

SAML Lab Part 1 - Enable Tableau Online for SAML

This lab assumes you have a Tableau Online Site and an Okta Development Account. If you have already configured your site for SAML you may want to save your existing configuration and create a new configuration for the lab as we will use Okta to configure SCIM and MFA.

Step 1 - Sign into Online and Enable SAML

In your Web Browser Log into your Online site as a Site Administrator and Select the **Authentication** section from the **Settings** menu. Create a Bookmark for your site - you will use it several times during the lab.

Under Authentication types, Check 'Enable an additional authentication method'. Then, under SAML, click 'Edit Connection'.

The screenshot shows the Tableau Online Settings page for a site named 'Tableau Rocks (BETA)'. The 'Authentication' tab is selected. The page is divided into several sections: 'Connected Clients', 'Authentication types', 'Manage users', 'Default authentication type for embedded views', and 'System for Cross-domain Identity Management (SCIM)'. In the 'Authentication types' section, the 'Tableau' option is checked, and 'Enable an additional authentication method' is also checked. Under this, 'oktapreview.com (SAML)' is selected as the additional method. In the 'Default authentication type for embedded views' section, 'oktapreview.com (SAML)' is selected. In the 'System for Cross-domain Identity Management (SCIM)' section, 'Enable SCIM' is unchecked, and the 'Base URL' field is empty.

← → ↻ <https://10ax.online.tableau.com/#/site/tableaurocksbeta/authentication>

Apps Bookmarks Who : Tableau Active TC18 - Big Data Strat Tableau Help | Table mytableau Log my time! Strategic SC Projects

Tableau Rocks (BETA) Content Users Groups Schedules Tasks Status Settings

General **Authentication** Bridge Extensions

Connected Clients

Tableau clients such as mobile apps, Tableau Bridge, and others can stay authenticated to this site after the user provides sign-in credentials the first time. Connections are established using secure tokens that uniquely identify each user and client, without storing the user's credentials.

☒ Allow connected clients for this Tableau Online site.

Authentication types [Learn more](#)

☒ Tableau
This is the default authentication type for Tableau Sites, and is always enabled.

☒ Enable an additional authentication method

☐ Google
This allows you to set OpenID as your users' authentication method

☒ oktapreview.com (SAML)
This allows you to set up your SAML provider to work with Tableau so your users can sign in to this Tableau Site with SAML (i.e. Okta, OneLogin, etc.)
[Edit Connection...](#)

Manage users

[Select users](#) Select existing users and change their authentication method.

[Add users](#) Enter the username and email of a new user that will authenticate via the selected method.

Default authentication type for embedded views

☐ Allow users to choose their authentication type

☐ Tableau

☒ oktapreview.com (SAML)

System for Cross-domain Identity Management (SCIM) [Learn more](#)

Allow a third-party identity provider to manage users on this site.

☐ Enable SCIM

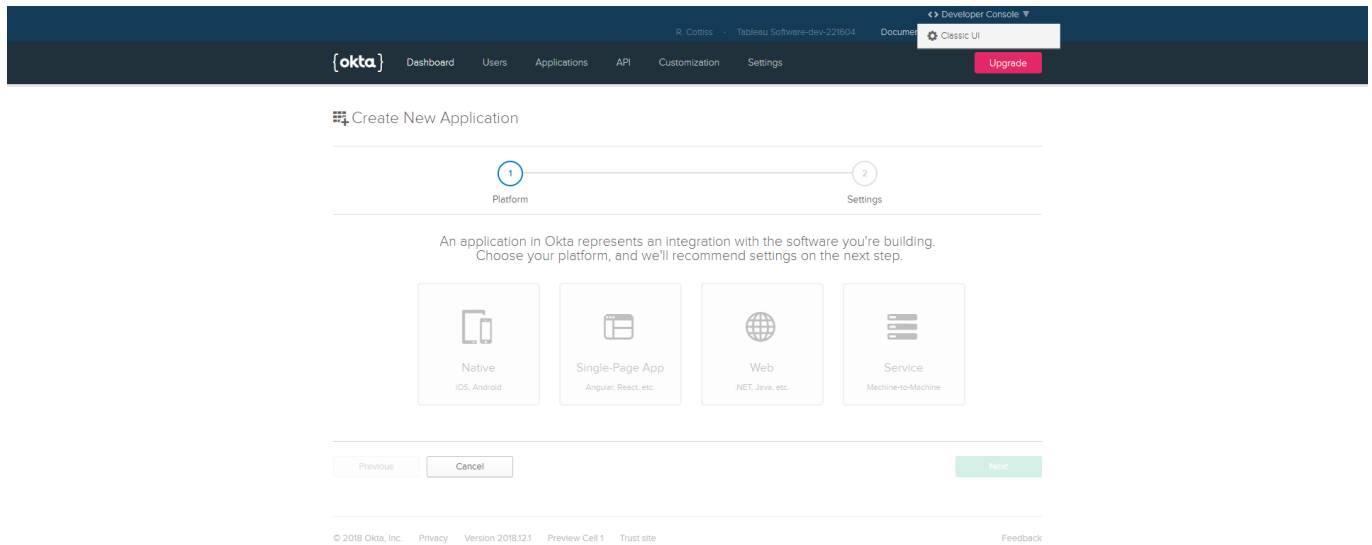
Base URL

[Generate New Secret](#)

Step 2 - Sign into the Okta Development Console and create a new application

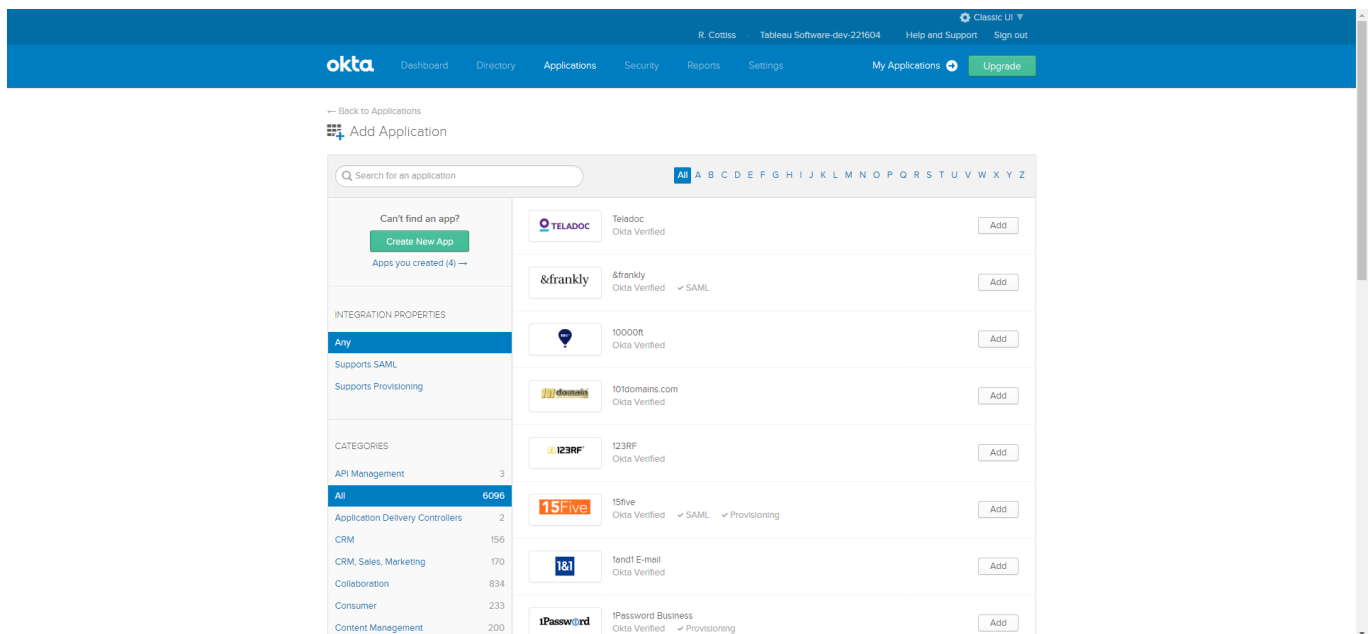
The console will be at [Okta - Dev Console](#) where xxxxxx is your personal dev account (sent by Okta). Create a Bookmark for this link - you will use it several times during the lab.

You may need to switch from the **Developer Console** to the **Classic UI**. The Developer console looks like this after clicking **Add Application** You can do that from the top right corner

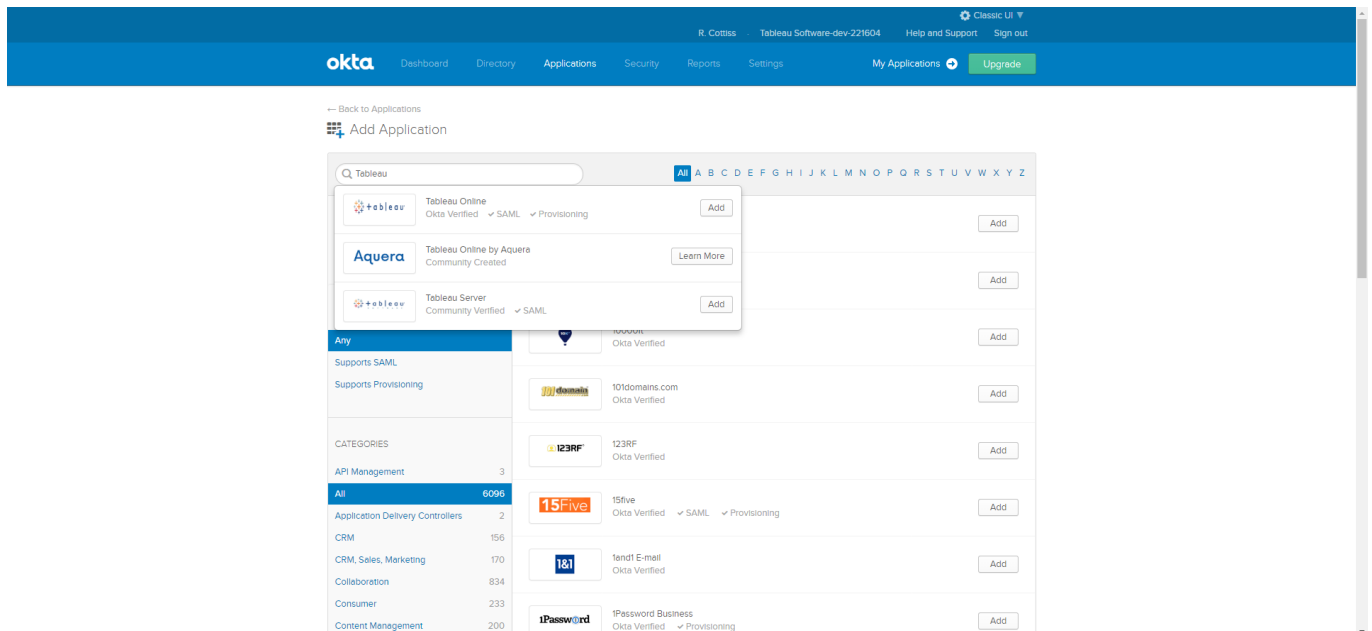


<https://dev-221604-admin.oktapreview.com/dev/console/apps/new#>

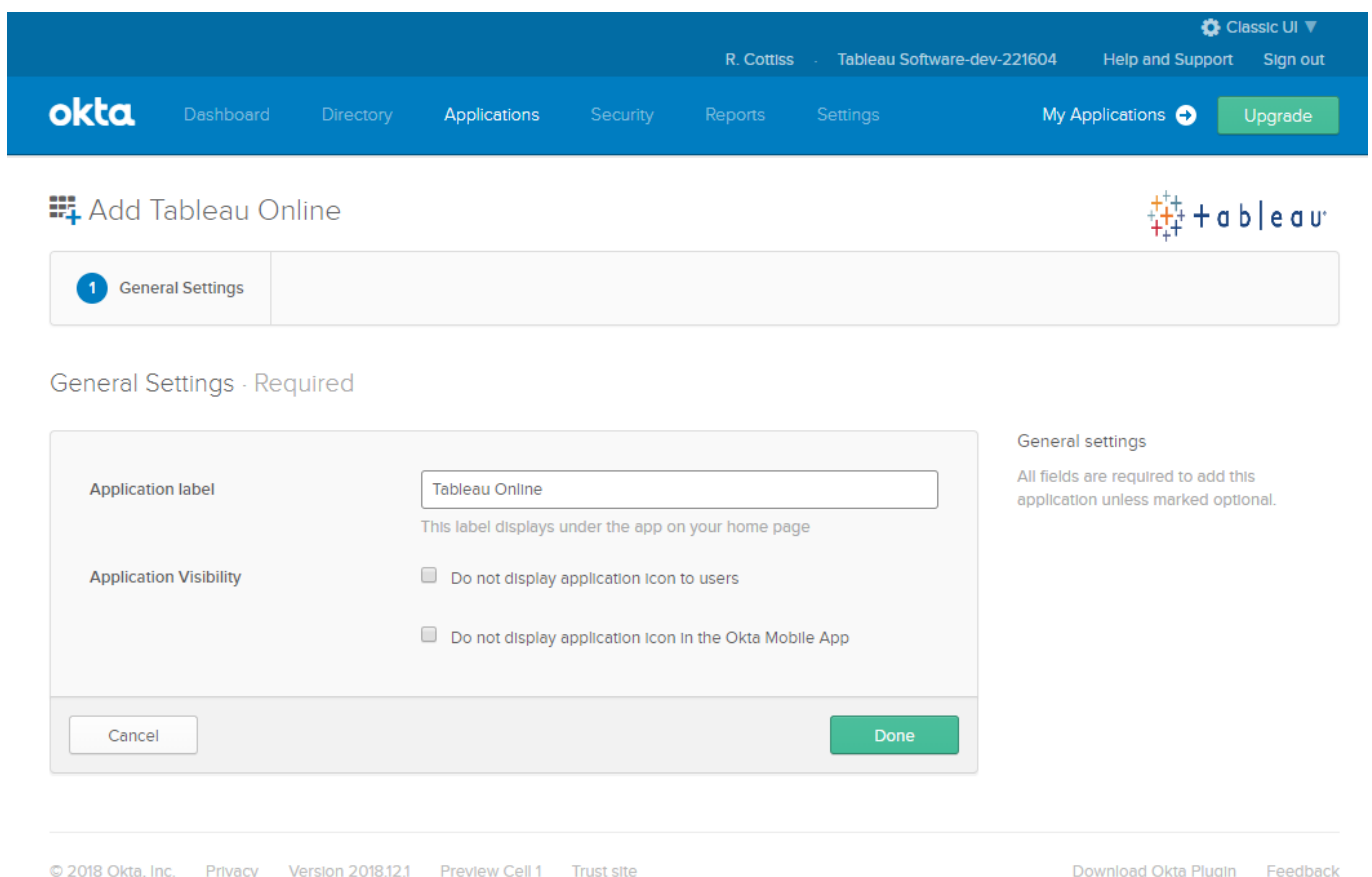
The Classic UI looks like this:



Search for Tableau and Select Tableau Online:



You can change the Application Label and change the application visibility. For the lab you can leave the defaults. Click **Done** to continue



The **Assignments** tab will display next. You can add users here but we are going to enable automatic provisioning with SCIM so we will add users later. If you do not want to enable SCIM you can add users and/or groups on this tab.

Classic UI

R. Cottiss · Tableau Software-dev-221604 · Help and Support · Sign out

Okta

Dashboard · Directory · Applications · Security · Reports · Settings

My Applications · Upgrade

← Back to Applications

Tableau Online (2)

Active · View Logs

General · Sign On · Provisioning · Import · Assignments · Push Groups

Assign · Convert Assignments · Search... · People

FILTERS

People

Groups

Person

Type

01101110

01101111

01101100

01101000

01101101

01101110

01100111

No users found

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app. [Go to self service settings](#)

Requests Disabled





Edit

For now select the **Sign On** tab and then the **edit** button:

Step 3 - Configure the Okta Sign On details and Import IdP Metadata to Tableau Online

← Back to Applications

Tableau Online (2)

Active     [View Logs](#)

General **Sign On** Provisioning Import Assignments Push Groups

Settings Edit

SIGN ON METHODS


The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ SAML 2.0

Default Relay State

Disable Force Authentication ☒

 **SAML 2.0** is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Tableau Online proprietary sign-on option or general setting.

ACS URL

Tableau Server entity ID

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

You can now add the *ACS URL* and *Tableau Server entity ID* from your Online site.



Okta does not read the Metadata file but uses the second option in Step 1.

You can click on the **View Setup Instructions** on the Okta page. This link is specific to your Site as it includes the link to the Idp Metadata. The setup instructions tell you to the following:

Copy the Entity ID and ACS from Tableau to Okta:

General

Authentication

Bridge

Extensions

Connected Clients

Tableau clients such as mobile apps, Tableau Bridge, and others can stay authenticated to this site after the user provides sign-in credentials the first time. Connections are established using secure tokens that uniquely identify each user and client, without storing the user's credentials.

☒ Allow connected clients for this Tableau Online site.

Authentication types [Learn more](#)

☒ Tableau

This is the default authentication type for Tableau Sites, and is always enabled.

☒ Enable an additional authentication method

☐ Google

This allows you to set OpenID as your users' authentication method

☒ oktapreview.com (SAML)

This allows you to set up your SAML provider to work with Tableau so your users can sign in to this Tableau Site with SAML (i.e. Okta, OneLogin, etc.)

[Edit Connection...](#)

Follow the steps below to use SAML for single sign-on.

1 Export metadata from Tableau Online

Select an option for obtaining metadata required by the Identity Provider (IdP):

- Export an XML file that contains the metadata.

or


- Copy the Tableau Online entity ID and ACS URL individually, and download the X.509 certificate and save it as a CER file.

Tableau Online entity ID	<input type="text" value="https://sso.online.tableau.com/public/sp/metadata?alias=d82b53da-7d9e-4542-b159-"/>
Assertion Consumer Service URL (ACS)	<input type="text" value="https://sso.online.tableau.com/public/sp/SSO?alias=d82b53da-7d9e-4542-b159-cdd5"/>

2 External Step: Enter metadata in your Identity Provider (IdP)

Go to your IdP's website and follow the instructions they provide to connect to a service provider (in this case, Tableau Online). Depending on your IdP, you will either import the metadata file that you exported in step 1, or manually add the Entity ID, ACS URL, and certificate information.

3 External Step: Export metadata from your Identity Provider (IdP)

 SAML 2.0 is not configured until you complete the setup instructions.
[View Setup Instructions](#)
Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Tableau Online proprietary sign-on option or general setting.

ACS URL

Enter your ACS URL. Refer to the Setup Instructions above to obtain this value.

Tableau Server entity ID

Enter your Tableau Server entity ID. Refer to the Setup Instructions above to obtain this value.

CREDENTIALS DETAILS

Application username format


Okta username ▼

Update application username on

Create and update ▼

Password reveal

☐ Allow users to securely see their password (Recommended)



Password reveal is disabled, since this app is using SAML with no password.

Save



The Form fields may be in a different order between the app. This is why exchanging metadata via the metadata files is usually the safest option if it is available. Take care to copy the fields correctly. The Entity ID looks like a URL but has the word *metadata* in it. The ACS URL is a real URL and has SSO in it.



Technically the Entity ID is just a string identifier



We do not need to download the Tableau certificate and load it into Okta. Why not?

Make sure you click

Save

Classic UI

R. Cottiss · Tableau Software-dev-221604 · Help and Support · Sign out

Okta

Dashboard · Directory · Applications · Security · Reports · Settings

My Applications · Upgrade

← Back to Applications

Tableau Online

Active

View Logs

General · Sign On · Provisioning · Import · Assignments · Push Groups

Settings

Cancel

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.
Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

Disable Force Authentication

☒

Never prompt user to re-authenticate.

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Tableau Online proprietary sign-on option or general setting.

ACS URL

https://sso.online.tableau.com/public/sp/SSO?alias=d82b53da-7d9e

Enter your ACS URL. Refer to the Setup Instructions above to obtain this value.

Tableau Server entity ID

https://sso.online.tableau.com/public/sp/metadata?alias=d82b53da-

Enter your Tableau Server entity ID. Refer to the Setup Instructions above to obtain this value.

CREDENTIALS DETAILS

Application username format

Okta username

Update application username on

Create only

Password reveal

☐ Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

Save

About

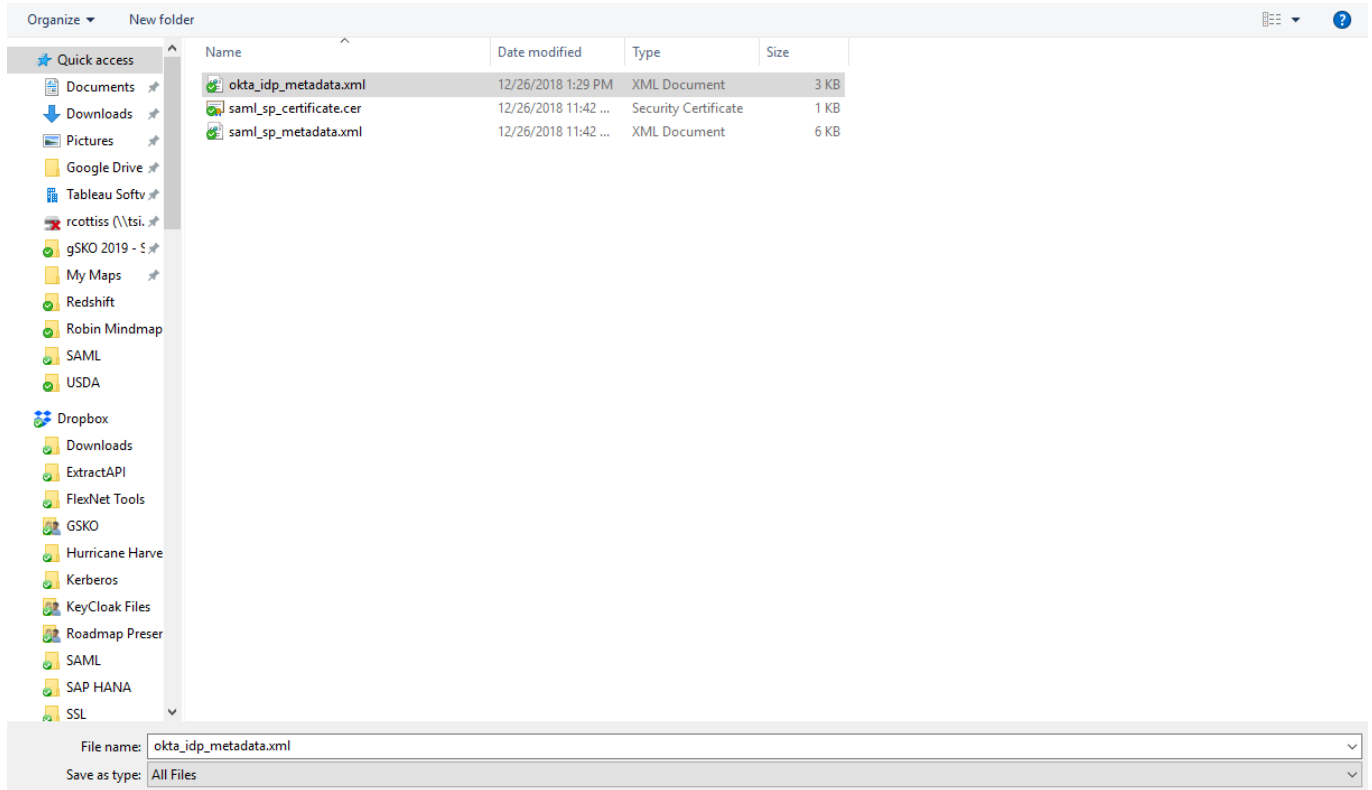
SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

8 / 22



Back in Tableau Online go to *Step 4* and Browse to the IdP metadata file you just downloaded:

4 Import metadata file into Tableau Online

IdP metadata file	<input type="text"/>	<input data-bbox="1050 1088 1244 1133" type="button" value="Browse..."/>	<input data-bbox="1267 1088 1418 1133" type="button" value="Apply"/>
IdP entity ID	<input data-bbox="461 1137 1418 1182" type="text" value="http://www.okta.com/exki3cer7wxbuEbvL0h7"/>		
SSO Service URL	<input data-bbox="461 1184 1418 1229" type="text" value="https://dev-221604.oktapreview.com/app/tableauonline/exki3cer7wxbuEbvL0h7/sso/s"/>		
IdP is not configured to support SAML single logout (SLO)			
<input data-bbox="229 1267 486 1312" type="button" value="Test Connection"/>	<input data-bbox="1198 1267 1418 1312" type="button" value="Remove IdP"/>		

Step 4 - Configure Okta Provisioning

Tableau Online now supports automatic user provisioning from Okta using an open standard called [System for Cross-domain Identity management \(SCIM\)](#)

Configuring SCIM requires some setup in Tableau Online and Okta.

In Tableau Online you enable SCIM at the bottom of the Authentication Setup page:

System for Cross-domain Identity Management (SCIM) [Learn more](#)

Allow a third-party identity provider to manage users on this site.

☒ Enable SCIM

Base URL

Store the secret in a safe place. If you lose it, you'll have to return here to generate a new one.

In Okta you select the Provisioning Tab in the Applications menu:

← Back to Applications

Tableau Online (2)

Active

General Sign On Provisioning Import Assignments Push Groups

SETTINGS

API Integration

Tableau Online: Configuration Guide

Provisioning Certification: Partner Built EA

This provisioning integration is partner-built by Tableau

Contact partner support: customerservice@tableau.com

Provisioning is not enabled

Enable provisioning to automate Tableau Online user account creation, deactivation, and updates.

Configure API Integration

Click on **Configure API Integration** then check *Enable API integration* and copy the *Base URL* and *API Token* from the Online setup page.

← Back to Applications

Tableau Online

Active

General Sign On Provisioning Import Assignments Push Groups

SETTINGS

API Integration

Tableau Online: Configuration Guide

Provisioning Certification: Partner Built EA

This provisioning integration is partner-built by Tableau

Contact partner support: customerservice@tableau.com

Cancel

Tableau Online was verified successfully!

☒ Enable API integration

Enter your Tableau Online credentials to enable user import and provisioning features.

Base URL


https://scim.online.tableau.com/pods/10ax/1sites/d82b53da-7d9e-4542-b159-

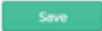
API Token

Test API Credentials



The Secret API Token will not show again and if you forget it you will need to generate a new one to configure Okta.

You can click **Test API Credentials** to make sure you copied the Base URL and Secret correctly. Click  when done.

You will need to Enable at least **Create User**. Do this by selecting **To App** in the Provisioning Settings. Enable *Create Users* and *Deactivate Users* check boxes and click . This will enable Okta to make changes to Tableau Online.

Classic UI

R. Cottiss · Tableau Software-dev-221604 Help and Support Sign out

okta

Dashboard Directory Applications Security Reports Settings

My Applications Upgrade

← Back to Applications

+ a b l e a u

Tableau Online

Active View Logs

General Sign On Provisioning Import Assignments Push Groups

SETTINGS

To App

To Okta

API Integration

okta → + a b l e a u

Provisioning to App

Cancel

Create Users

Enable

Creates or links a user in Tableau Online when assigning the app to a user in Okta.

The default username used to create accounts is set to Okta username.

Deactivate Users

Enable

Deactivates a user's Tableau Online account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Save

Tableau Online Attribute Mappings

Select a(n) Tableau Online attribute to set its value based on values stored in Okta.

Go to Profile Editor

Force Sync

Attribute	Attribute Type	Value	Apply on	
Username userName	Personal	Configured in Sign On settings		
Given name givenName	Group	user.firstName	Create	<div></div> <div></div>
Family name familyName	Group	user.lastName	Create	<div></div> <div></div>
Primary email email	Group	user.email	Create	<div></div> <div></div>

Hide Unmapped Attributes

Optionally you can configure SCIM so that the users are maintained in Online and then imported into Okta. Review the Settings in the **To Okta** page:

Dashboard Directory Applications Security Reports Settings My Applications Upgrade

← Back to Applications

tableau

Tableau Online

Active

View Logs

General

Sign On

Provisioning

Import

Assignments

Push Groups

SETTINGS

To App

To Okta

API Integration

tableau

→

okta

General

Edit

Import users from Tableau Online to create new Okta users. If the Okta user already exists, the two accounts will automatically be linked. Imported users are assigned Tableau Online access when they are confirmed on the Import tab.

Schedule import

never

Select never if you prefer to import manually.

Okta username format

Email address

Select the username users should enter to log into Okta.

Update application username on

Create only

Max Import Unassignment

20% (default)

User Creation & Matching

Edit

Imported user is an exact match to Okta user if

☐ Okta username format matches

☒ Email matches

☐ The following combination of attributes matches:

☐ Partial match on first and last name

Allow partial matches

☐ Partial match on first and last name

Confirm matched users

☐ Auto-confirm exact matches

☐ Auto-confirm partial matches

Confirm new users

☐ Auto-confirm new users

☐ Auto-activate new users

Okta Attribute Mappings

Select a(n) Okta attribute to set its value based on values stored in Tableau Online.

Go to Profile Editor

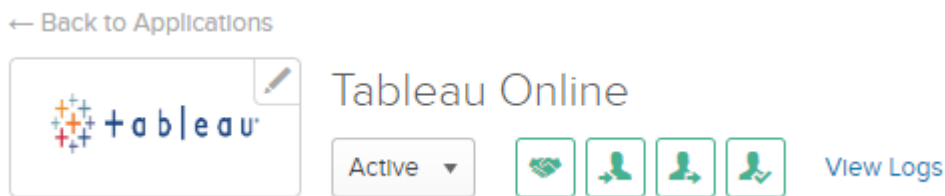
Force Sync

Okta Attribute	Value	Apply on	
Username login	Configured in Sign On settings		
First name firstName	appuser.givenName	Create	<div><div></div><div></div></div>
Last name lastName	appuser.familyName	Create	<div><div></div><div></div></div>
Primary email email	appuser.email	Create	<div><div></div><div></div></div>

Show Unmapped Attributes

14 / 22

If you have correctly configured Okta to add and deactivate users in Online you should see the Icons enabled on the Application in Okta like this:



The two push options on the right should NOT be grayed out.

Step 5 - Add a User to Okta

Now that Okta and Tableau Online are configured you can add a new user to Okta and test the SCIM provisioning (and de-provisioning). Most Tableau customers will link Okta to an external Directory or Identity Store like Active Directory or LDAP so pushing from Okta to Online is a good option. Also, most customers will manage users via groups but in this lab you can create a single user directly in Okta then assign the user to our Tableau Online application.

In the **Directory** menu select **People** then **Add Person**

Classic UI

R. Cottiss · Tableau Software-dev-221604 · Help and Support · Sign out

okta

Dashboard · Directory · Applications · Security · Reports · Settings · My Applications · Upgrade

People

Help

Add Person · Reset Passwords · Reset Multifactor · More Actions

Search...

	Person & Username	Primary Email	Status
Everyone	119	Colin Adler cadler@tableau.rocks	cadler@tableau.rocks Active
ONBOARDING		Tableau Administrator tabadmin@tableau.rocks	tabadmin@tableau.rocks Active
Staged	0	Anna Andreadi aandreadi@tableau.rocks	aandreadi@tableau.rocks Active
Pending user action	0	Vikram Bandarupalli vbandarupalli@tableau.rocks	vbandarupalli@tableau.rocks Active
ACTIVE		Luca Bandini lbandini@tableau.rocks	lbandini@tableau.rocks Active
Active	113	Zeeshan Baqir zbaqir@tableau.rocks	zbaqir@tableau.rocks Deactivated
Password Reset	0	John Barnes jbarnes@tableau.rocks	jbarnes@tableau.rocks Active
Password Expired	1	Ashley Bass abass@tableau.rocks	abass@tableau.rocks Active
Locked out	0	Nick Beaton nbeaton@tableau.rocks	nbeaton@tableau.rocks Active
INACTIVE		Chris Beck cbeck@tableau.rocks	cbeck@tableau.rocks Active
Suspended	0	Jeff Black jblack@tableau.rocks	jblack@tableau.rocks Active
Deactivated	6	Kyle Bohac kylebohac@tableau.rocks	kylebohac@tableau.rocks Active

Enter the details of a new Okta user.

This user can be assigned to multiple applications in Okta and that is an extra step below.

Click 

You can assign users to applications in several ways. You can either do it from the Directory by clicking the user then **Assign Applications**

Classic UI

R. Cottiss - Tableau Software-dev-221604 Help and Support Sign out

Okta

Dashboard Directory Applications Security Reports Settings My Applications Upgrade

Jane Smith

jsmith@tableau.rocks

Active View Logs

Reset Password More Actions

Applications Groups Profile

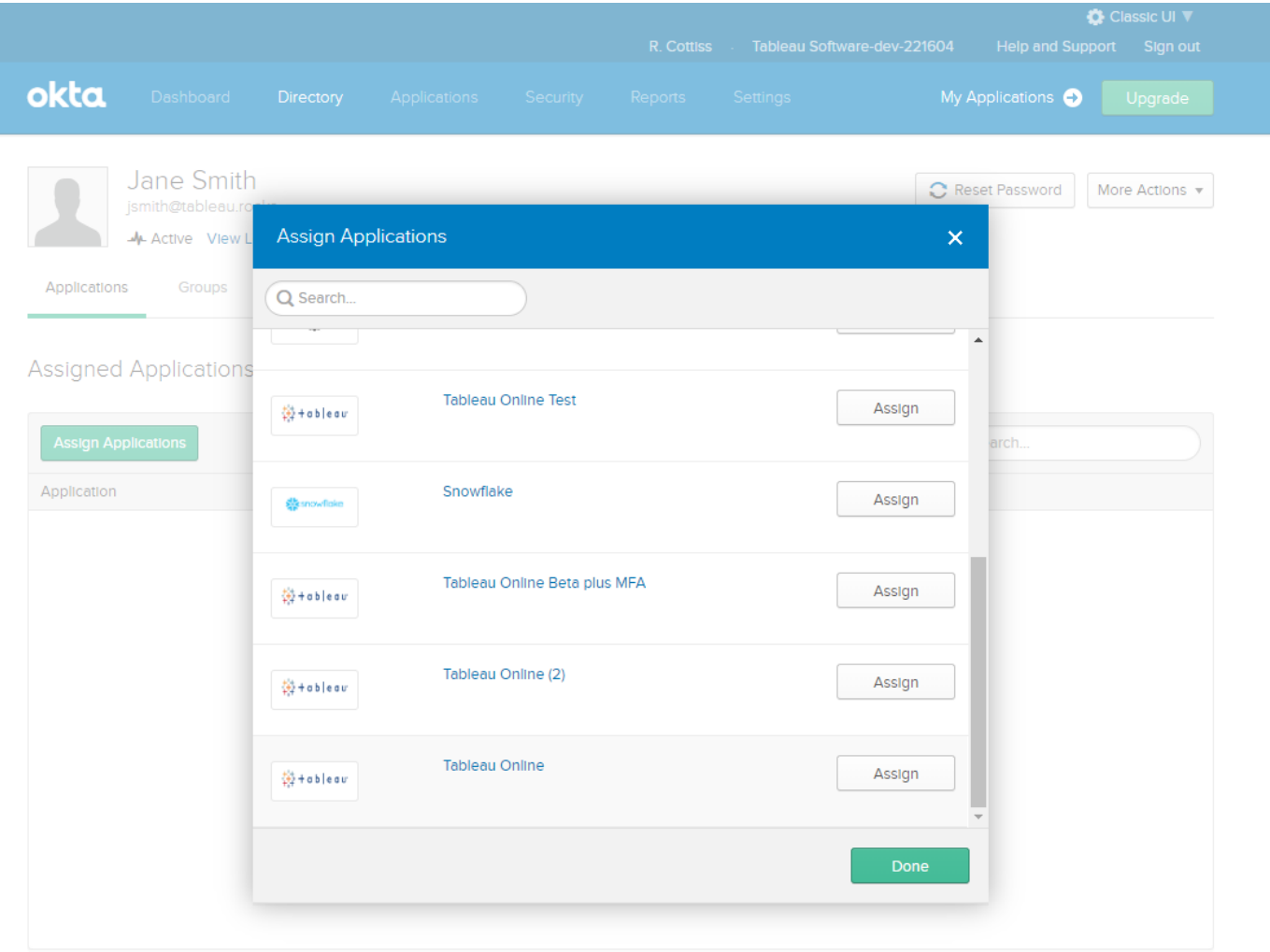
Assigned Applications

Assign Applications

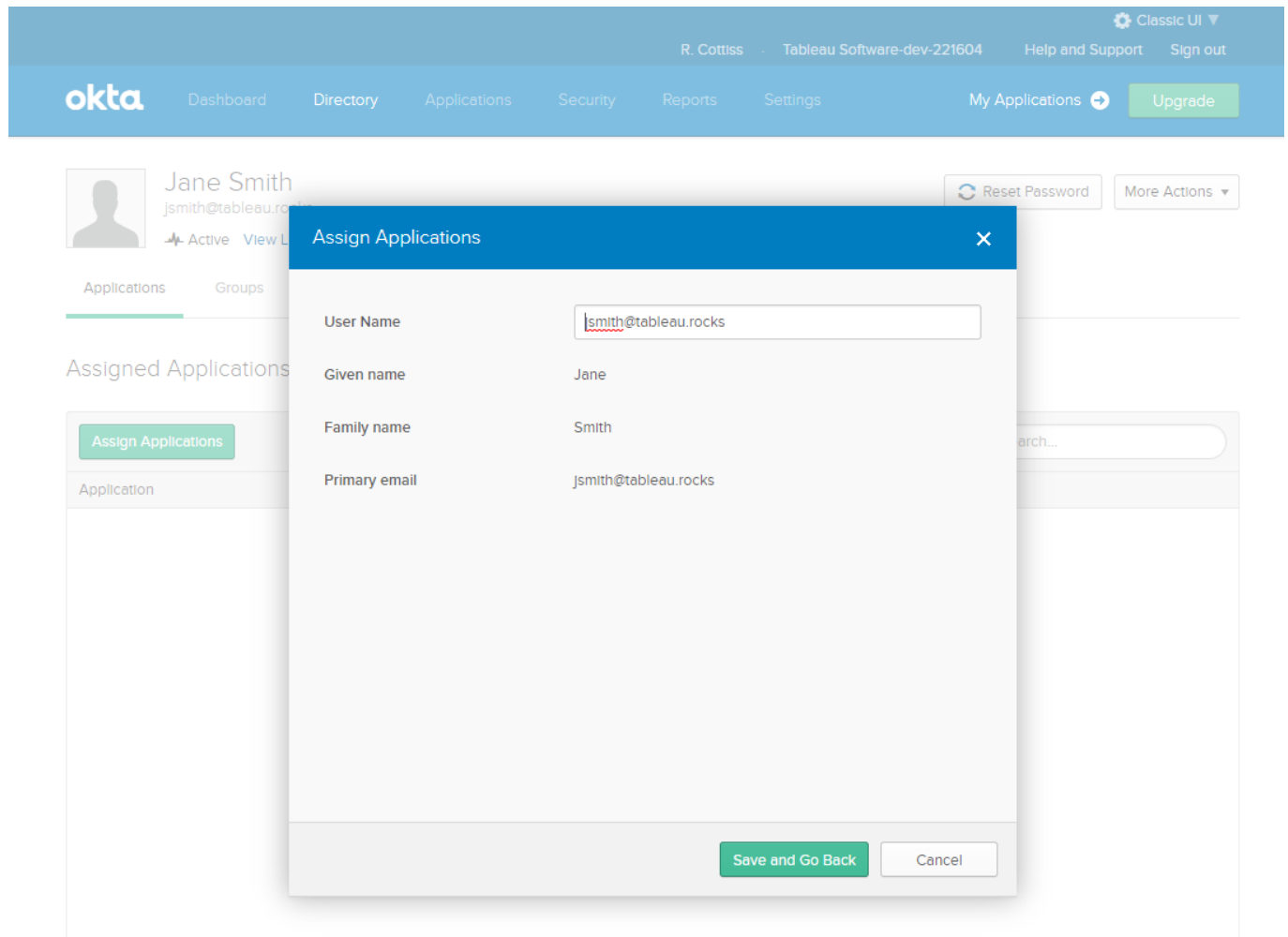
Search...

Application	Assignment & App Username
<div><div>01101110</div><div>01101111</div><div>01101100</div><div>01101100</div><div>01101101</div><div>01101110</div><div>01100111</div><div></div></div> <div>No apps assigned to this user.</div>	

and then selecting one or more applications:



Leave the username as the email and click **Save and Go Back**



Alternatively you can select **Applications** then the Tableau Online Application. Now you can assign the new user to Tableau Online. Click on **Assignments** in the Applications menu in Okta. Click on **Assign** then *Assign to People*

Okta Admin Console - Tableau Online configuration page. The 'Assignments' tab is active, showing a list of users assigned to the application. The list includes John Doe (jdoe@tableau.rocks) and Jane Smith (jsmith@tableau.rocks), both assigned as 'Individual' users. A 'SELF SERVICE' warning box on the right states: 'You need to enable self service for org managed apps before you can use self service for this app. Go to self service settings'. The 'Requests' status is 'Disabled'.

With SCIM enabled this is all you need to do. Okta will provision the new user in Tableau. You can confirm this by going back to Tableau Online and checking to see if the user got added:

Tableau Online 'Users' page. The page shows a list of site users. The table below contains the details of the users:

Display name	Username	Site role	Groups	Authentication	Last signed in
J jdoe@tableau.rocks	jdoe@tableau.rocks	Viewer	1	oktapreview.com (SAML)	
J jsmith@tableau.rocks	jsmith@tableau.rocks	Viewer	1	oktapreview.com (SAML)	
RC Robin Cottiss	rcottiss@tableausoftware.com	Site Administrator Creator	1	Tableau	Dec 5, 2018, 6:49 PM
RC Robin Cottiss	rcottiss@tableau.com	Site Administrator Creator	1	oktapreview.com (SAML)	Dec 26, 2018, 1:23 PM

[Note that the user was added as a Viewer - I am not sure if the default site role can be configured. Try testing with groups?]

Step 7 - Test SAML Login

Sign out of your Site Admin account in Tableau Online and also sign out of the Okta Developer Console. If you do not sign out of Okta then when you sign in to Tableau using the new account Okta might show an error

or send back the wrong assertion.

Now Sign into Tableau Online using the username of the user you assigned to the Tableau Online application in Okta. The browser should redirect you to Okta and present a login form.