
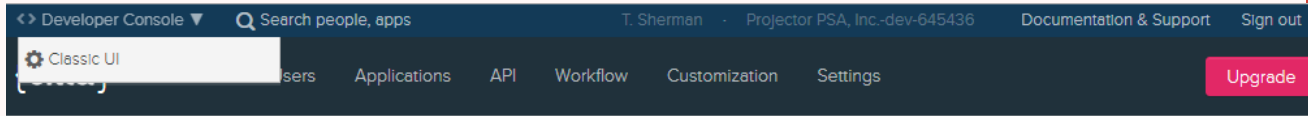


Single Sign On (SSO) for Okta

 Some basic help in getting Okta configured to work with Projector's Single Sign On implementation.

Classic UI

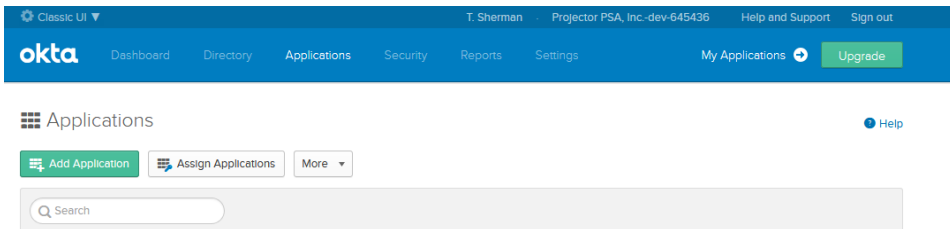
Make sure you switch from Okta's *Developer Console* to *Classic UI* in order to follow these instructions. The dropdown is in the upper left of the navigation bar.



Use Pre-Built Okta Connector

Projector has pre-built application in Okta. You can quickly and easily configure Okta using this. If you want to manually configure Okta, see the next section, Manually Configure Okta.

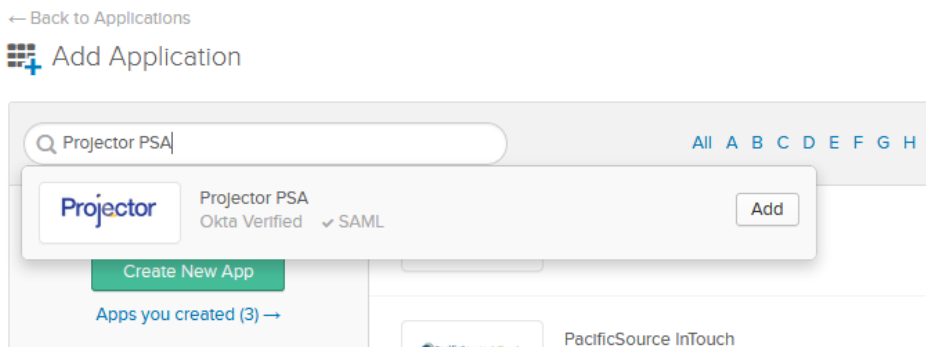
1. Log into Okta and go to the Administration area
2. Click **Applications**



3. Click **Add Application**



4. Search for "Projector" and click **Add**



5. Click **Next**

General Settings - Required

Application label	<input type="text" value="Projector PSA"/>
	<small>This label displays under the app on your home page</small>
Application Visibility	<input type="checkbox"/> Do not display application icon to users
	<input type="checkbox"/> Do not display application icon in the Okta Mobile App
Browser plugin auto-submit	<input checked="" type="checkbox"/> Automatically log in when user lands on login page

6. Choose the **SAML 2.0** radio button

Sign-On Options - Required

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](#)

Secure Web Authentication

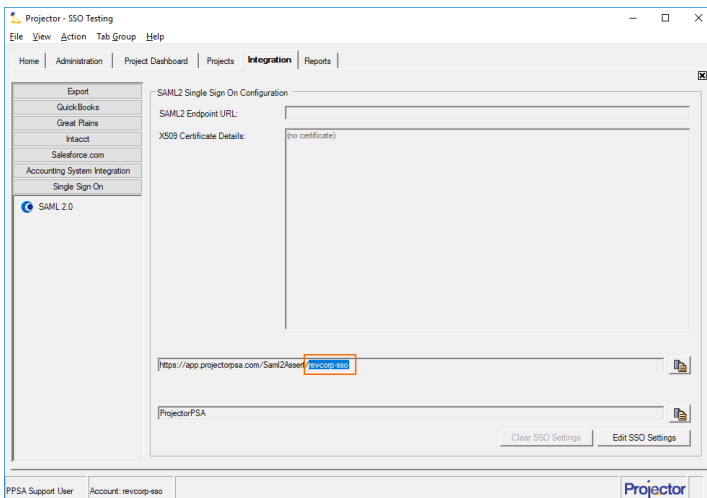
SAML 2.0

7. Click **View Setup Instructions**. This opens a new web page.

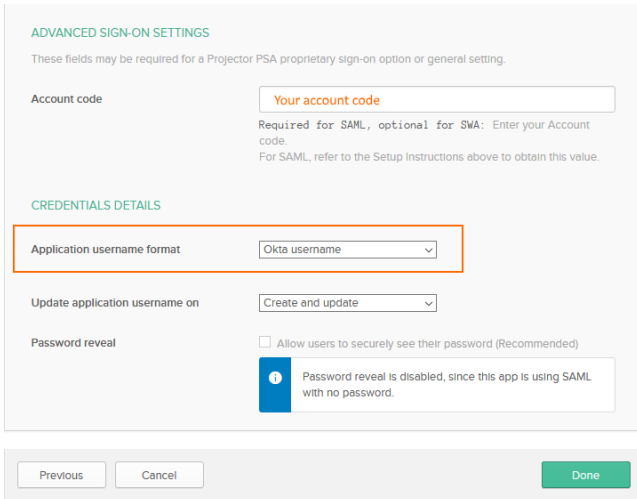
 SAML 2.0 is not configured until you complete the setup instructions.

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

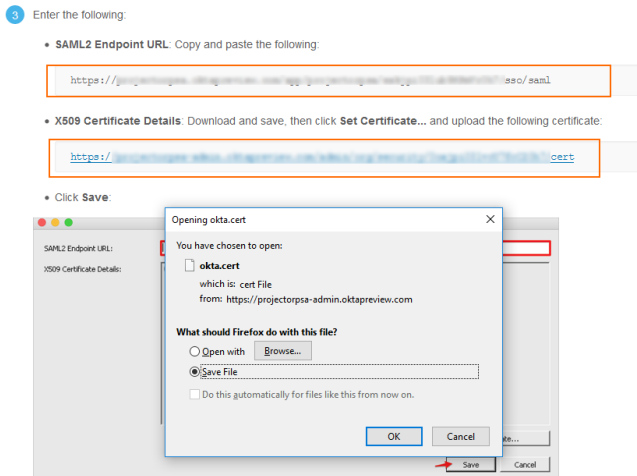
8. Open Management Portal. Go to **Integration tab | SSO Settings subsection | SAML 2.0** blue dot. Copy the account code from the end of the URL.



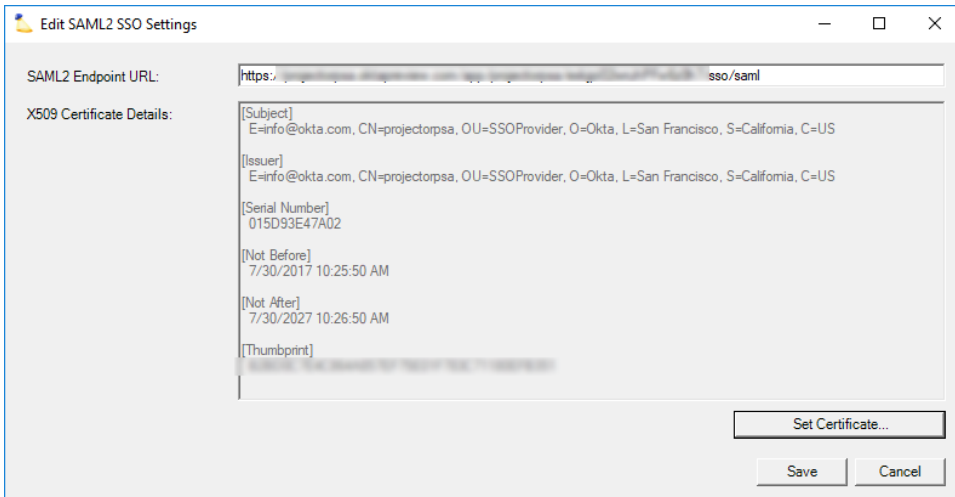
9. Paste it into the **Account Code** field in Okta



10. From step 3 on the setup instructions, copy the **SAML2 Endpoint URL** and download the **okta.cert** file



11. In Management Portal click **Edit SSO Settings**. Paste the URL into **SAML2 Endpoint URL**. Click **Set Certificate** and upload your **okta.cert** file. Click **Save**.



12. Set your **Application username format**. By default Projector expects Okta to send us an email address. The email should be the same as the user's Projector email address. If you don't want to use email addresses, you can edit users in Projector and specify the value we will receive from Okta.

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.

First Name: Tom
Middle Name:
Last Name: Sherman
Display Name: Tom Sherman
Email Address: jw@projectokta.com
Username: jw@okta.com
Employee ID: 054015
Client: GRT-05-03 System Test US & Canada

User Types: User Type Overrides | Contact Information
General | Global Permissions | Cost Center Permissions | Notifications

Override

- Allow access to Management Portal
- Use default tab group: Projector Administrator
- Link access to projects in time entry, expense entry, and project workspaces
- Include in Project Manager list
- Use delegated authentication
- Single sign on: Required
- Resource can: Update their skills, with approval
- Resource can: Request future time off, with approval needed
- Resource can: Get view advanced analytics content
- Allow resource to request their own time
- Allow resource to book their own time

Save Cancel

Edit Pre-built Connector

If you find that you need to edit or review your pre-built connector settings, edit your application and go to the **Sign On** section.

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](#)

Secure Web Authentication

SAML 2.0

Default Relay State

Disable Force Authentication

Manually Configure Okta

Basic steps:

1. Log into Okta as administrator.
2. Switch to **Classic UI** from Developer Console.
3. Click **Applications menu**
4. Click **Add Application**
5. Click **Create New App**
6. Configure the application to assert your email address to Projector
 - a. If your Okta username is not your email address, you'll need to create a mapping that sends your email instead of your username to Projector. This can be done from **Directory | Profile Editor**. See screenshot below.

The screenshot shows the 'Projector PSA (Production) User Profile Mappings' interface. It features two tabs: 'Projector PSA (Production) to Okta' and 'Okta to Projector PSA (Production)'. The 'Okta to Projector PSA (Production)' tab is active. On the left, the 'Okta User Profile' is shown with the attribute 'user_email'. A dropdown menu is open, showing 'user_email' as the selected option. A green arrow icon points to the right. On the right, the 'Projector PSA (Production) User Profile' is shown with the attribute 'userName' of type 'string'.

7. Enter ACS URL and Upload x.509 Cert to Projector
 - a. Go to **Applications | SignOn | View Setup Instructions**. A new web page will pop up. Get your ACS URL and x.509 certificate.
 - b. In Management Portal, go to **Integration tab | Single Sign On subsection | SAML 2.0 blue dot**
 - c. Click **Edit SSO Settings**
 - d. Enter your ACS URL in the **SAML2 Endpoint URL** field
 - e. Click **Set Certificate** and upload your x.509 certificate

Projector PSA, Inc. Active View Logs

← Back to Applications

General Sign On Import People Groups

Settings

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.

SAML 2.0

Default Relay State

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.

CREDENTIALS DETAILS

Application username format: Email

Password reveal: Allow users to securely see their password (Recommended)

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.

Edit SAML2 SSO Settings

SAML2 Endpoint URL: `https://projectorpsa.oktapreview.com/app/projectorpsaincdev645436_projectorpsaproduction_1/exkbqa0`

X509 Certificate Details:

```
[Subject]
E=info@okta.com, CN=projectorpsa, OU=SSOProvider, O=Okta, L=San Francisco, S=California, C=US

[Issuer]
E=info@okta.com, CN=projectorpsa, OU=SSOProvider, O=Okta, L=San Francisco, S=California, C=US

[Serial Number]
015D93E47A02

[Not Before]
7/30/2017 10:25:50 AM

[Not After]
7/30/2027 10:26:50 AM

[Thumbprint]
B2BD0C7E4C864A857EF75E01F783C71180EFB351
```

Set Certificate...

Save Cancel

Test Your SSO

See: [Single Sign On \(SSO\) Implementation Guide](#)

