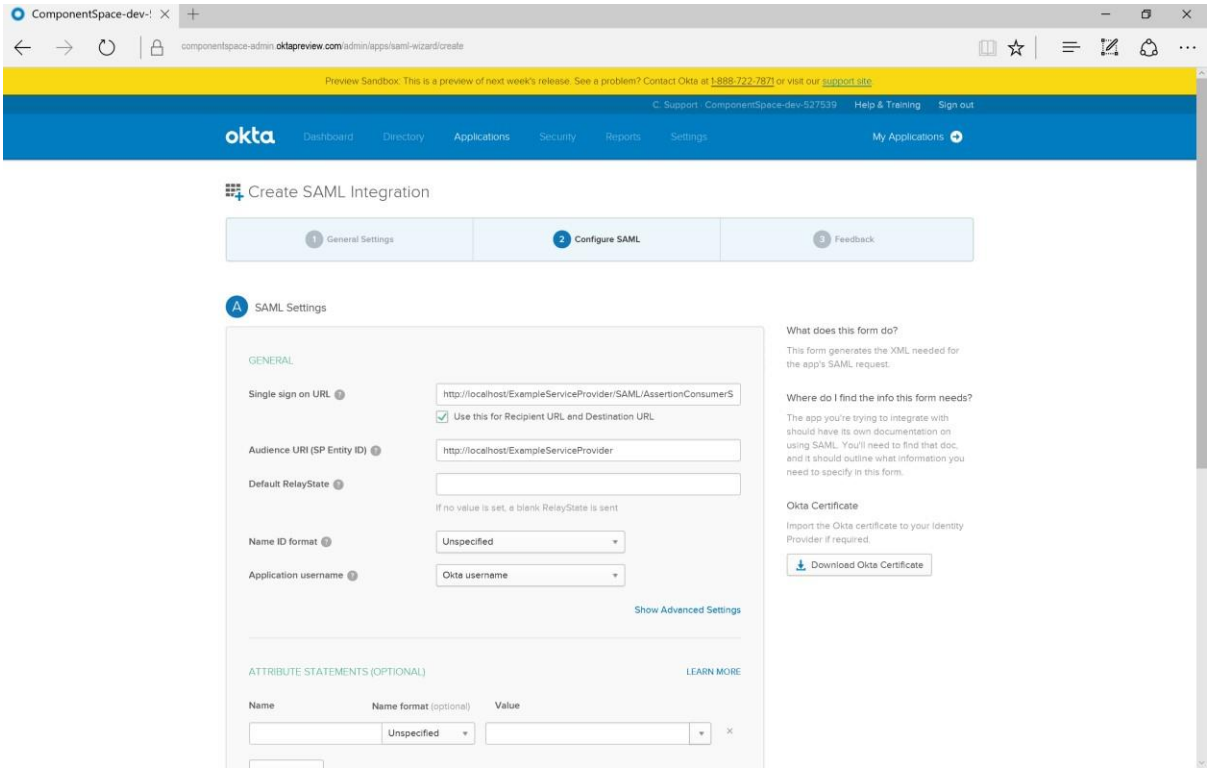
   Specify the Audience URI (SP Entity ID) - enter MyWorkDrive as the audience URI.

   Relay state is not required.

   The name ID format is unspecified.

   The application user name is the Okta user name.

   Attribute and group attributes are not required.



8. Click the Show Advanced Settings link and check the Enable Single Logout option.

   Specify the single logout service URL (eg https://YourMWDServer.yourdomain.com/SAML/SLOService.aspx) as the logout URL.

   Specify the SP Issuer. This is the local service provider name – Enter “MyWorkDrive”.

   Specify the service provider certificate used to sign logout requests. This is your own SSL certificate that is one of the following 3 types:

   1. (Recommended) public certificate specifically fo SAML installed on the MyWorkDrive Server. For example: https://saml.yourdomain.com.

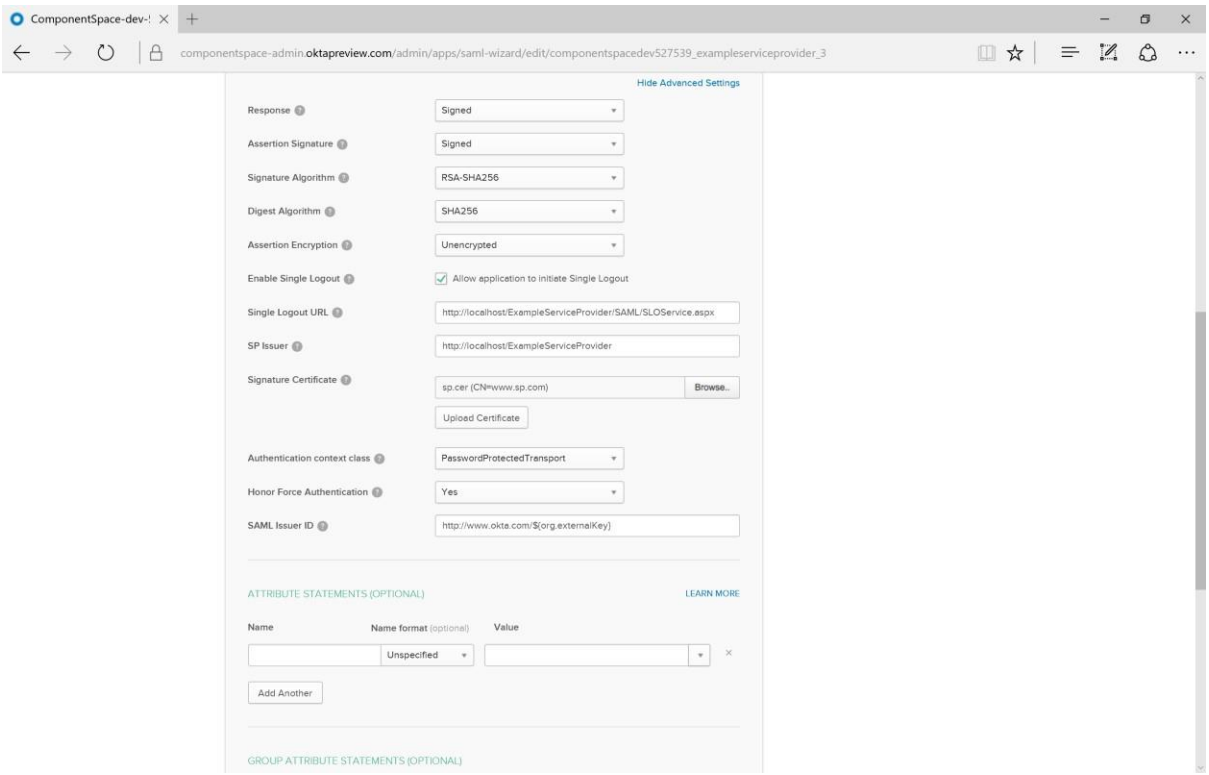
   A public copy <u>without</u> the private key should be exported and uploaded here to Okta (in a later step we will place the certificate pfx file with the private key in the MyWorkDrive Server SAML folder for use by MyWorkDrive for signing SAML). Click the Upload Certificate button.

   2. The same public certificate used for your MyWorkDrive server web address. For example: https://share.yourdomain.com

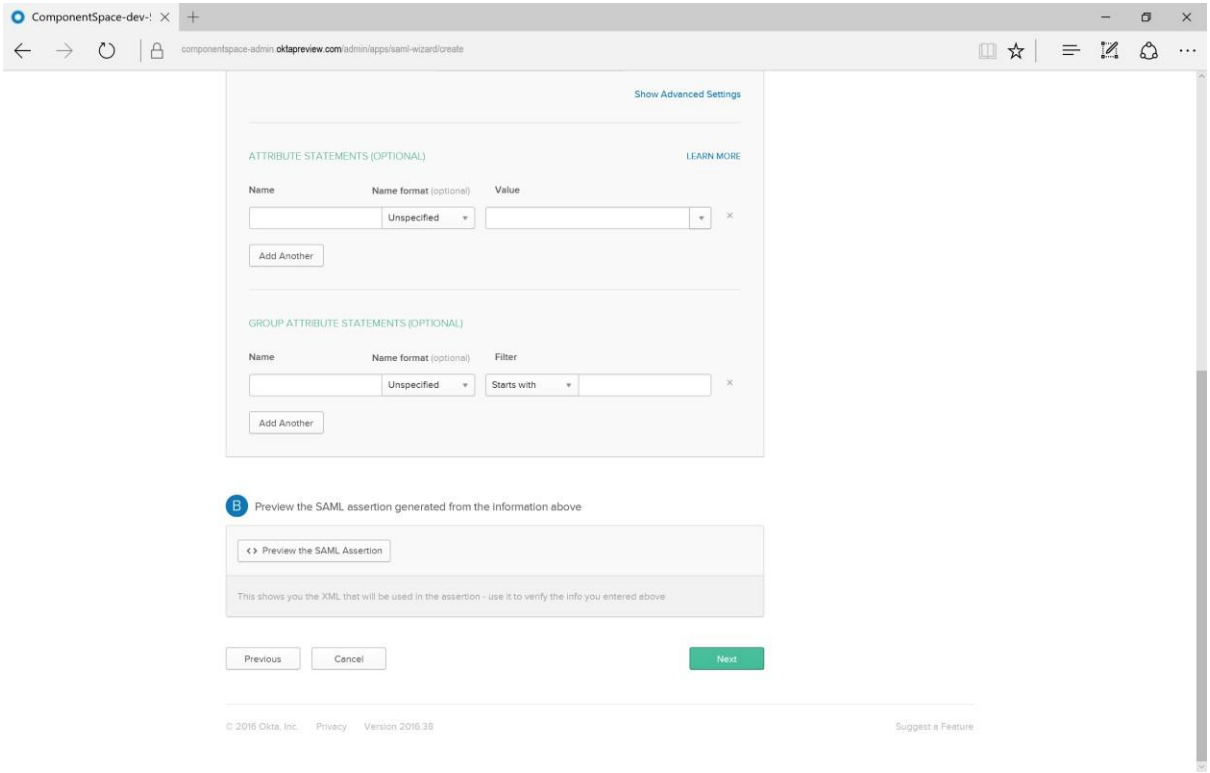
   A public copy <u>without</u> the private key should be exported and uploaded here to Okta (in a later step we will place the certificate pfx file with the private key in the MyWorkDrive Server SAML folder for use by MyWorkDrive for signing SAML). Click the Upload Certificate button.

   3. Your own Self Signed SSL Certificate that you generate using IIS Administrator.

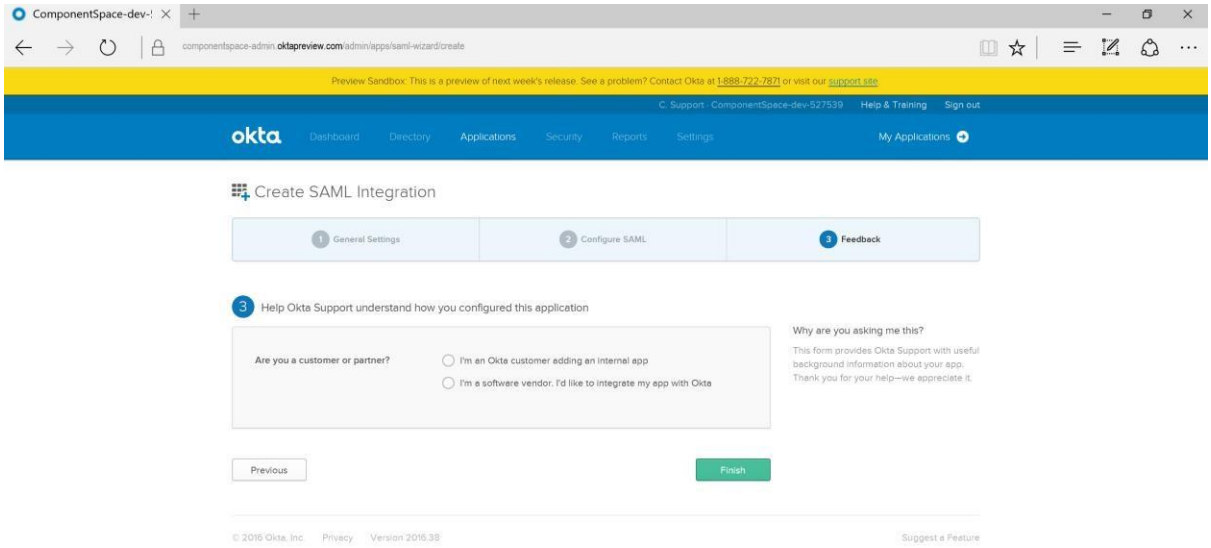
A public copy <u>without</u> the private key should be exported and uploaded here to Okta (in a later step we will place the certificate pfx file with the private key in the MyWorkDrive Server SAML folder for use by MyWorkDrive for signing SAML). Click the Upload Certificate button.



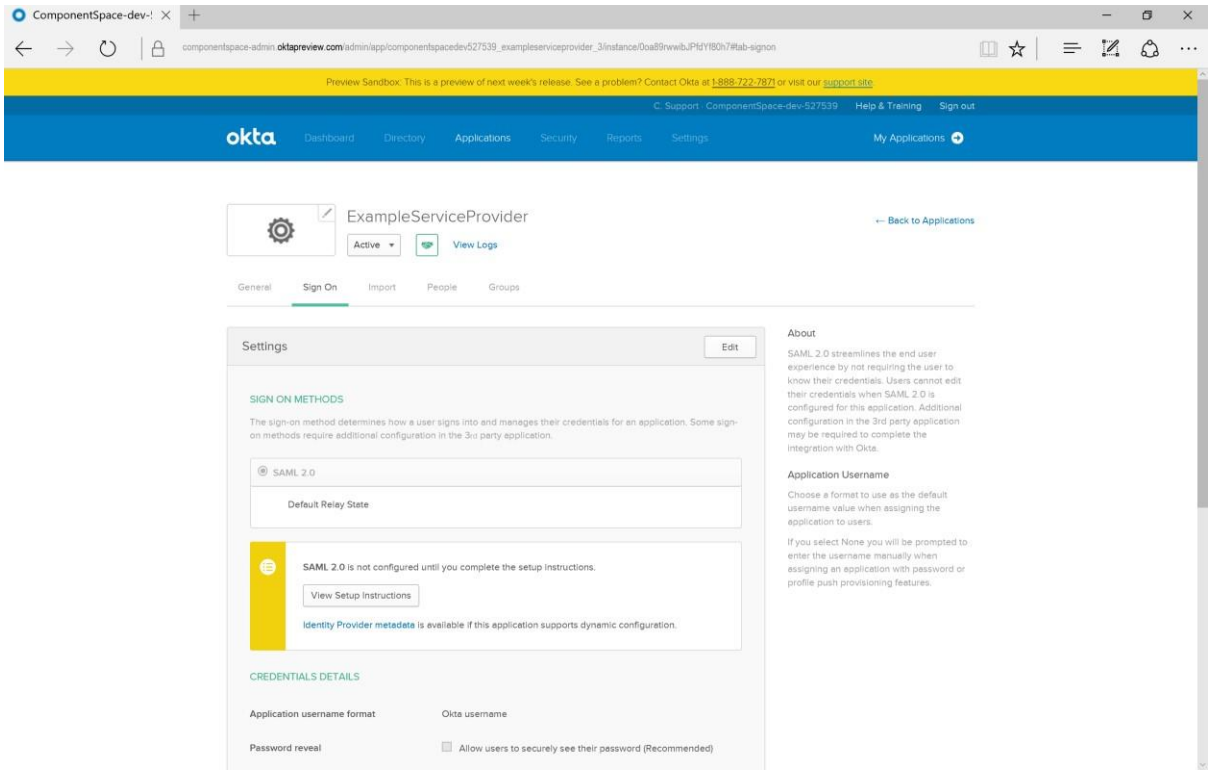
9. Click the Next button.



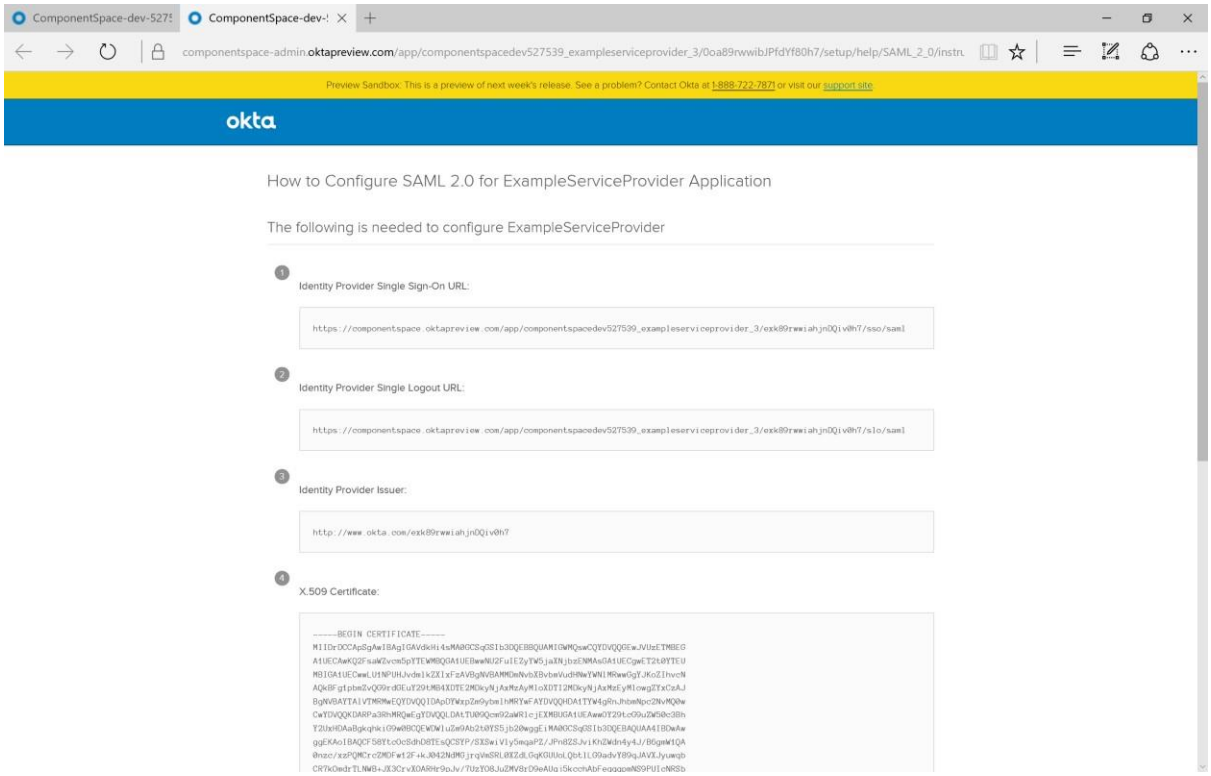
10. Click the Finish button.



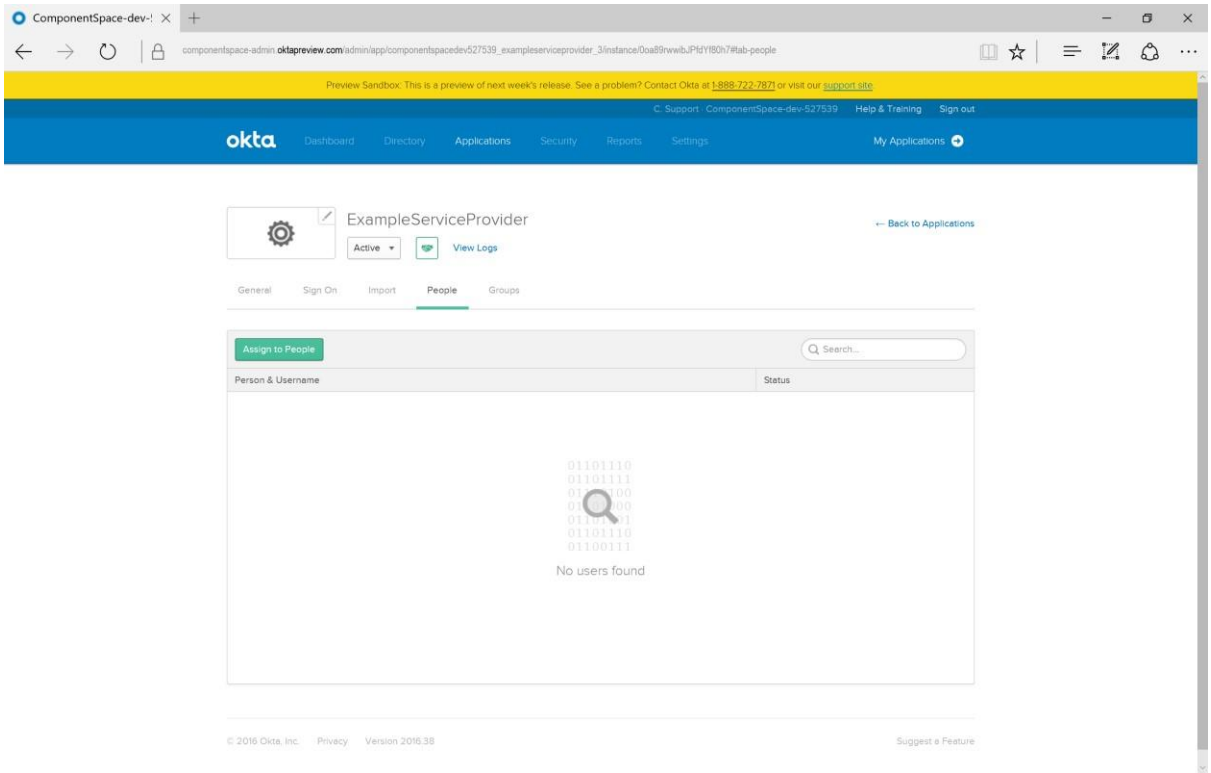
11. View the setup instructions or click the Identity Provider metadata link to download the SAML metadata.



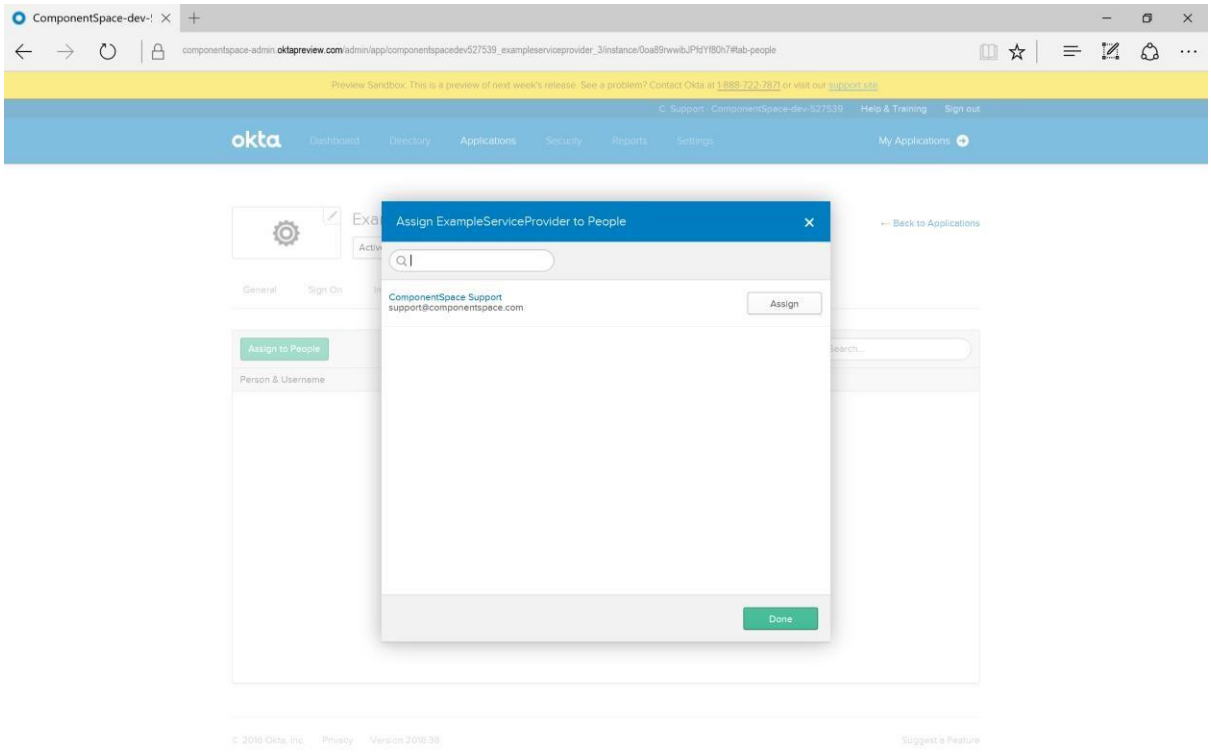
12. Click the View Setup Instructions and record the details. These will be required when configuring the service provider.



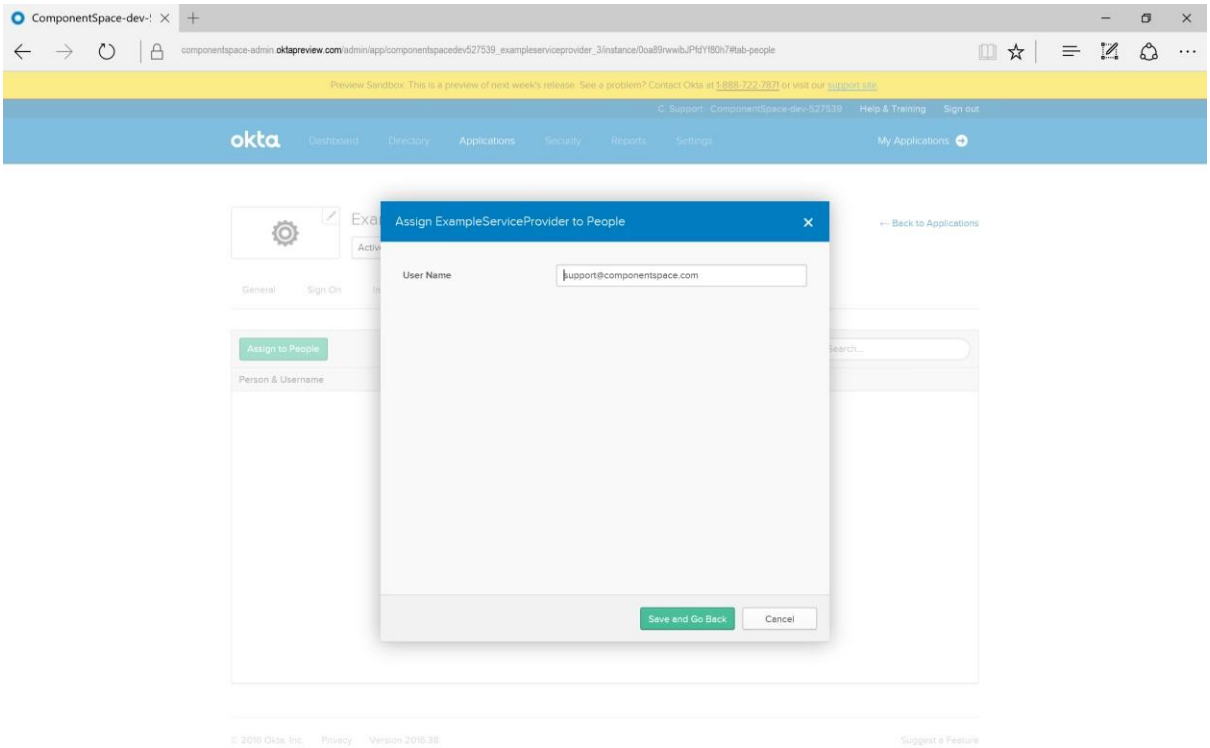
13. Click the People link and the Assign to People button. For testing a manually created a user with the same username upn suffix – okta@yourdomain.com and password can be used.



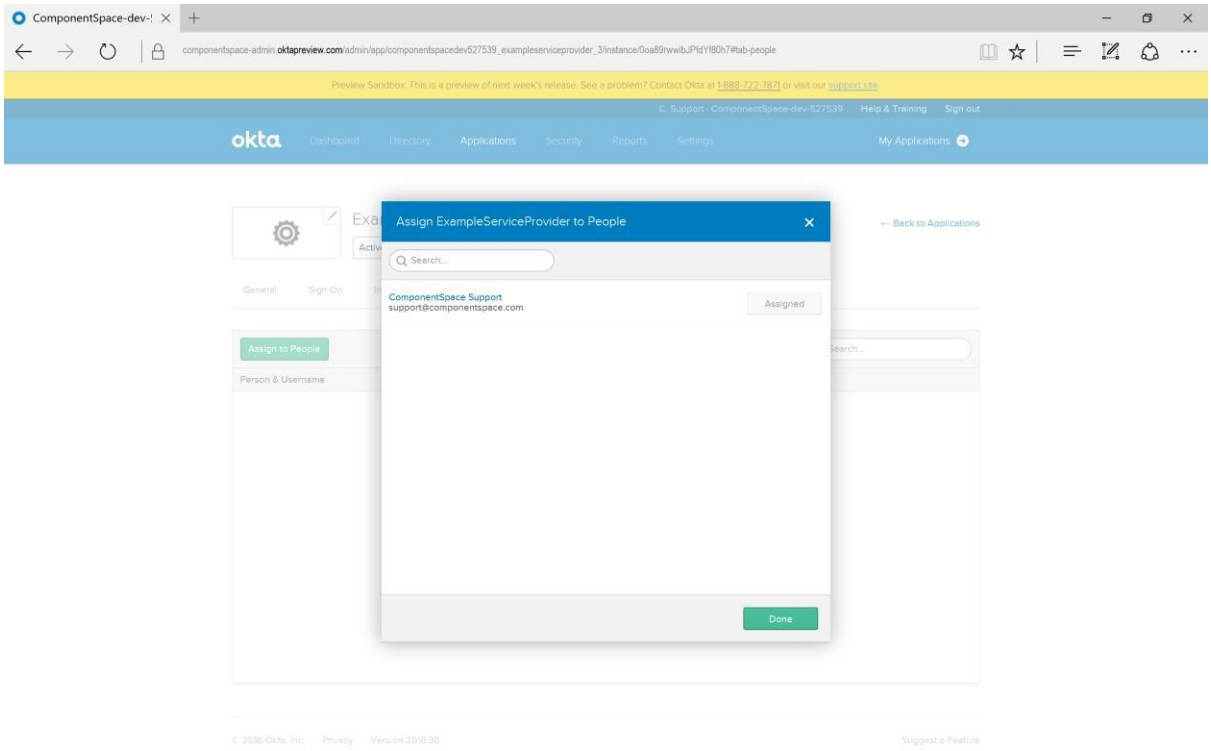
14. Select a user and click the Assign button.



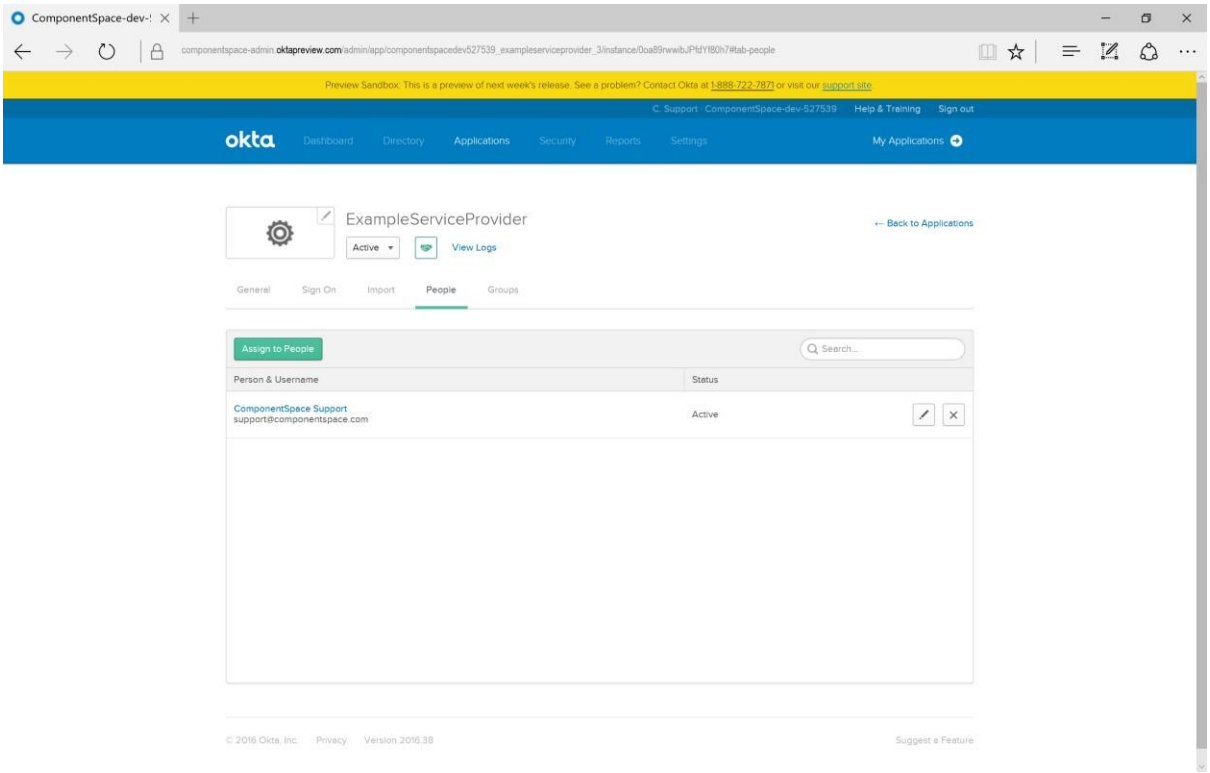
15. Click the Save and Go Back button.



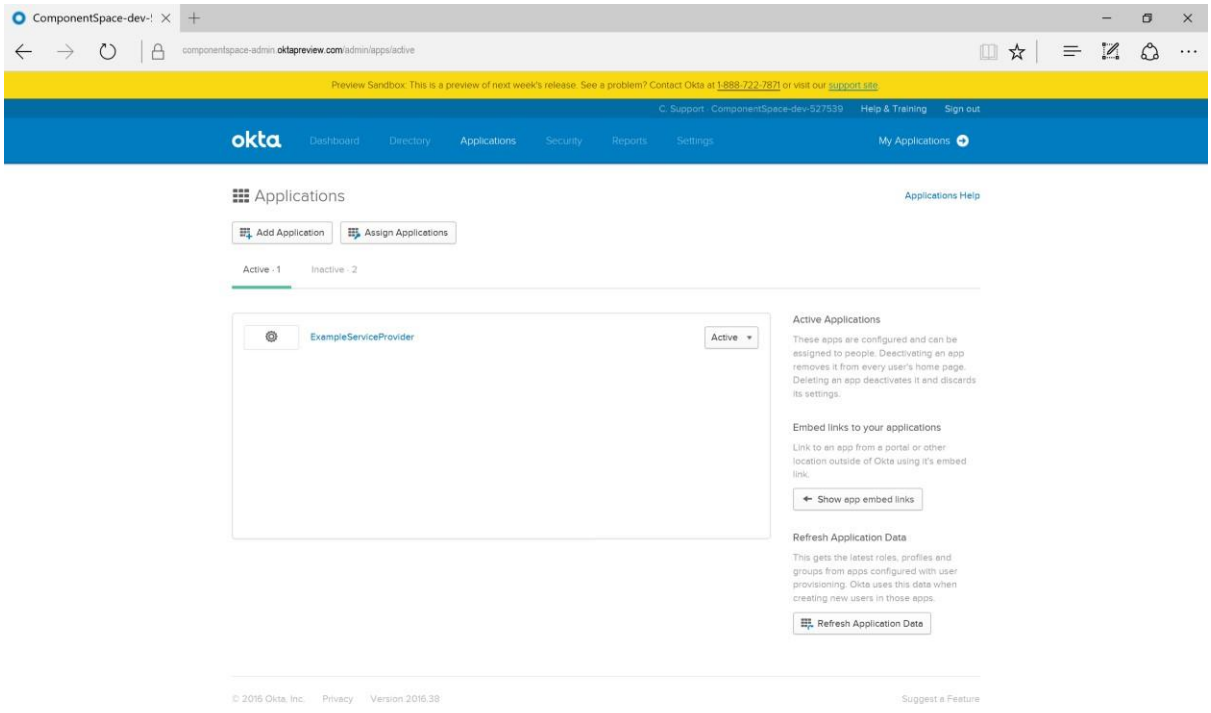
16. Click the Done button.



17. Confirm the user is listed.



18. Click the Back to Applications link and confirm the application is listed.



MyWorkDrive Server Configuration

1. Update the saml.config located in C:\Wanpath\WanPath.Data\Settings to uncomment out the <PartnerIdentityProvider> entry for Okta located in
2. Place your SSL Certificate PFX export file into C:\Wanpath\WanPath.Data\Settings\Certificates and reference it in the service provider section with the password you used during the export.

3. In the Okta Identify provider section: Set the Name to the identity provider issuer. This value is also the metadata entityID.

4. In the Okta Identify provider section: Set the SingleSignOnServiceUrl to the identity provider single sign-on URL.

5. In the Okta Identify provider section: Set the SingleLogoutServiceUrl to the identity provider single logout URL.

6. Download the partner certificate file or copy it from the identity provider metadata to C:\Wanpath\WanPath.Data\Settings\Certificates and update the Okta PartnerCertificateFile section with the complete path and name of the file.

The partner identity provider configuration section should be similar to the following saml.conf

```
<!-- Okta -->
  <PartnerIdentityProvider Name=" http://www.okta.com/ exxxxxdasDbO3SoOGQ355"
                Description="Okta"
```

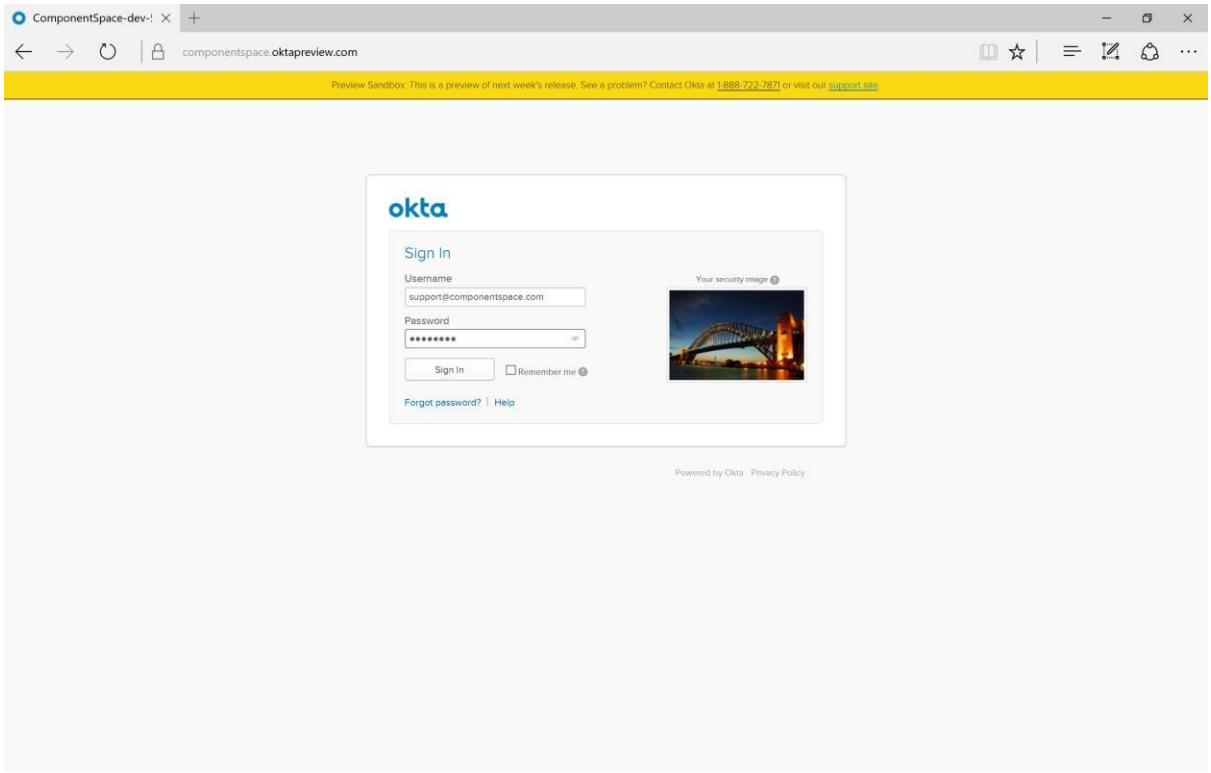
```
SignAuthnRequest="true"
SignLogoutRequest="true"
SignLogoutResponse="true"
WantLogoutRequestSigned="true"
WantLogoutResponseSigned="true"

SingleSignOnServiceUrl="hhttps://yourcompany.okta.com/app/yourcompany_mwd_
1/exxxxxdasDbO3SoOGQ355/sso/saml"

SingleLogoutServiceUrl="https://yourcompany.okta.com/app/yourcompany_mwd_1
/exxxxxdasDbO3SoOGQ355/slo/saml"
PartnerCertificateFile="C:\wanpath\WanPath.Data\Settings\Certificates\okta.cer"/>
```

The Service provider section configuration should be similar to the following saml.conf

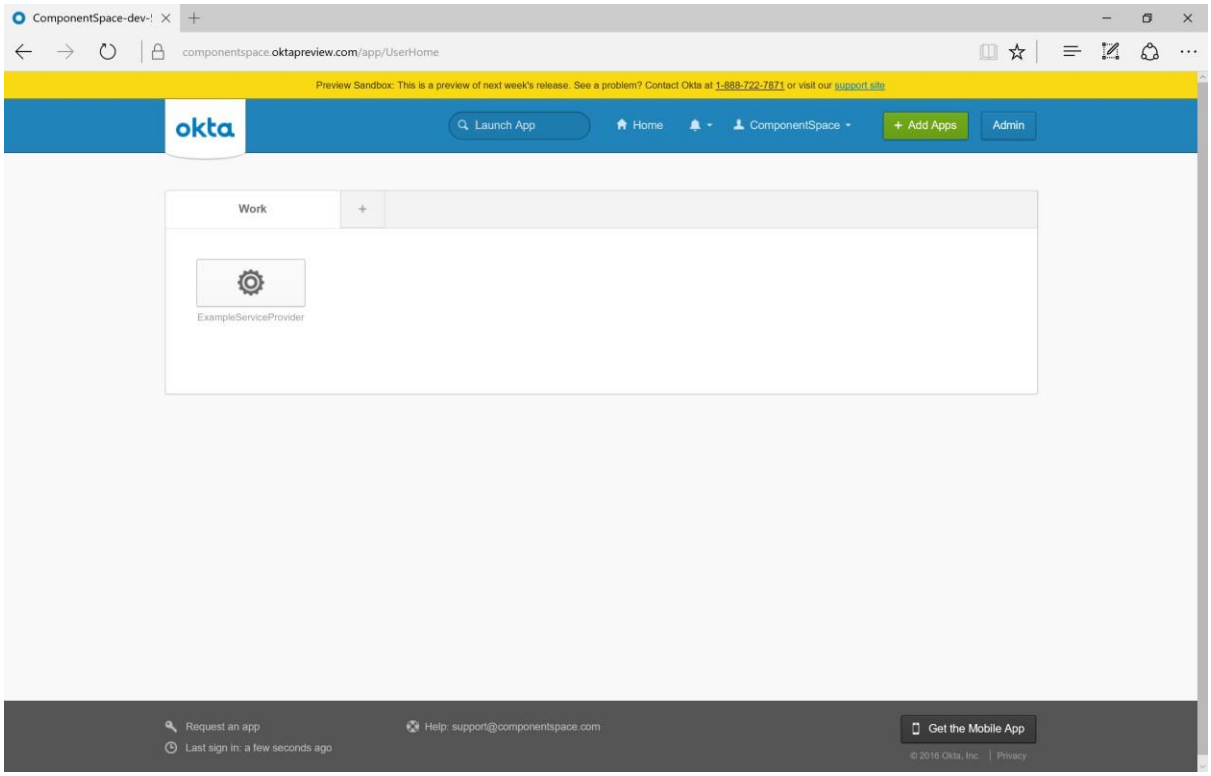
```
<ServiceProvider Name="MyWorkDrive"
        Description="MWD Service Provider"
        AssertionConsumerServiceUrl="~/SAML/AssertionConsumerService.aspx"
        LocalCertificateFile="C:\Wanpath\WanPath.Data\Settings\Certificates\yourdomain.pfx"
        LocalCertificatePassword="password"/>
```

Test Okta initiated SSO

1. Log into Okta.



2. Click the MyWorkDrive application.

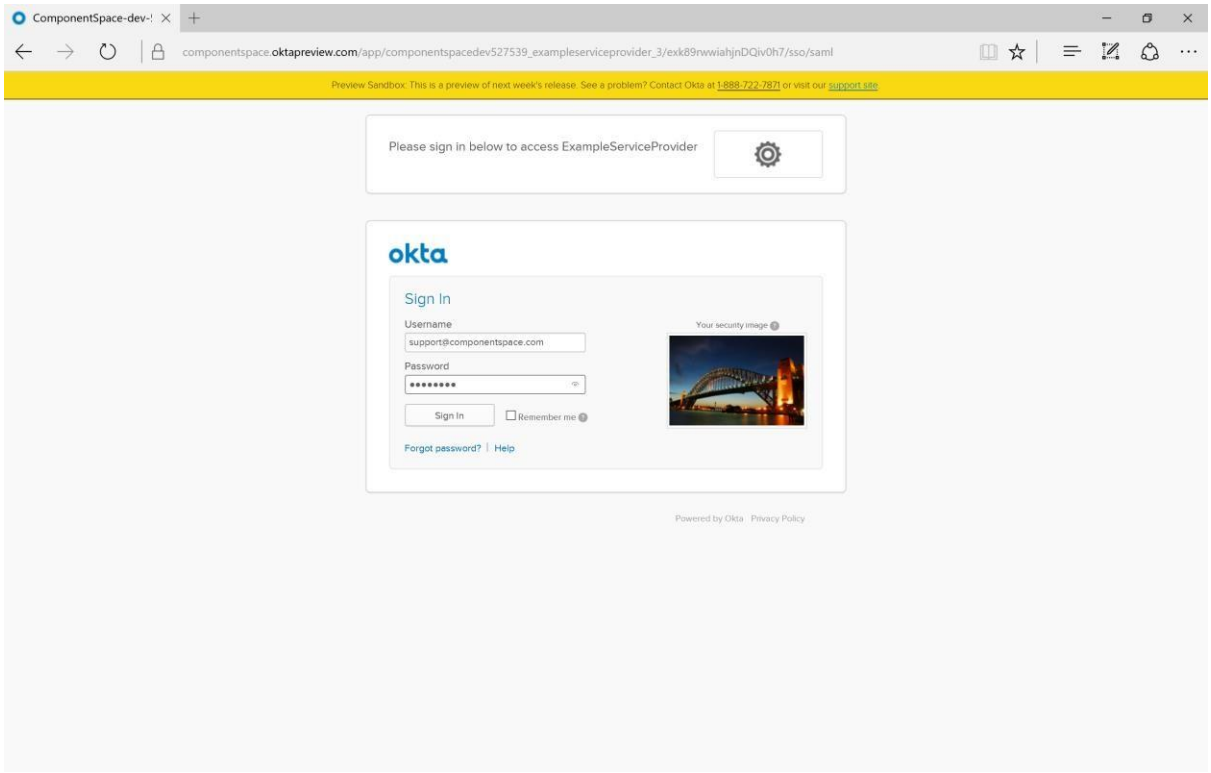


3. You are now automatically logged into the MyWorkDrive Web File Manager application.

MyWorkDrive Initiated SSO

1. Browse to the url of your MWD Site /Account/Login-SAML.aspx (for example https://MWDserver.yourdomain.com/Account/Login-SAML.aspx) and click the link to SSO to the identity provider.

2. Login to Okta.



3. You are now automatically logged into Okta.

Single Logout

1. Click the logout button. You are now logged out of the identity provider and service provider.