Lab Guide:

Okta Fundamentals - Intro Labs

Table of Contents

Prerequisites

The following items are needed for the completion of this lab:

- Okta Developer Account.
- Salesforce Developer Account
- SAML Tracer

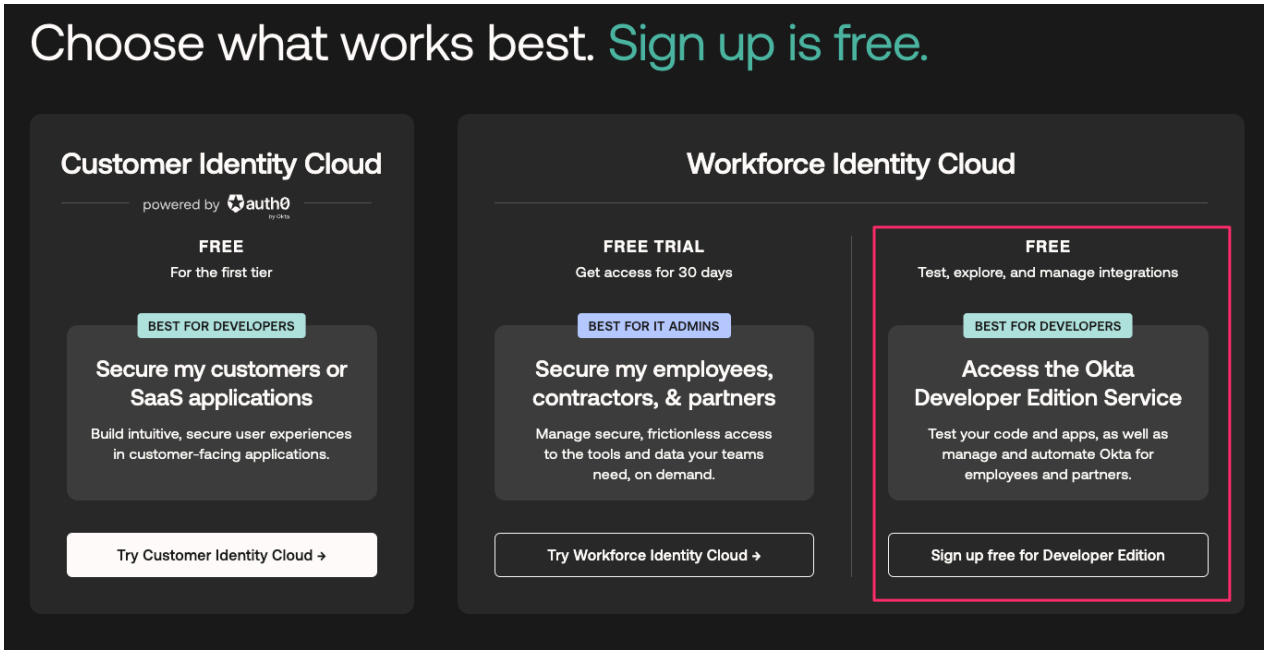
Lab 1-1: Create an Account and Access your Okta Tenant

Objective	To create an Okta developer account and sign in
Duration	5-10 minutes

Okta offers a free developer account. Follow the steps below to sign up and access your tenant.

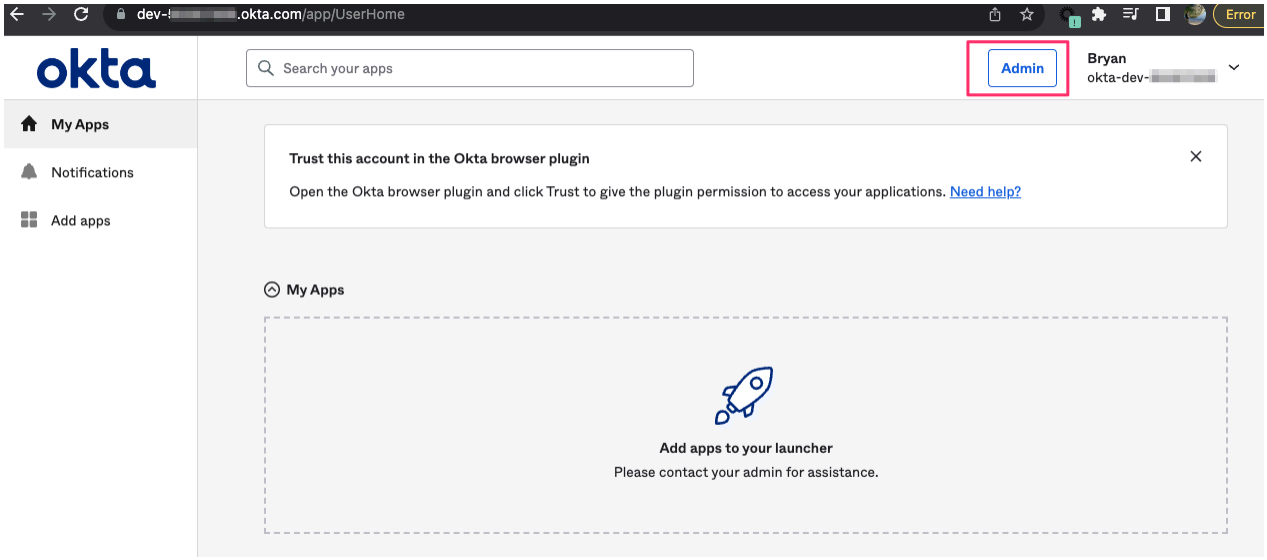
Create an Okta developer account

1. Navigate to https://developer.okta.com/signup/.
2. Under the 'Workforce Identity Cloud' section, click the **Sign Up free for Developer Edition** button.



3. Fill in your information and click **Sign Up**.
4. You will receive an email to activate your account. Enter a new password.
5. You will be logged into your Okta dashboard. **Note** that this first user is your Super Admin user.
6. Your Okta tenant should be something like: https://dev-xxxxxxxx.okta.com. This is your end-user dashboard. The admin dashboard is https://dev-xxxxxxxx-**admin**.okta.com

   When you are logged in the first time, you'll be directed to the end-user dashboard. Clicking on **Admin** will bring you into the admin dashboard.

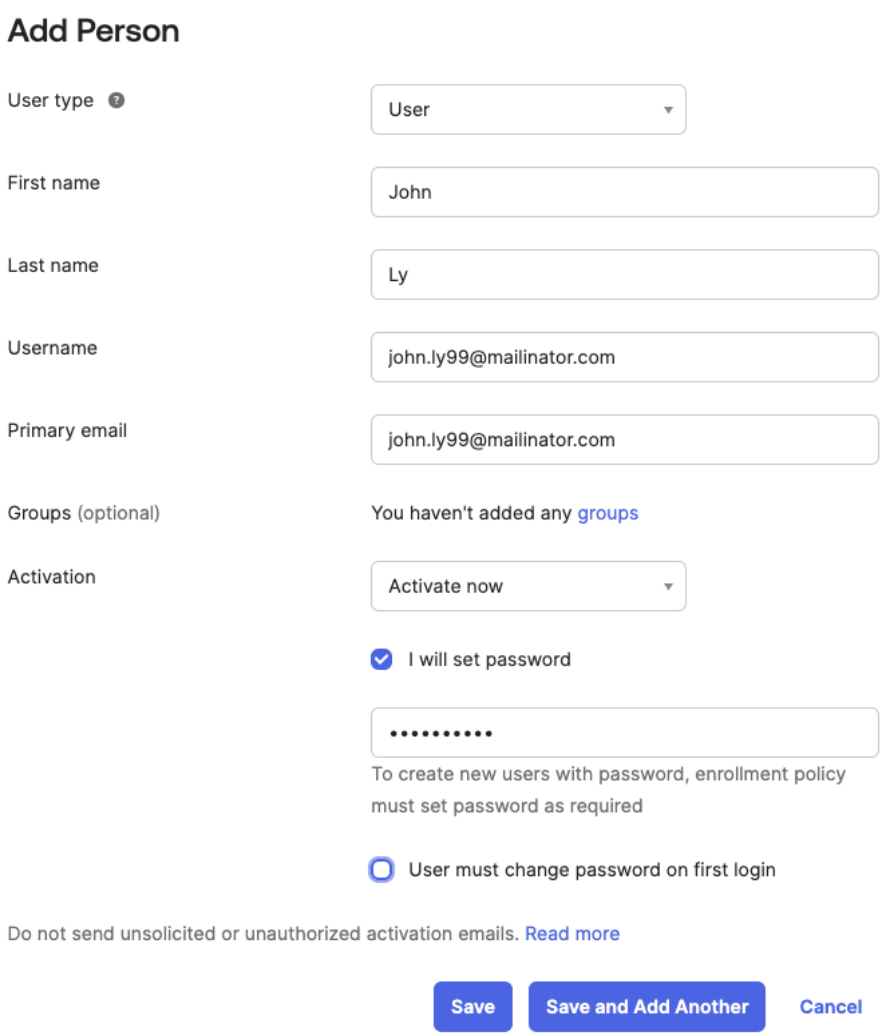


Lab 1-2: Create Okta Sourced Users

Objective	To create and import users into Okta
Procedures	• Create 3 accounts via the admin UI • Import a list of users from a CSV file • Assign administrative roles
Duration	20-30 minutes

1.1 Create and activate two accounts in the Okta Admin portal

1. From your Okta dashboard, click **Admin** to switch to the Okta Administrator dashboard if not already in the admin portal.
2. Navigate to **Directory** > **People**.
3. Click on **Add Person** to create a user account. Fill in the information similar to below:



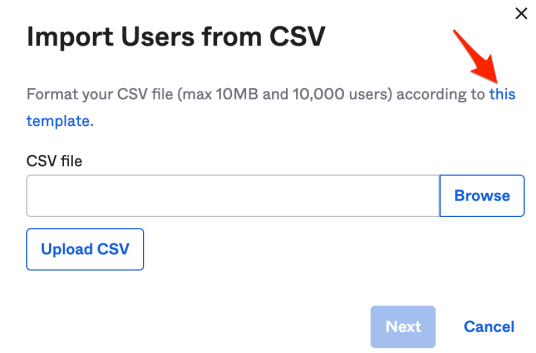
If you'd like to use a free email service, check out https://www.mailinator.com. You can use this to create your test users.

4. Click **Save**. Your user is now created and activated.
5. Repeat Step 3 to create and activate 2 more users.

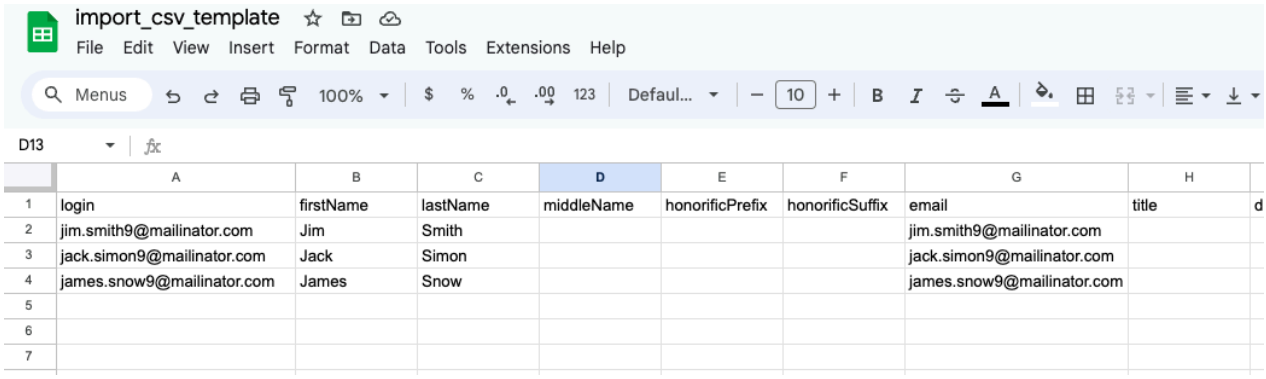
1.2 Import a list of users from a CSV file

Another way to create users is through a CSV import

1. Navigate to **Directory** > **People** > **More Actions** > **Import Users from CSV**
2. Click on the link 'this template' from the interface. This will download a *'import_csv_template.csv'* file.

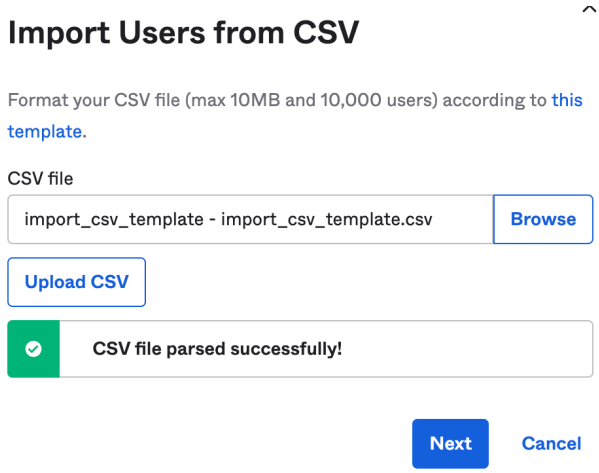


3. Open the file and add a few users. Fill in **login**, **firstName**, **lastName** and **email** at the minimum. Be sure NOT to change the names/variables in row 1 as it contains Okta user attributes. Save the file.

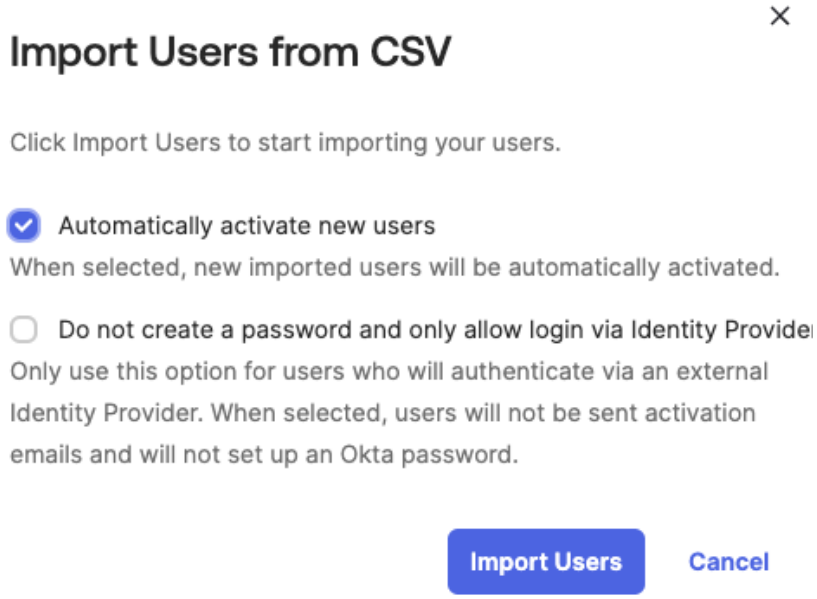


	A	B	C	D	E	F	G	H
1	login	firstName	lastName	middleName	honorificPrefix	honorificSuffix	email	title
2	jim.smith9@mailinator.com	Jim	Smith				jim.smith9@mailinator.com	
3	jack.simon9@mailinator.com	Jack	Simon				jack.simon9@mailinator.com	
4	james.snow9@mailinator.com	James	Snow				james.snow9@mailinator.com	
5								
6								
7								

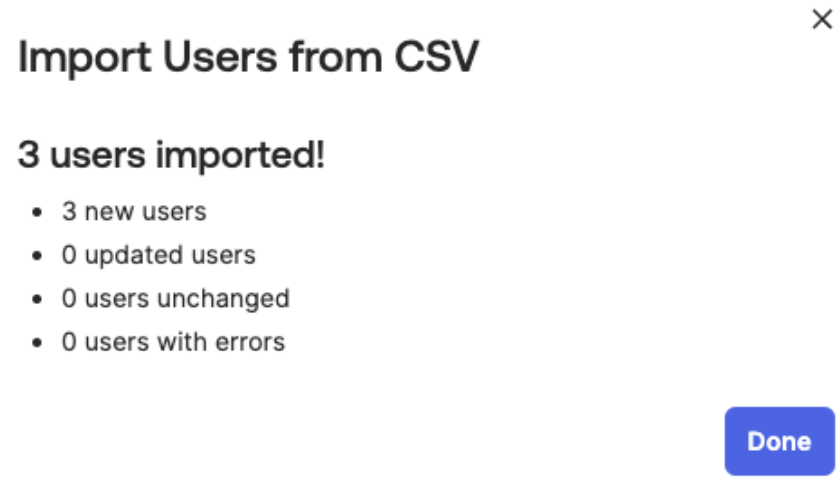
4. Click **Browse** and select the saved file.
5. Click **Upload CSV**.



6. Click **Next.**
7. Click **Import Users** and go ahead and check *'Automatically activate new users'*.



8. The users should now be imported. Click **Done**.



NOTE: If you receive any errors during the import, it means that some variables have been changed in Row 1 and caused it to have an incorrect format.

The users are imported and their status is 'pending user action'. At this point, an email has been sent to the user's email address and they can activate the account. As an Okta administrator, you can alternatively set a password and activate the account.

okta

okta-dev-55357309 - Welcome to Okta!

Hi James,

Your organization is using Okta to manage your web applications. This means you can conveniently access all the applications you normally use, through a single, secure home page. Watch this short video to learn more: https://www.okta.com/intro-to-okta/

Your system administrator has created an Okta user account for you.
Click the following link to activate your Okta account:

Activate Okta Account

This link expires in 7 days.

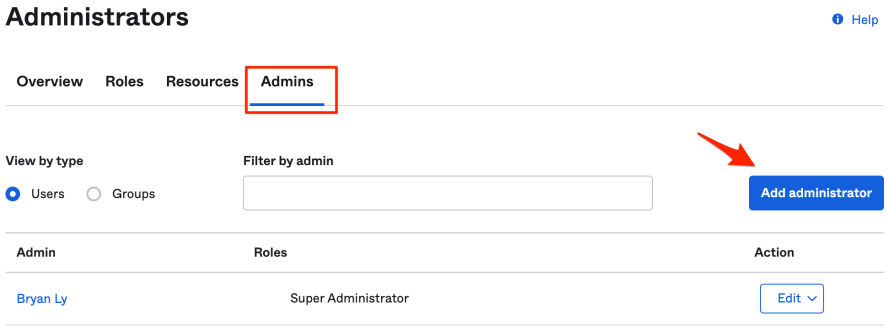
Your username is **james.snow9@mailinator.com**
Your organization's sign-in page is https://dev-55357309.okta.com

If you experience difficulties accessing your account, you can send a help request to your system administrator using the link: https://dev-55357309.okta.com/help/login

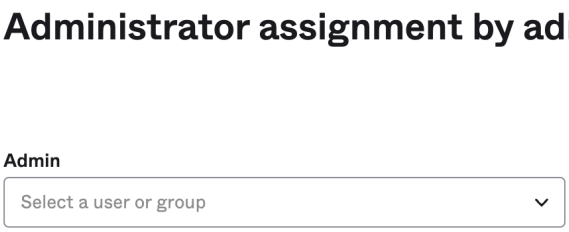
1.3 Assign Admin Roles

In this section, we'll be assigning administrator roles to users. Okta administrators (or admins) are responsible for maintaining all aspects of the end-user experience in their orgs. There are many types of admins, and each has a unique set of permissions and restrictions. What most Okta admins have in common is their access to the Admin Console, where they perform administrative tasks like user lifecycle management, application provisioning, and org customization.

1. In your Admin console, navigate to **Security** > **Administrators**.
2. Select the **Admins** tab, click **Add administrator**.

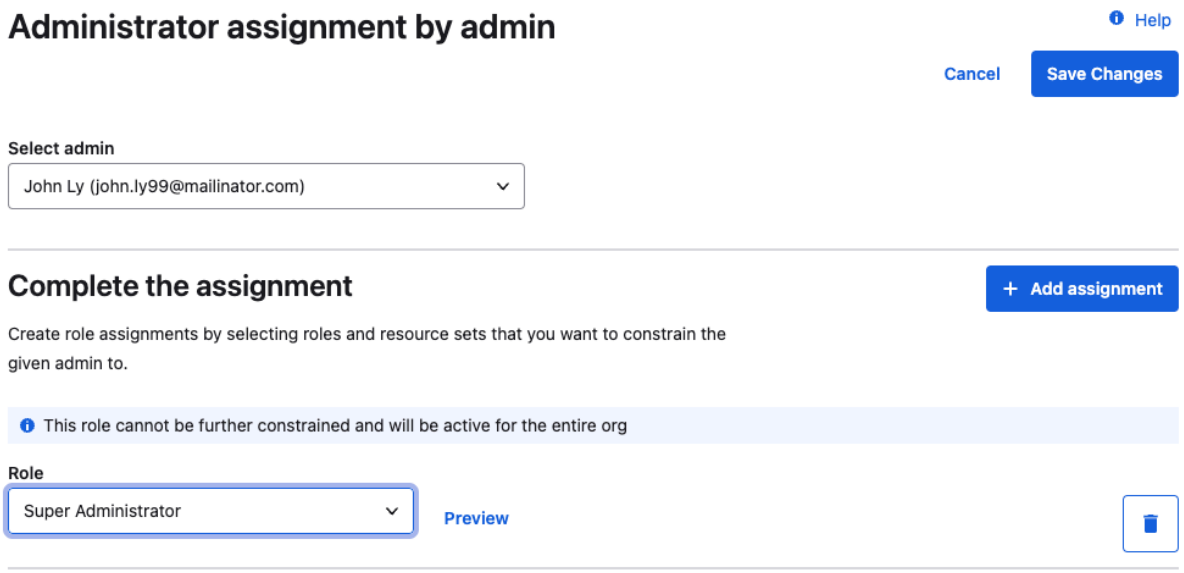


3. Search for an active user that you imported from the previous steps.



4. Select the user.

5. Select the drop-down under Role and choose ‘Super Administrator’.



6. Click **Save Changes**. You now have 2 Super Admins in your org.

   NOTE: Recommended best practice is to have at least two super admins in your org. This is for situations where your first user may be locked out and a second administrator is needed.

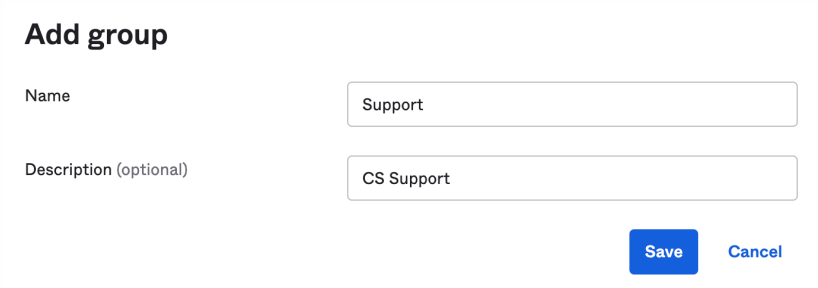
Lab 1-3: Create and Manage Groups in Okta

Objective	To understand how to create and manage groups in Okta
Procedures	• Create Groups via the admin UI. • Assign Users to groups. • Configure group membership rules.
Duration	20-30 minutes

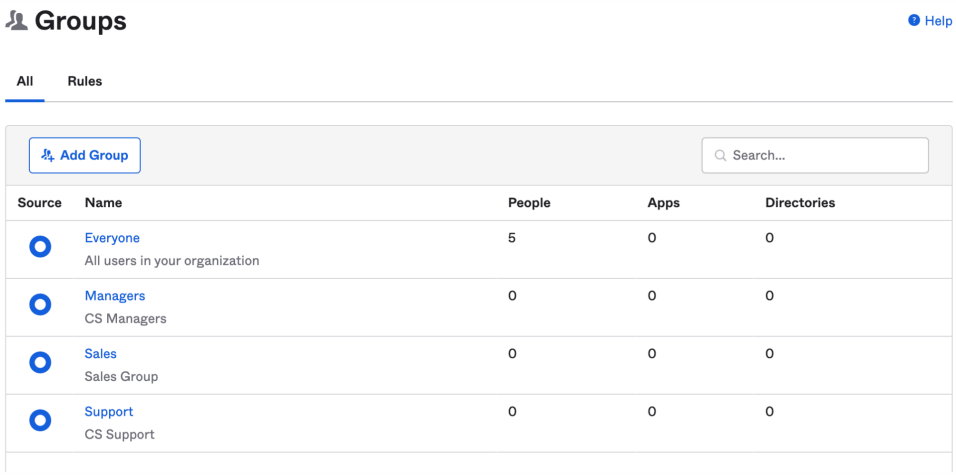
1.1 Create Groups via the admin UI

1. Navigate to **Directory** > **Groups**.

2. Click **Add Group**. Provide a name and optional description.



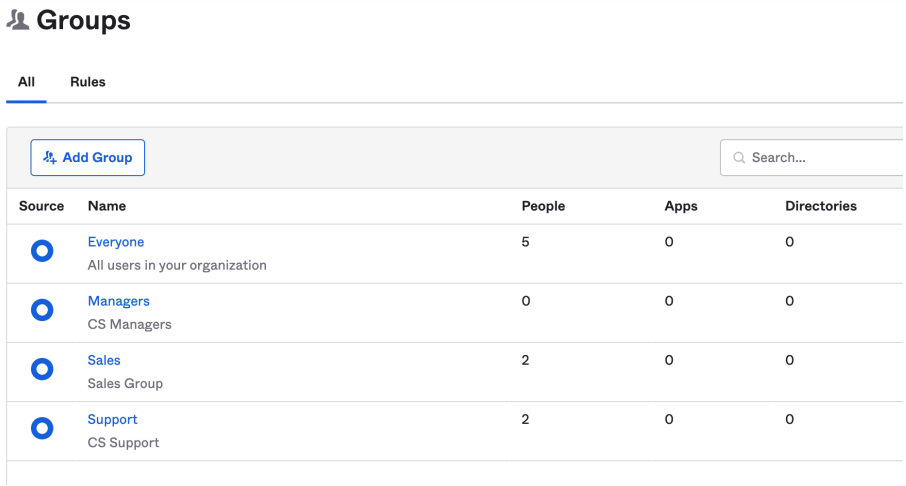
3. Repeat the process and create two more groups: **Sales**, **Managers**.



1.2 Assign Users to Groups

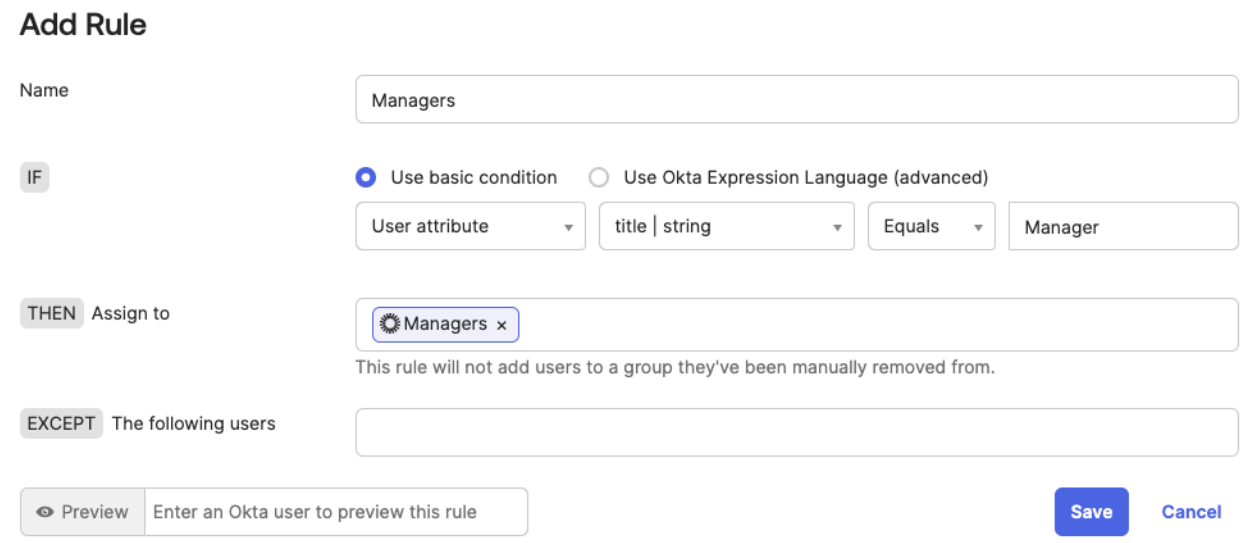
1. Navigate to **Directory** > **Groups.**
2. Select the group name you created earlier. In my case, the name is ‘Support’.
3. Click **Assign People** to assign users to the group.
4. Add two active users to the **Support** group by clicking on the + sign.
5. Add two active users to the **Sales** group by clicking on the + sign.

6. You should now have the following setup:

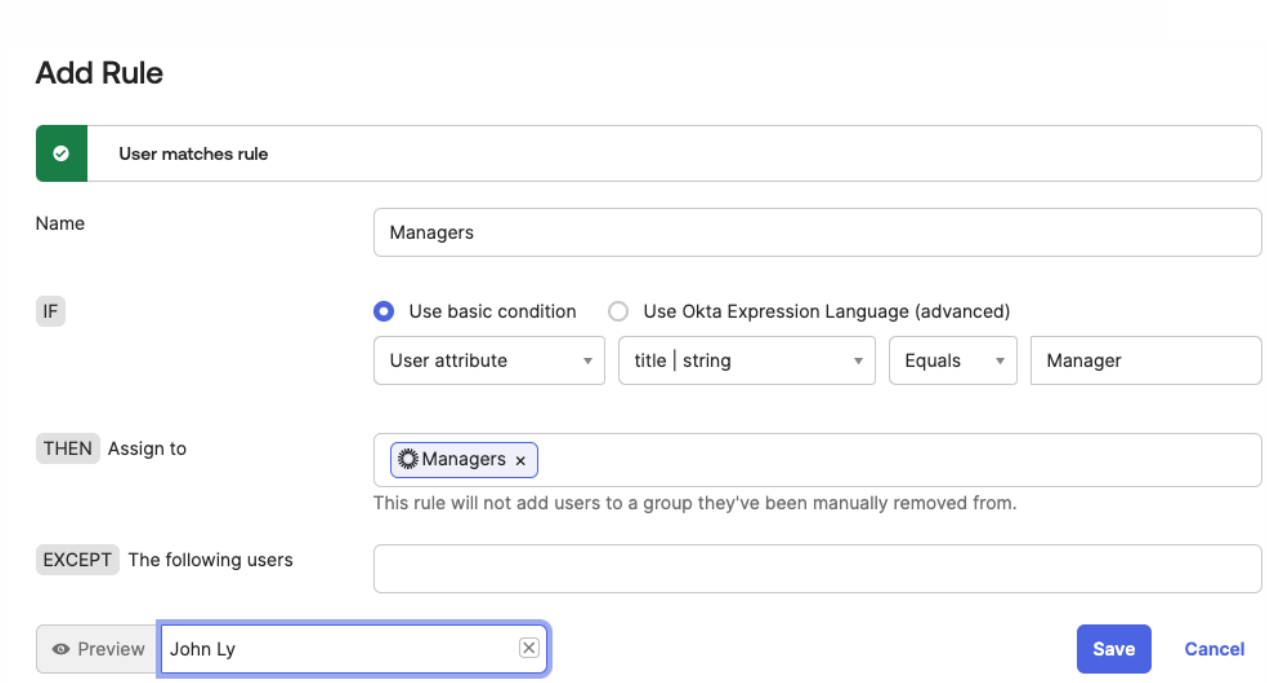


1.3 Configure Group Membership Rules

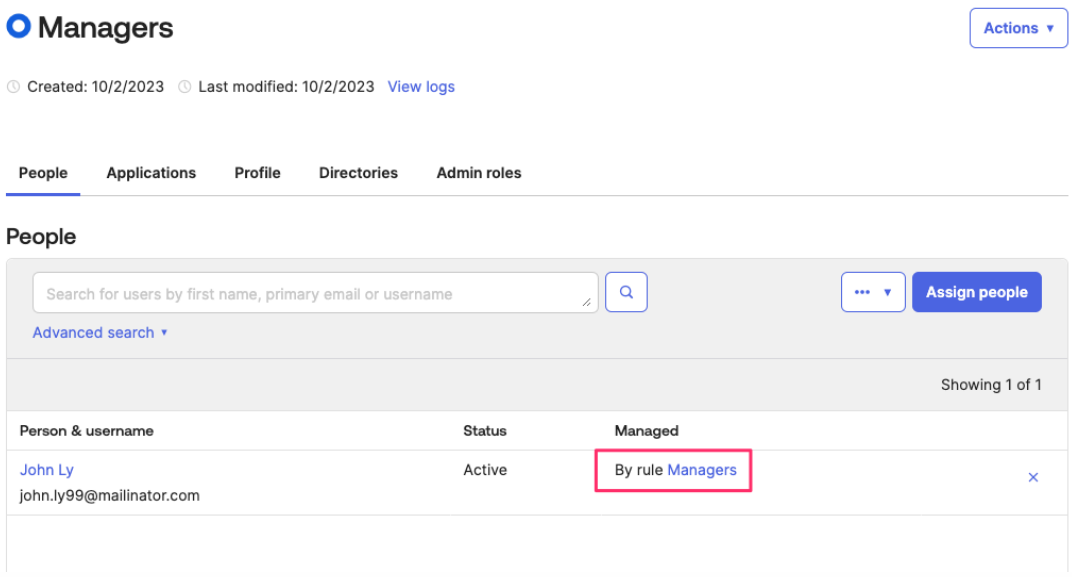
1. Navigate to **Directory** > **People** and select one of the Super Admins.
2. Navigate to the **Profile** tab and click **Edit**.
3. Add the 'Manager' value to the **Title** field. Scroll to the bottom and click **Save**.
4. Repeat the same process for the second Super Admin.
5. Navigate to **Directory** > **Groups** and click on the **Rules** tab.
6. Click **Add Rule**.
7. In the **Name** field, type in the following: **Managers**.
8. Select **User attribute** and choose **title** | **string** and equals to **Manager**.



9. Assign the rule to the **Managers** group. *You can preview the rule by entering an Okta user to see if the user matches the rule or not.*



10. Click **Save**.
11. By default, rules are created in the inactive status. Activate the rule by clicking **Actions** > **Activate.**
    NOTE: To edit a rule, you must first deactivate it by clicking **Actions** > **Deactivate** .
12. Notice how the group membership was assigned to users by rule in the 'Managers' group.

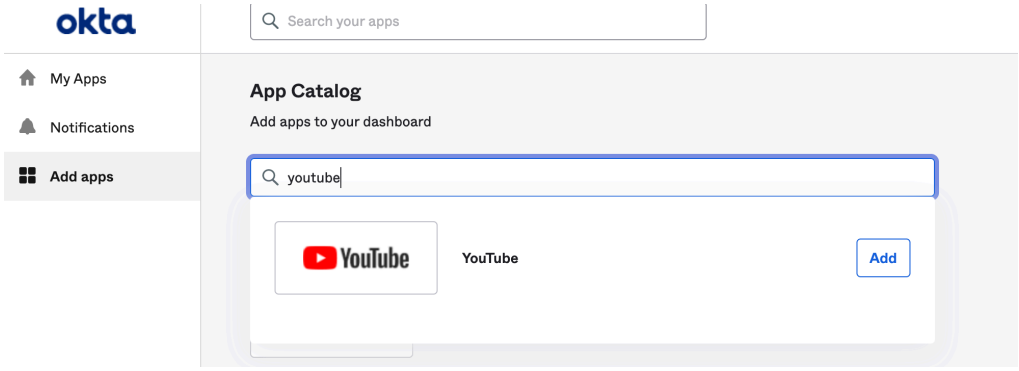


Lab 1-4: Add and Configure SWA Applications

Objective	To add and configure SWA applications in Okta
Procedures	• Create SWA apps • Assign Applications to users • Test Single Sign-On • Reveal Password
Duration	30-45 minutes

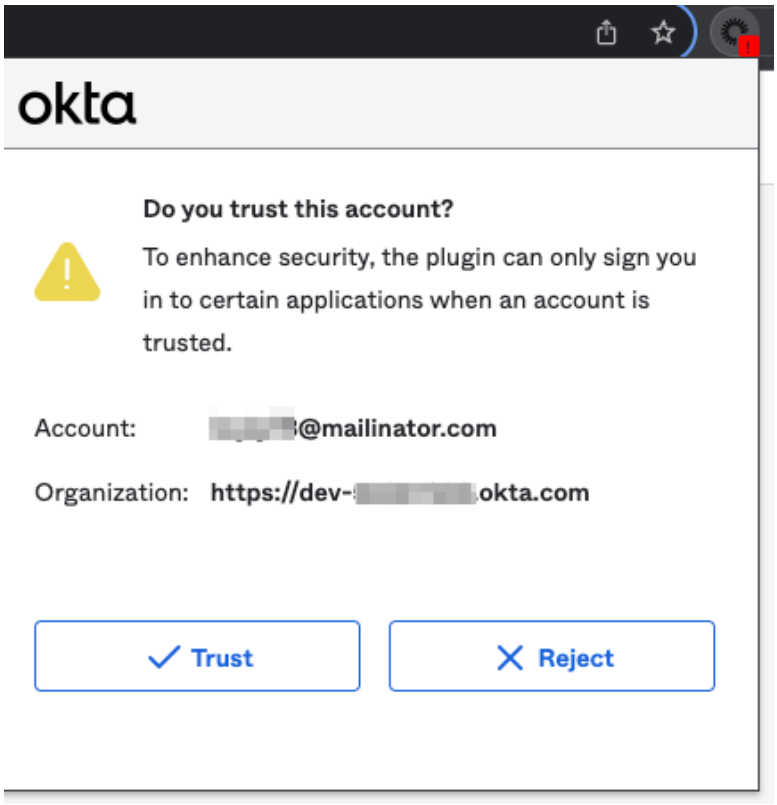
1.1 - Add and configure a SWA Application - Youtube (End-User flow)

1. Login into your Okta org.
2. From the end-user dashboard, click **Add Apps** on the left.
3. Search for Youtube in the **Search for an app** field and click **Add**.



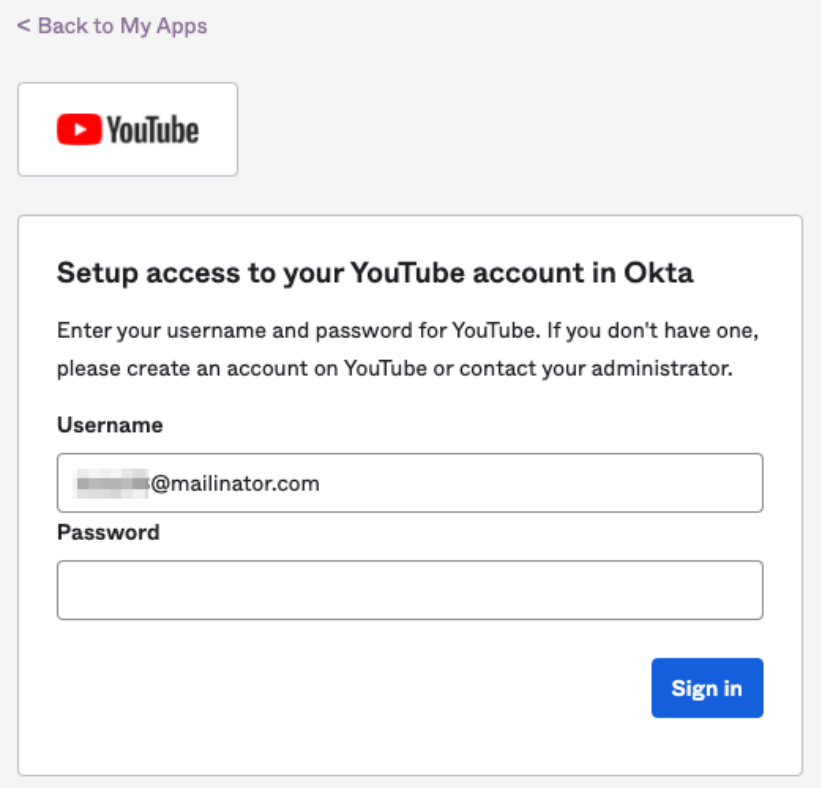
4. Click **My Apps** to go back to the main dashboard.

5. SWA applications require the Okta Browser Plugin. You must install the Okta Browser Plugin or give it permissions by selecting **Trust**.



6. Click **Youtube**.

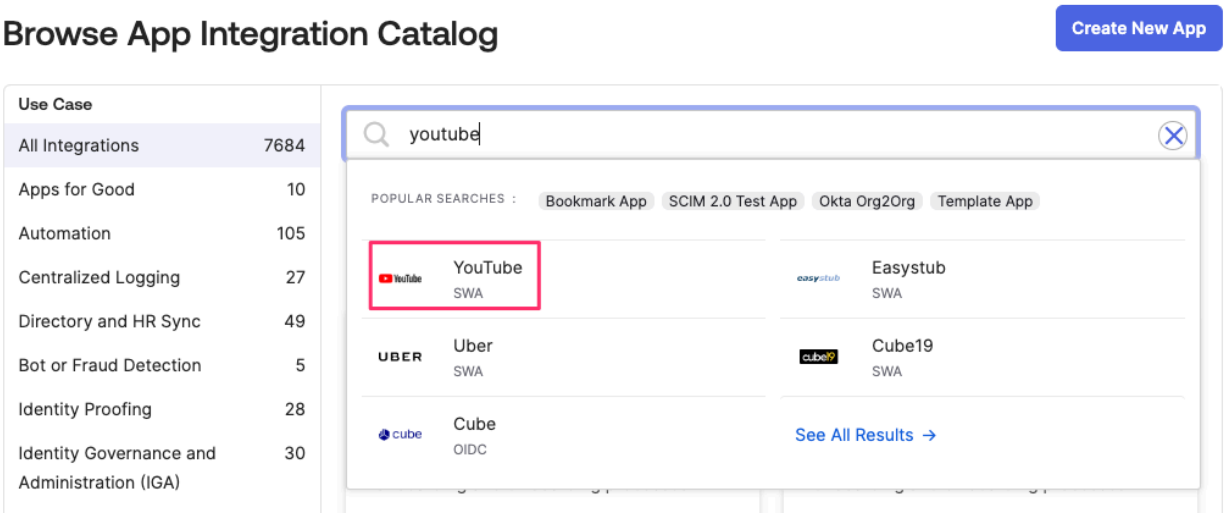
7. Add your existing Youtube account and click **Sign In**.



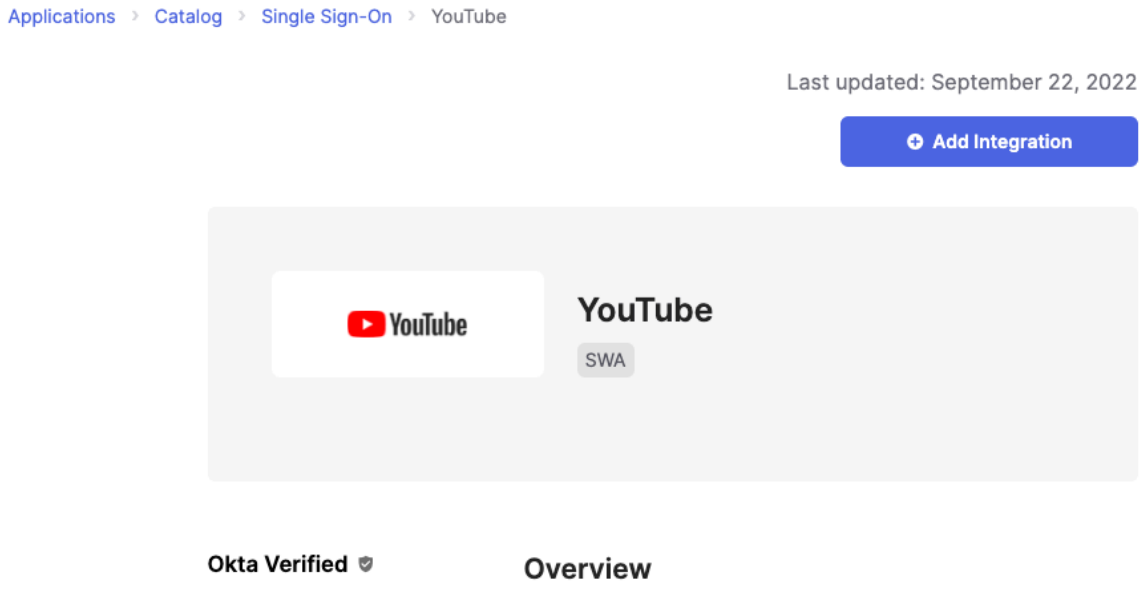
8. You should be logged in after entering in a valid credential.

1.2 - Add and configure a SWA Application - Youtube (administrator flow)

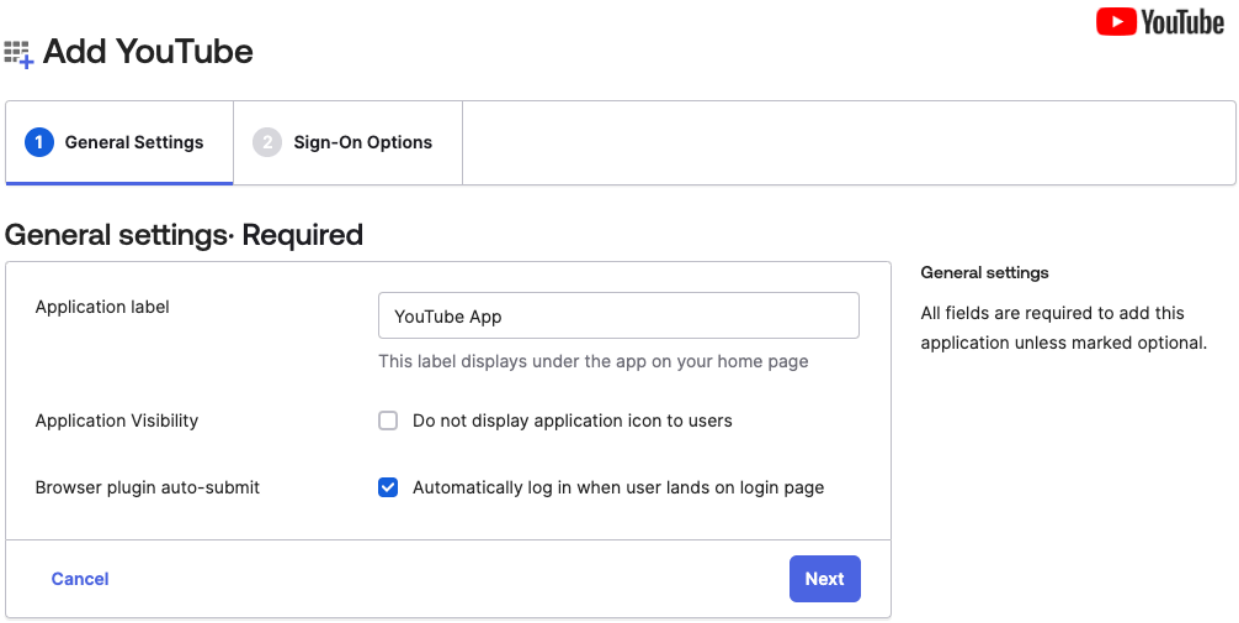
1. Log into your Okta org as an admin.
2. Go to **Applications**. Click on **Browse App Catalog**.
3. In the search area, type in 'Youtube'. You should see YouTube SWA.



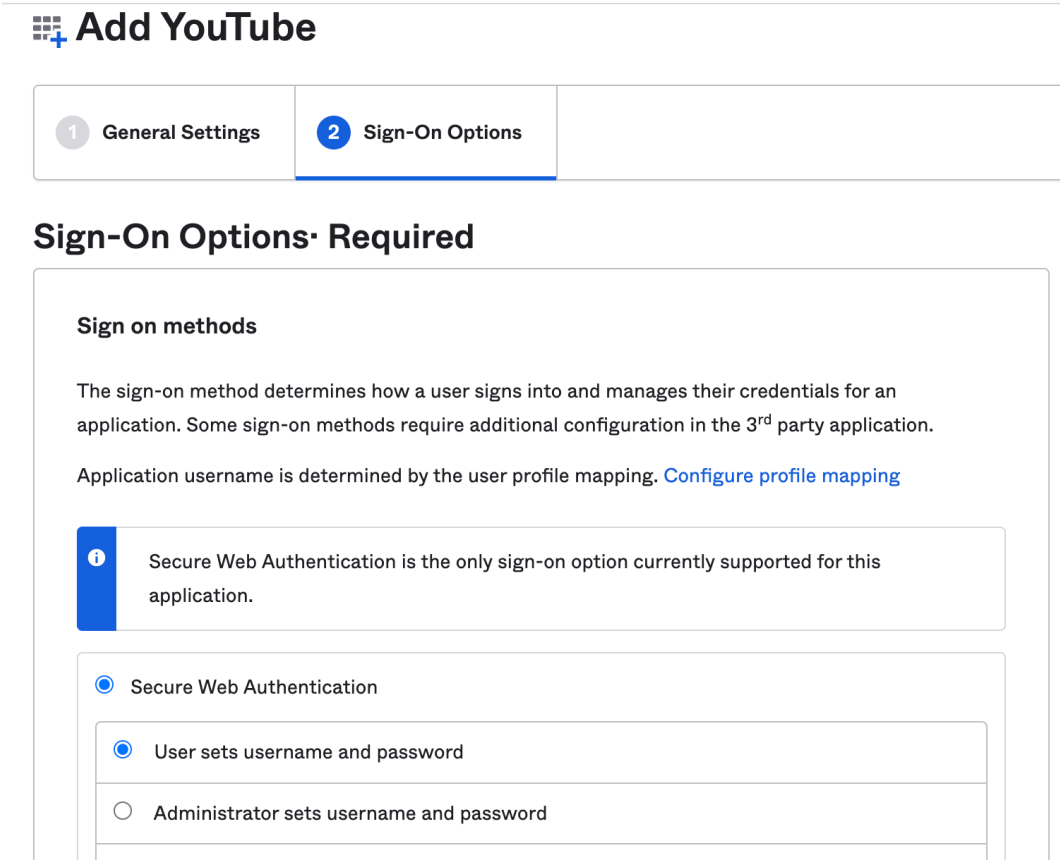
4. Click on the Youtube SWA app and click **Add Integration**.



5. Provide an application label and click **Next**.



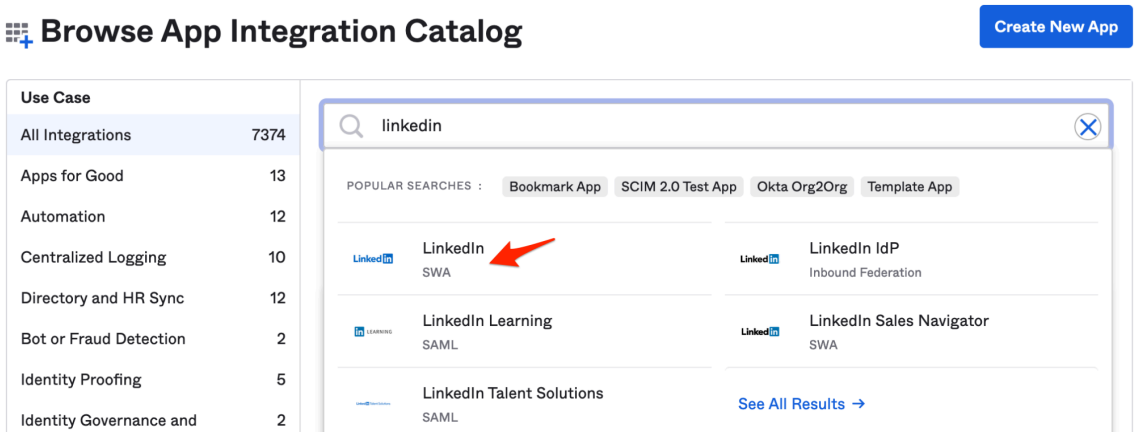
6. In the Sign-On option, leave the '**User sets username and password**' selected.



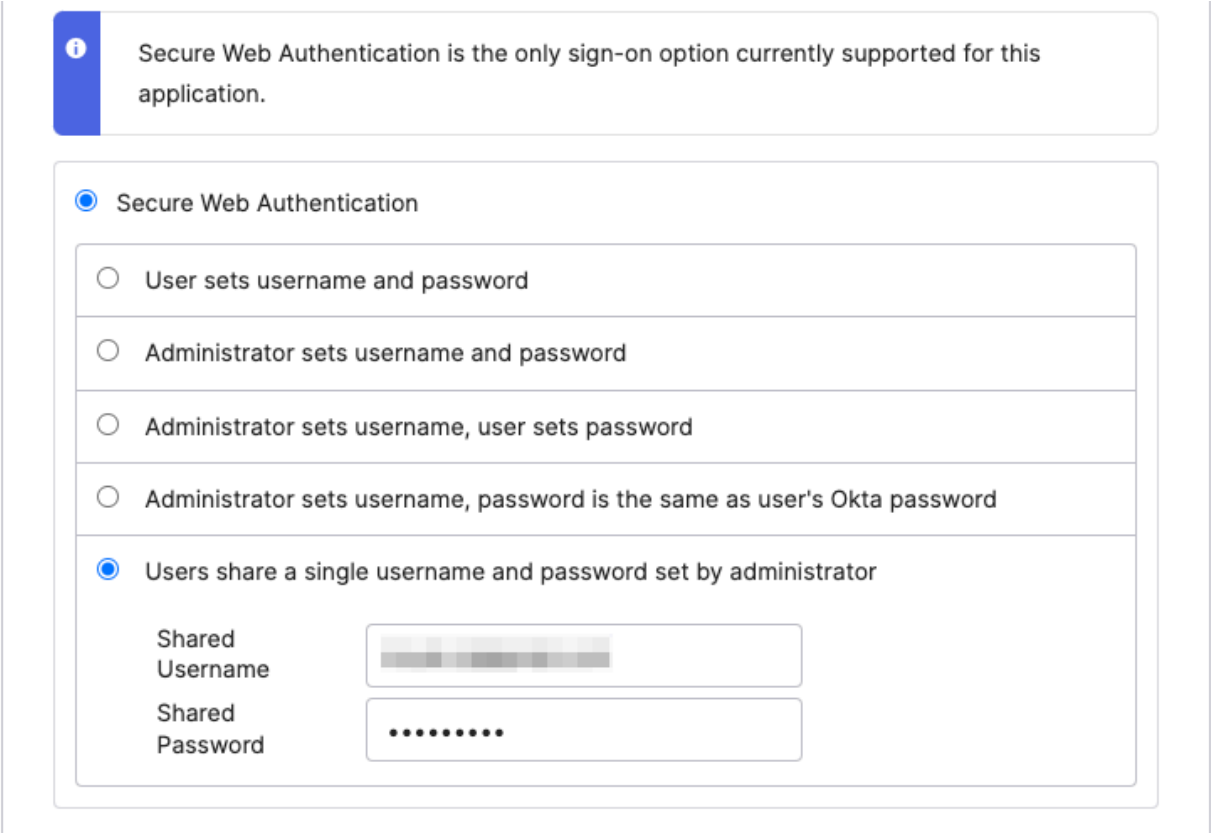
7. Click **Done**.
8. You will be directed to the 'Assignments' page. Click the blue **Assign** drop-down and select **Assign to People**.
9. Select one of the users and click **Assign**.
10. Click **Save and Go Back**. Click **Done**.
11. Youtube has now been successfully assigned to your user.
12. Log into the end user dashboard as the assigned user. The user should now see the Youtube app in their dashboard.
13. Click on the Youtube app and provide the username and password. You should be successfully logged in.

1.3 - Add and configure a SWA Application - Linkedin

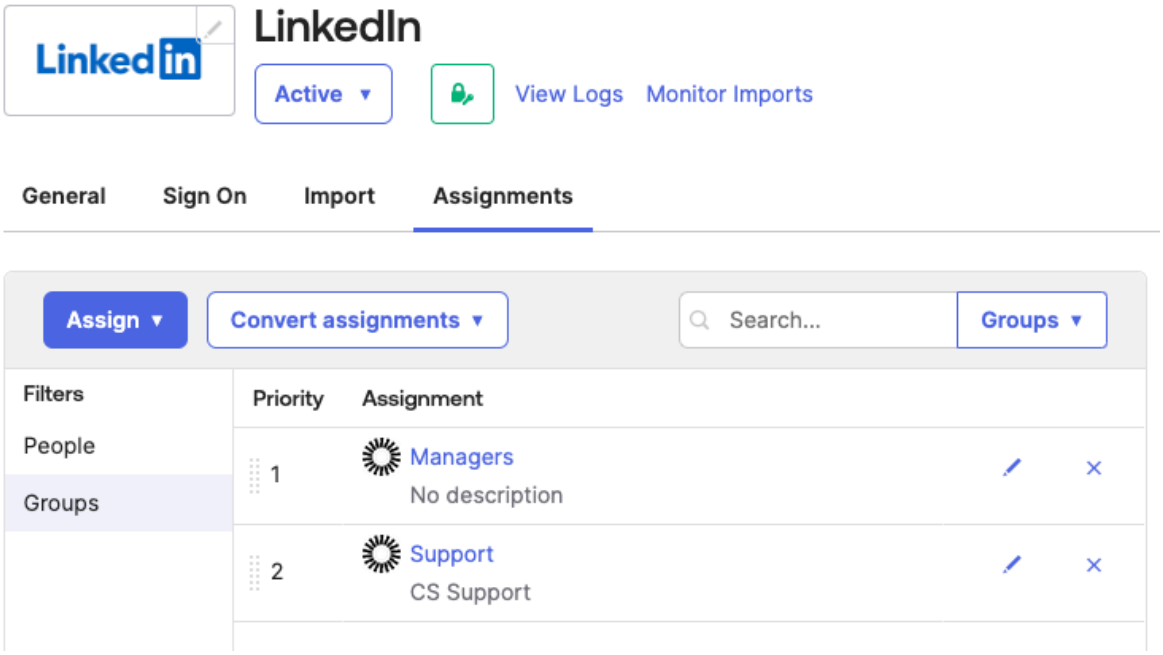
1. Log into your Okta org as an admin.
2. Go to **Applications**. Click on **Browse App Catalog**.
3. In the search area, type in 'Linkedin'. You should see Linkedin SWA.



4. Click on the Linkedin SWA app and click **Add Integration**.
5. Click **Next**.
6. In the Sign-On option, select the '**Users share a single username and password set by administrator**' selected. Click **Done**.



7. Click **Done**.
8. You will be directed to the 'Assignments' page. Click the blue **Assign** drop-down and select **Assign to Group**.
9. Assign the **Managers** and **Support** group. Click **Done**.
10. You should now have two groups assigned to the app.



11. Log into the end-user dashboard as one of the users from the groups.
12. You should see the 'LinkedIn' app. Click on it to login.

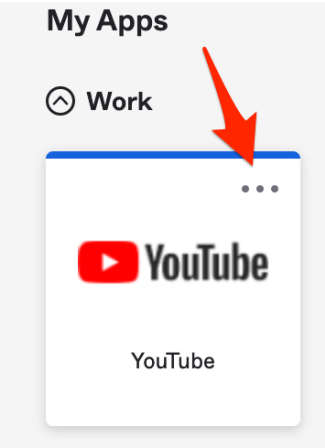
Lab 1-5: Delete Applications

Objective	To delete applications in Okta
Procedures	• Delete the end-user flow app • Delete the administrator flow app
Duration	5-10 minutes

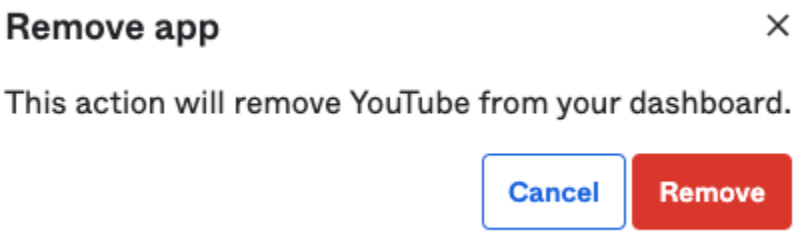
1.1 - Delete the Youtube application (end-user flow)

1. To remove an application as an end-user, log into your Okta dashboard.

2. Look for the youtube App and click on the 3 dots.



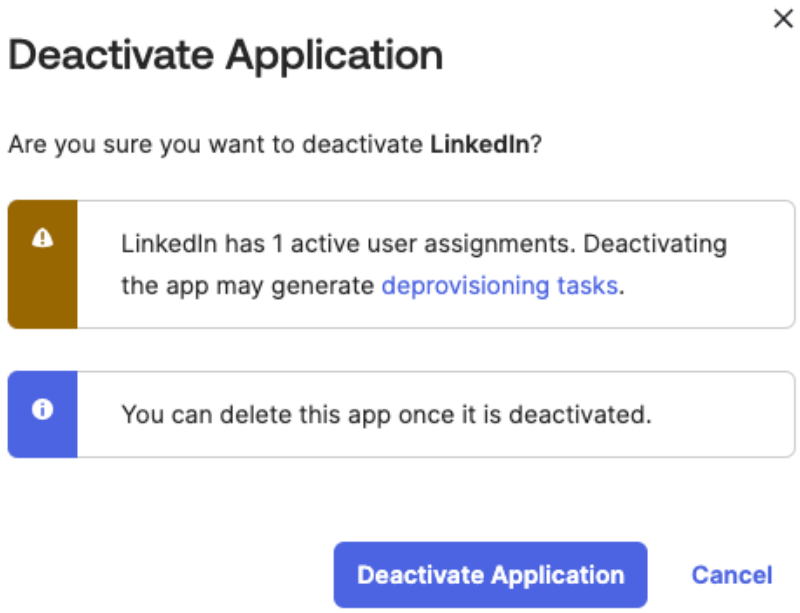
3. On the right side of the screen, click on **Remove**.
4. Click **Remove** to confirm removal of the app.



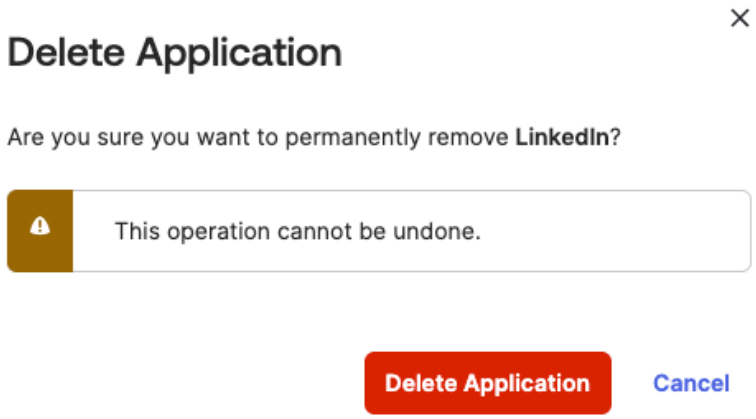
1.2 - Delete the Linkedin application (admin flow)

1. To remove an application as an admin, log into your Okta admin dashboard.
2. Navigate to **Applications** > **Applications**.
3. Search for the Linkedin application. Click the drown-down on the gear icon.

4. Select **Deactivate.** Click **Deactivate Application**



5. Select **Inactive** on the main applications page. Click the drown-down on the gear icon for Linkedin and choose **Delete**.
6. Click **Delete Application**.

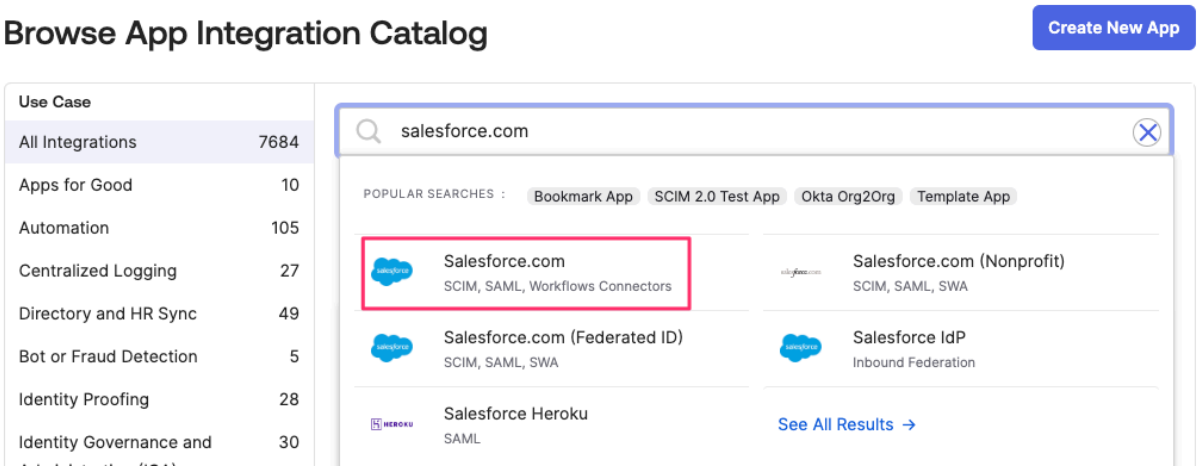


Lab 1-6: Configure SAML Applications in Okta

Objective	To configure SAML applications with provisioning
Procedures	• Configure SAML SSO for Salesforce • Configure SP-initiated SAML between Salesforce and Okta
Duration	30-45 minutes

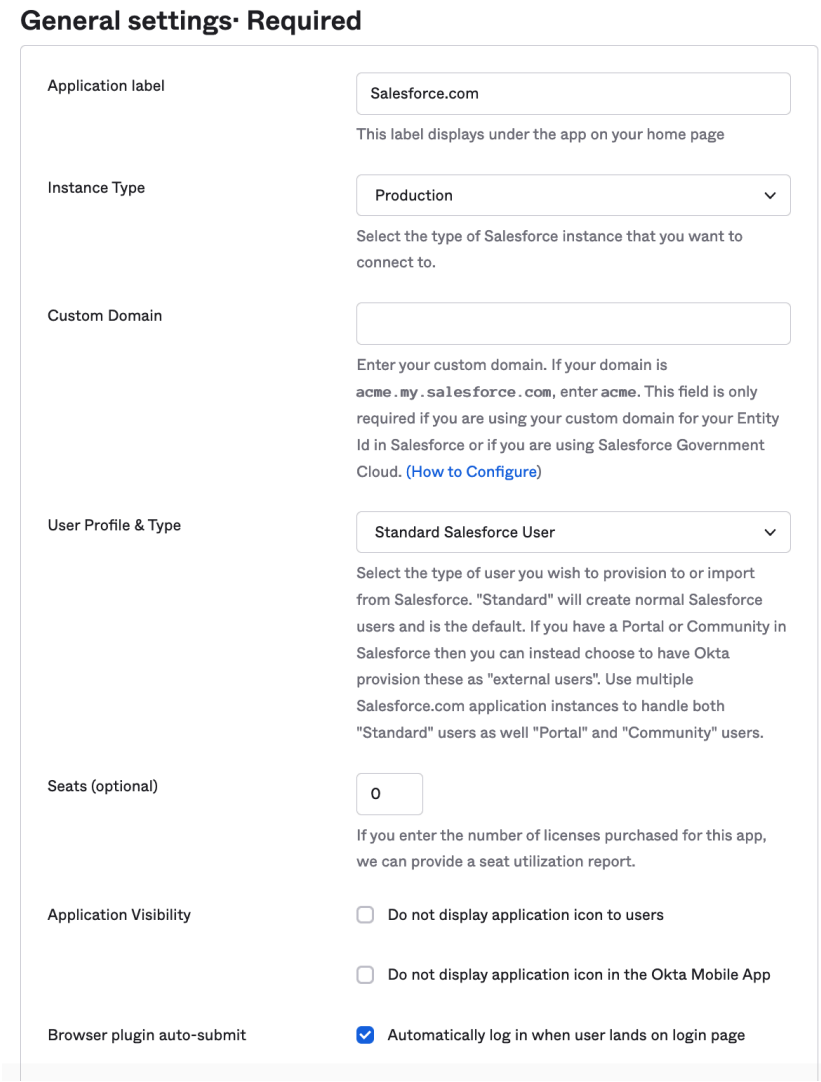
1.1 - Configure Salesforce application with SAML

1. Signup for a free Salesforce developer account.
2. Once your signup is complete, log into the Salesforce Developer account.
3. Log into your Okta admin console.
4. Navigate to **Applications** > **Applications.** Click on **Browse App Catalog**.
5. Search for Salesforce.com.

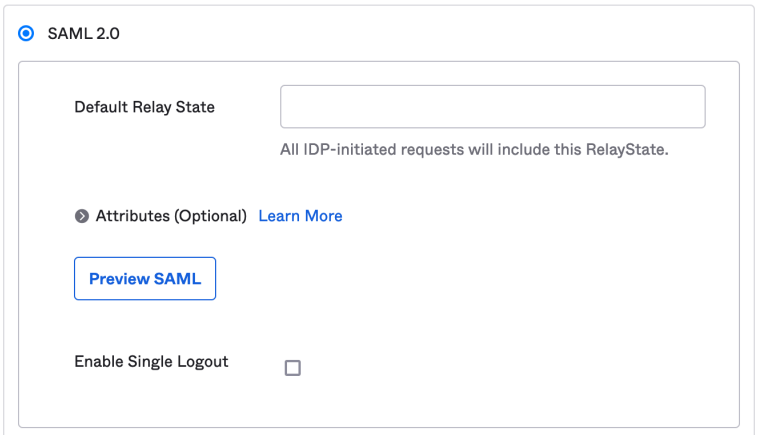


6. Click on the Salesforce.com app and click **Add Integration.**

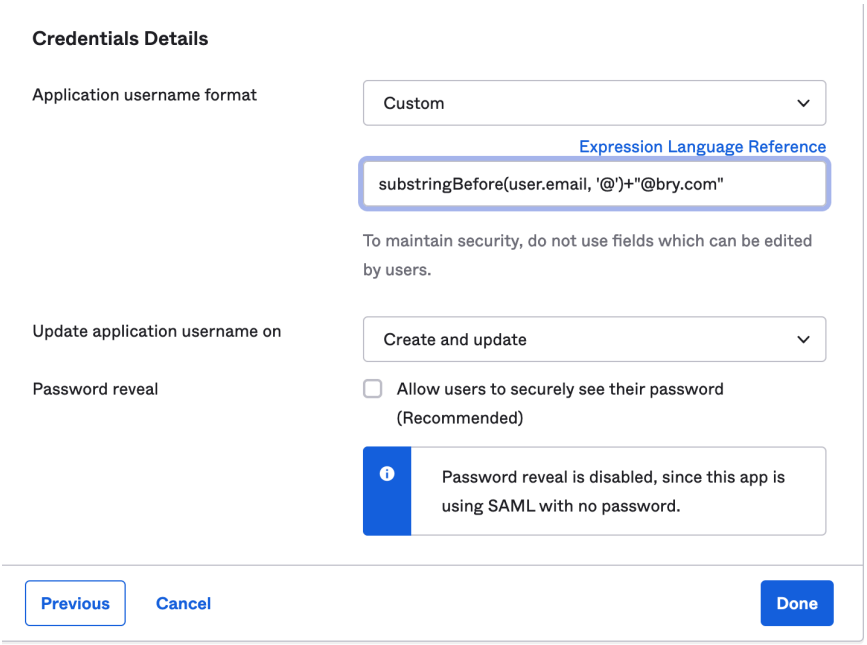
7. Leave the defaults under General Settings and click **Next**.



8. On the Sign-On Options page, select **SAML 2.0**.

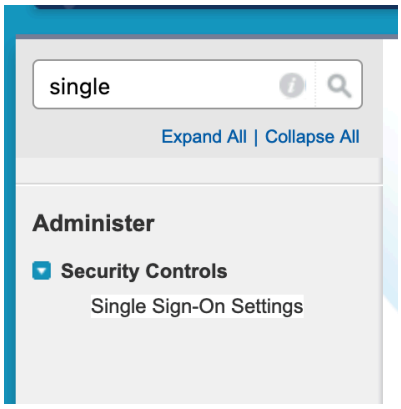


9. Salesforce requires unique names for provisioning. To avoid username conflicts, we are going to create a custom username format based on the Okta Expression Language. Scroll down to the **Credentials Details** section.
10. Change the Application username format from **Okta username** to **Custom**.
11. In the custom string field, type **substringBefore(user.email, '@')+"@bry.com"**, but with a domain of your preference. It doesn't have to be a valid domain. We will use this naming convention for the future lab to provision users to Salesforce. This custom string field takes the prefix of the email and adds **@bry.com** to it.



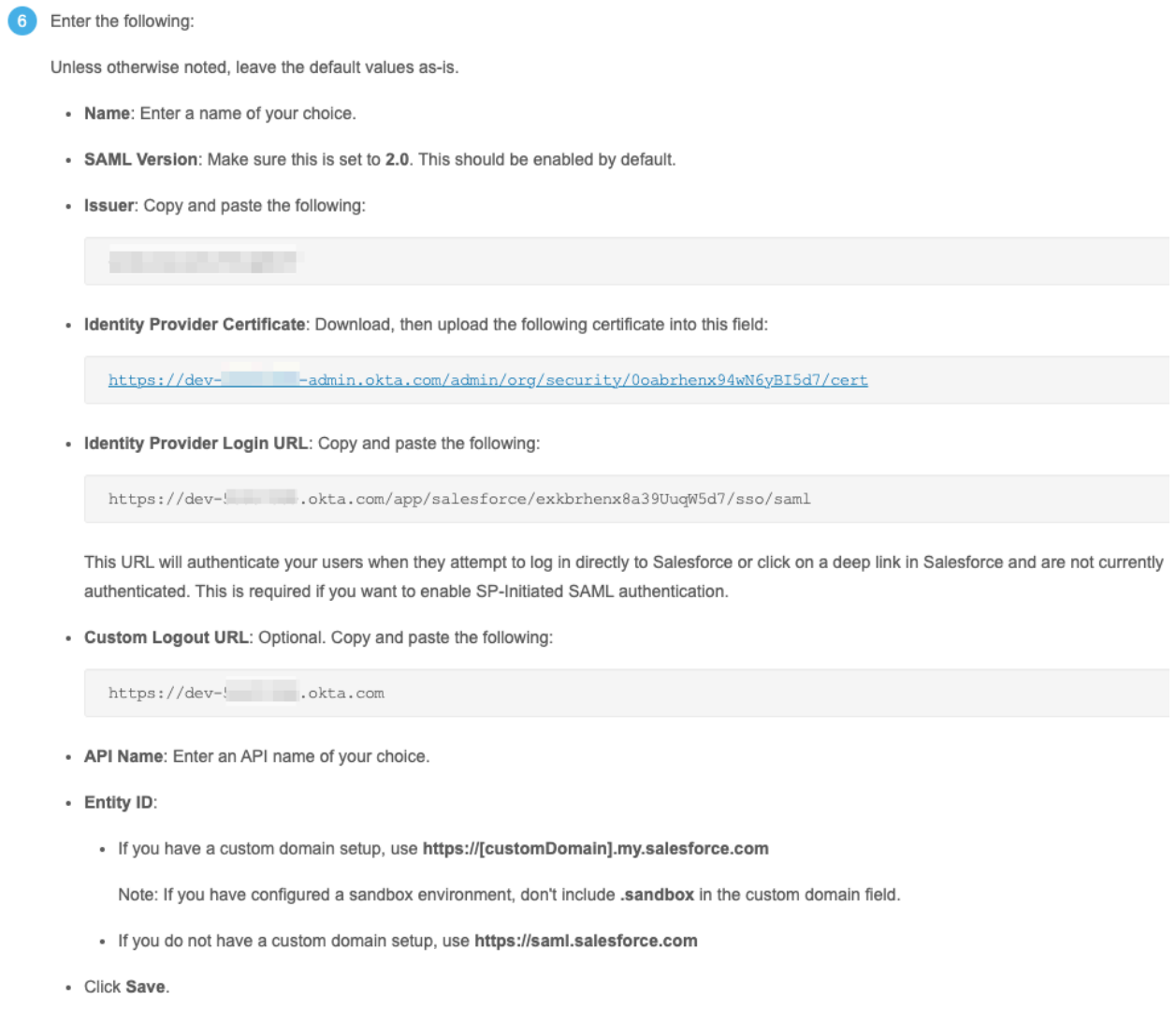
12. Click **Done**.
13. Click on the '**Sign On**' tab and on the right side of the page, click **View Setup Instructions** to open a page with instructions for configuring SAML 2.0 for Salesforce.
14. Open your Salesforce Developer account which you should still be logged in. If not, log into the account.

15. On the top left side in the Quick Find/ Search section, type in **Single Sign-On Settings**. Click on **Single Sign-On Settings** in the result.



16. Click **Edit** and check SAML Enabled under 'Federated Single Sign-On Using SAML'.
17. Click **New.**

18. Follow step 6 in the instructions from the Setup SSO page *(if you're missing the page, reopen it by clicking View Setup Instructions – step 13)*.



6 Enter the following:

Unless otherwise noted, leave the default values as-is.

- **Name**: Enter a name of your choice.
- **SAML Version**: Make sure this is set to **2.0**. This should be enabled by default.
- **Issuer**: Copy and paste the following:

  [redacted]

- **Identity Provider Certificate**: Download, then upload the following certificate into this field:

  https://dev-[redacted]-admin.okta.com/admin/org/security/0oabrhenx94wN6yBI5d7/cert

- **Identity Provider Login URL**: Copy and paste the following:

  https://dev-[redacted].okta.com/app/salesforce/exkbrhenx8a39UuqW5d7/sso/saml

  This URL will authenticate your users when they attempt to log in directly to Salesforce or click on a deep link in Salesforce and are not currently authenticated. This is required if you want to enable SP-Initiated SAML authentication.

- **Custom Logout URL**: Optional. Copy and paste the following:

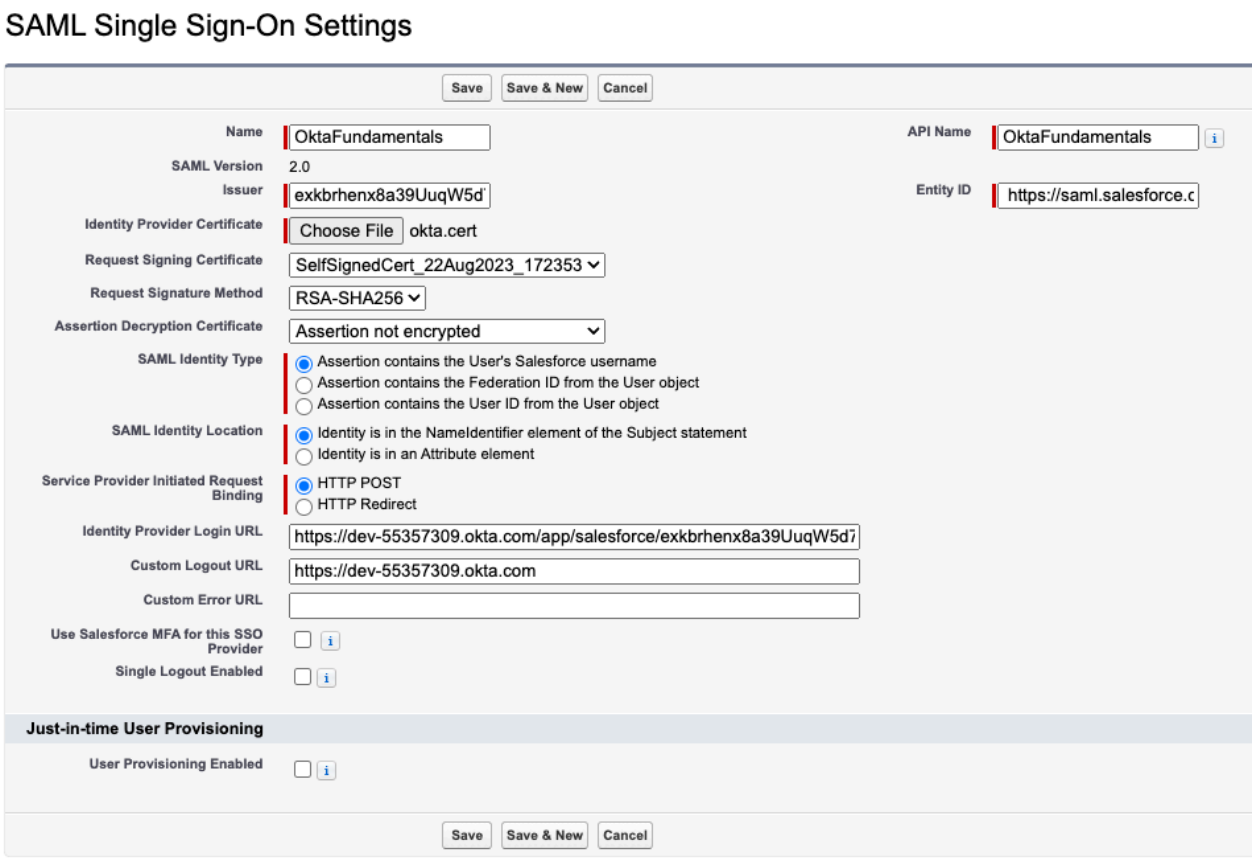
  https://dev-[redacted].okta.com

- **API Name**: Enter an API name of your choice.
- **Entity ID**:
  - If you have a custom domain setup, use **https://[customDomain].my.salesforce.com**

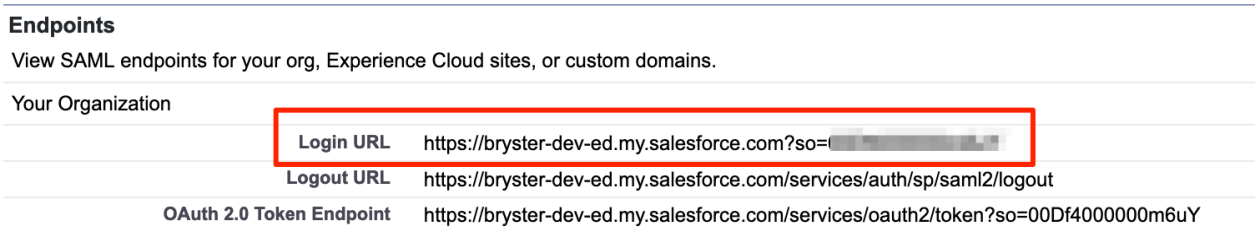
    Note: If you have configured a sandbox environment, don't include **.sandbox** in the custom domain field.

  - If you do not have a custom domain setup, use **https://saml.salesforce.com**
- Click **Save**.

19. You should have a similar configuration as the screenshot below after entering the information from the previous step:

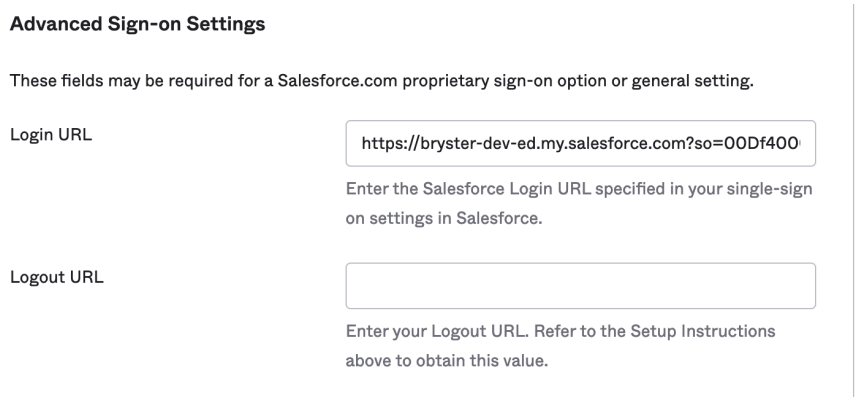


20. Click **Save.**
21. Scroll down to the Endpoints section and copy the **Login URL**.

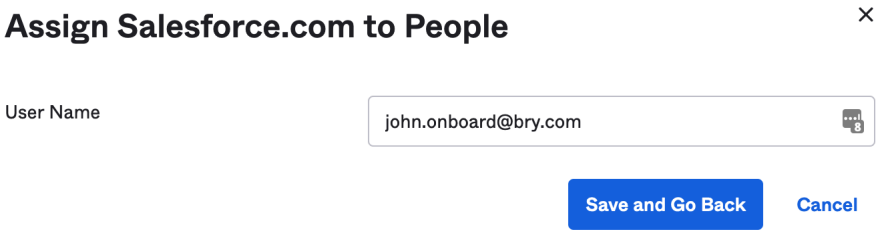


22. Go back to your Okta Admin console and the Sign-On tab from Salesforce. Click **Edit**.

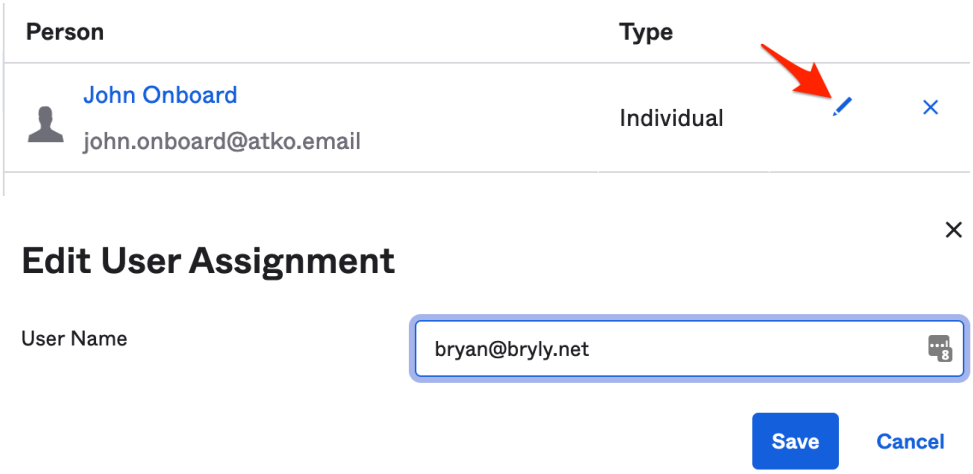
23. Paste the Login URL in the Advanced Sign-on Settings section.



24. Click **Save**.
25. In the assignment tab, select a user to assign to the Salesforce app. The username needs to match the exact Salesforce username that was created during the initial registration for the developer account.

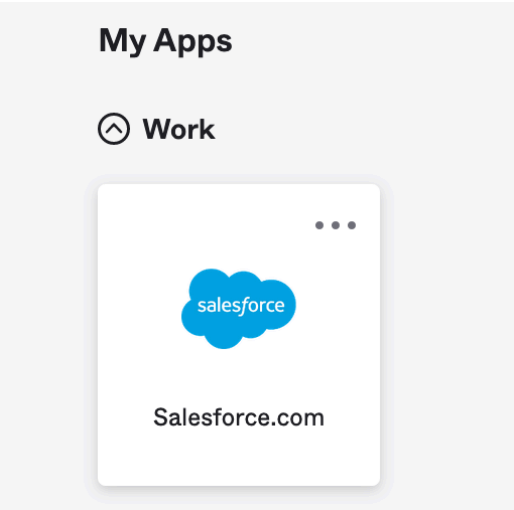


If you need to change the assignment of the username, you can go back to the Assignments tab and click the pencil icon.



26. Click **Save and Go Back**. Click **Done**.

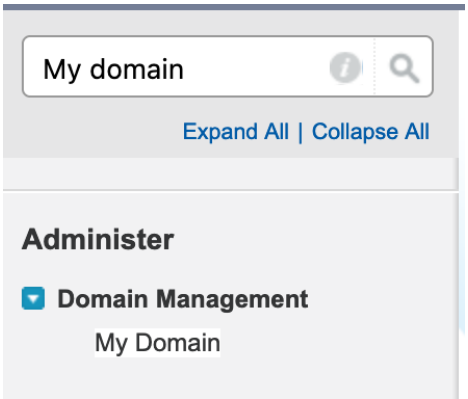
27. Log into the end user dashboard and you should see the Salesforce app.



28. Log out of all Salesforce instances.
29. Click on the **Salesforce.com** app from the user dashboard to SSO.
30. You should be logged in successfully as the user. Log out from Salesforce and confirm you are directed back to the main Okta dashboard. This is because we set the custom logout URL to Okta.
31. Great Work !!! You have now successfully configured Salesforce with SAML as a sign-on method.

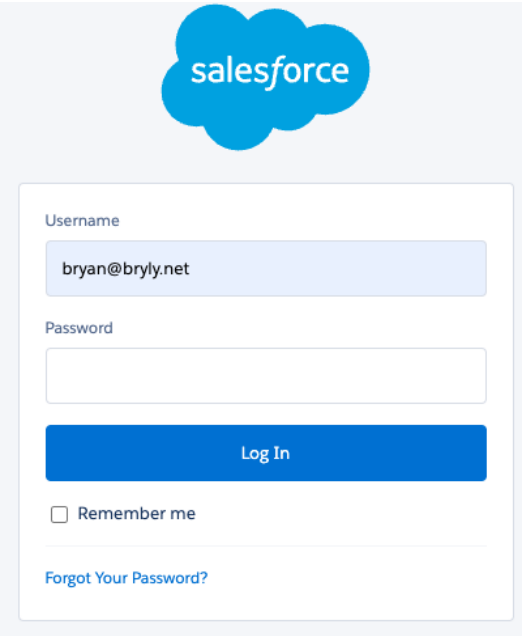
1.2 - Configure SP-Initiated SAML between Salesforce and Okta

1. We'll first need to configure a customized domain name in Salesforce.
2. Log in to your Salesforce instance.
3. Navigate to the **My Domain** page.
4. On the top left side in the Quick Find/ Search section, type in **My Domain**.



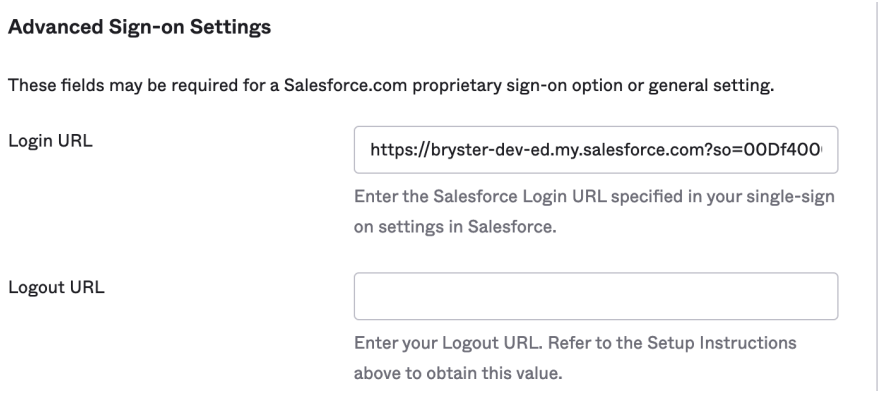
5. **Choose Your Domain Name** and **Check Availability**.
6. Click **Register Domain.**

7. At this point your new org name in Salesforce (https://[orgname].my.salesforce.com) will be published to the internet and should become widely available for use within 12-24 hours. You can test this by trying to navigate to your new org name in a browser window.
8. You'll receive an email when your **domain is ready for testing**.
9. The link will prompt you to manually login and test the functionality of your custom domain.

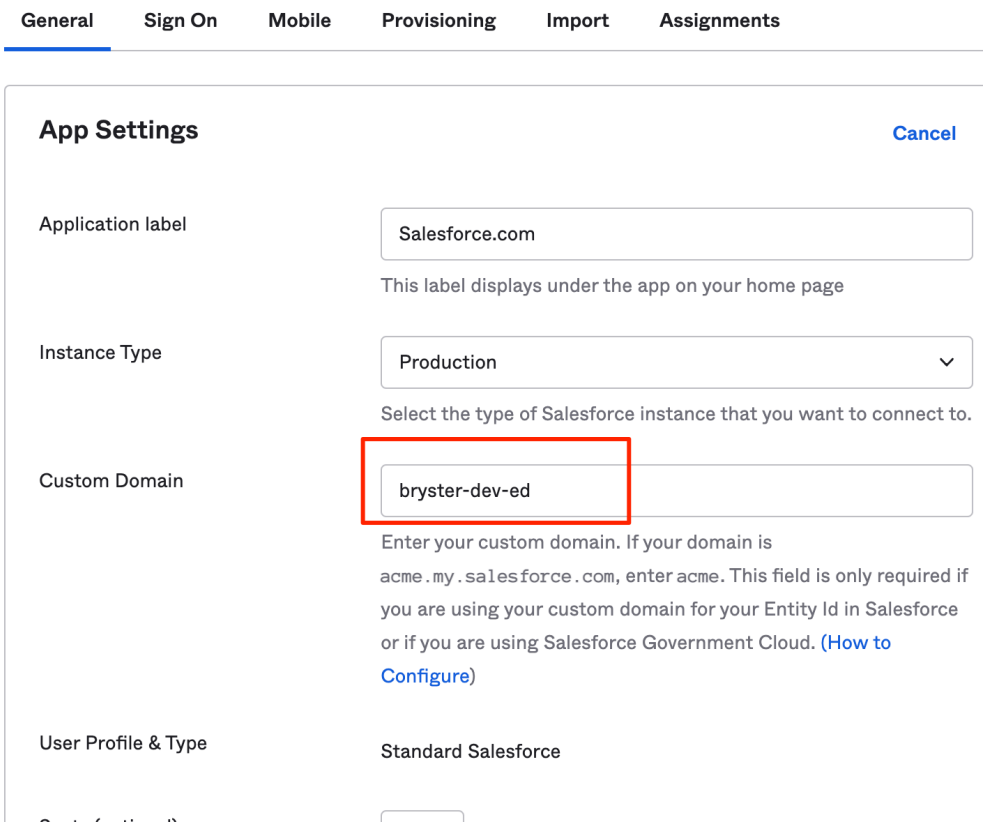


10. You should now be authenticated to Salesforce.
11. We need to make some configuration changes to our Single Sign-On Settings to use the new domain.
12. Navigate to **Single Sign-On Settings** using the Quick Find option.
13. Locate your current SAML configuration and click **Edit**.
14. Change the Entity ID from *https://saml.salesforce.com* to *https://[customDomain].my.salesforce.com*. Click **Save**.
15. Click on the **Name** of your SAML profile.
16. Copy the new **Login URL** from the Endpoints section.
17. Switch back to your **Okta Admin** console.
18. Navigate to **Applications** > **Applications > Salesforce** > **Sign On** tab and click **Edit**.

19. Under Advanced Sign-on Settings, paste the **Login URL**.

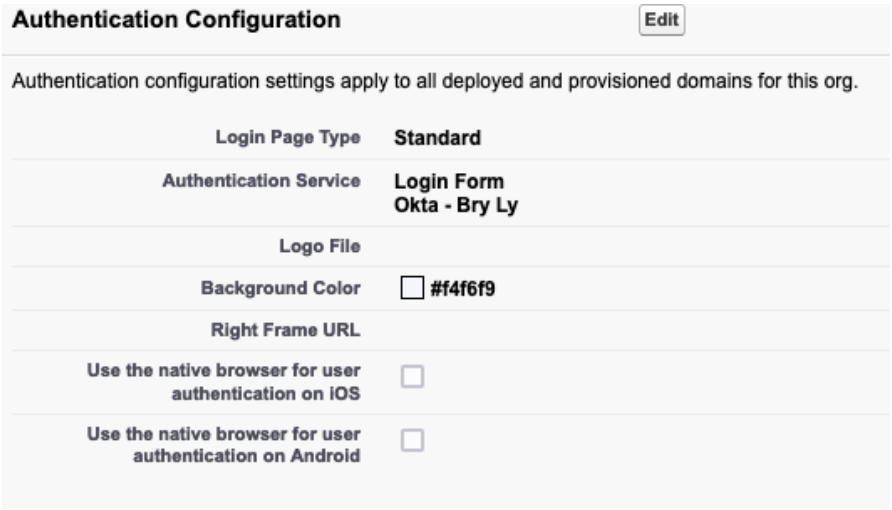


20. Click **Save**.
21. Navigate to **Applications** > **Applications > Salesforce** > **General** tab and click **Edit**. Enter in the custom domain.

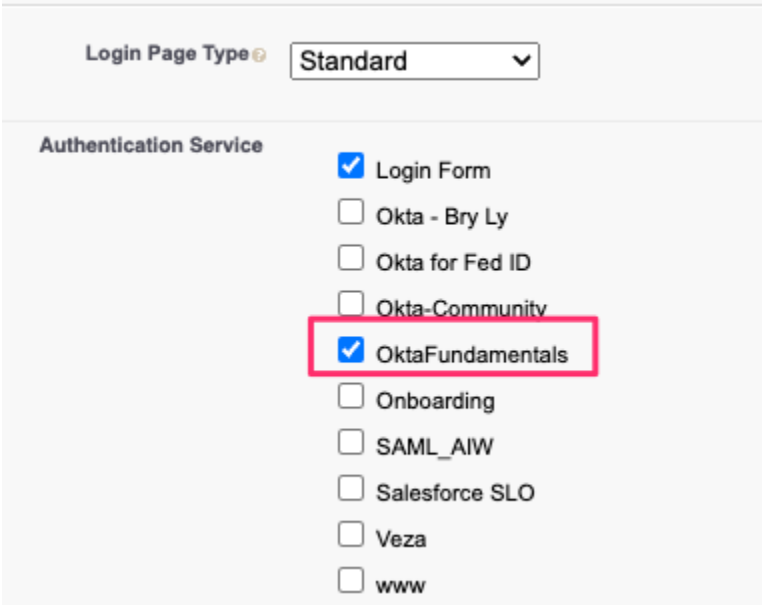


22. Click **Save**.
23. Next, we're going to choose Okta as the Default Authentication Services.
24. Switch back to your **Salesforce.com** login.
25. Use the Quick Find option to search for **My Domain**.

26. Under Authentication Configuration, click **Edit**.

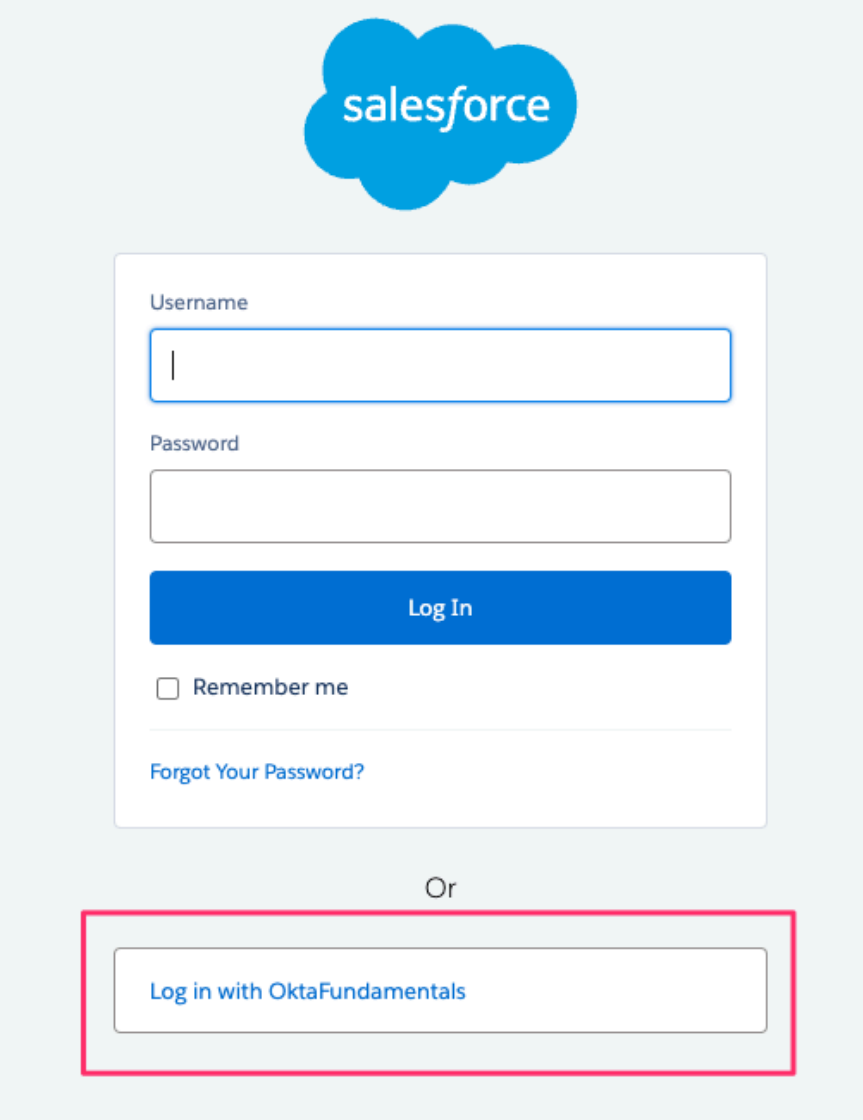


27. In the Authentication Service section, check the box next to the Okta instance you've set up in single-sign on settings and click **Save**.



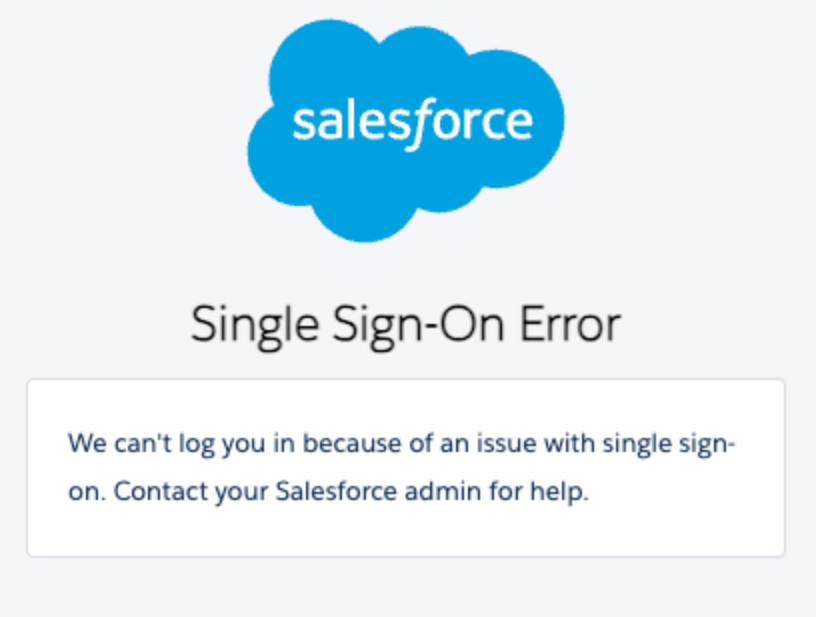
28. To verify if the SP-Initiated SAML flow has been configured properly, log out of all active Okta and Salesforce sessions.
29. Navigate to your Salesforce Custom Domain URL (*e.g. https://bryster-dev-ed.my.salesforce.com*) and you should see the option to login

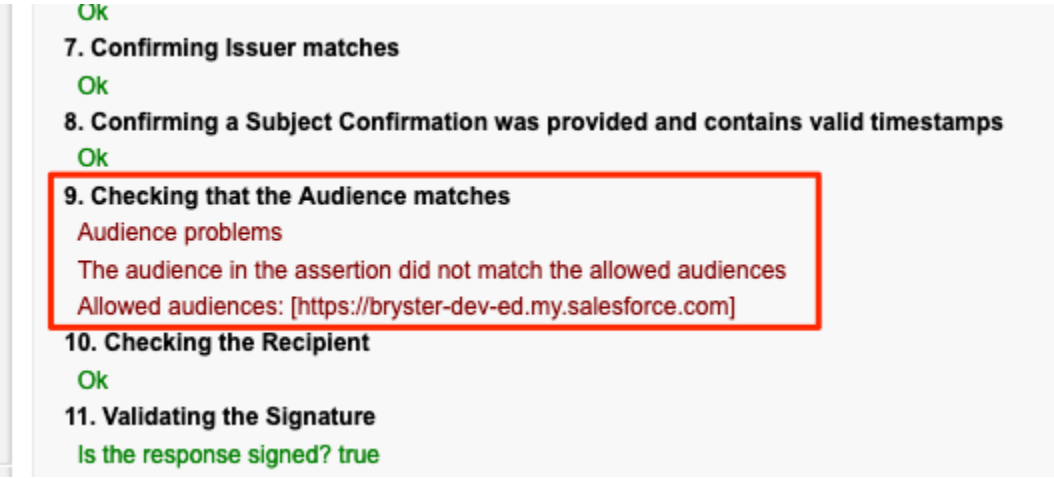
using your Identity Provider. i.e '*Log in with OktaFundamentals*'



30. Selecting your IDP will direct you to login into Okta.
31. Authenticating into Okta with a user assigned to the Salesforce app should then provide you access to Salesforce.

NOTE: If you receive the single sign-on error, check the entity ID in the SAML Single Sign-On settings in Salesforce. It's because we still had the Entity ID set to: *https://saml.salesforce.com*. We need to switch it to our custom domain URL.





Once you change the entity ID and save, try again and you should be successfully logged in.

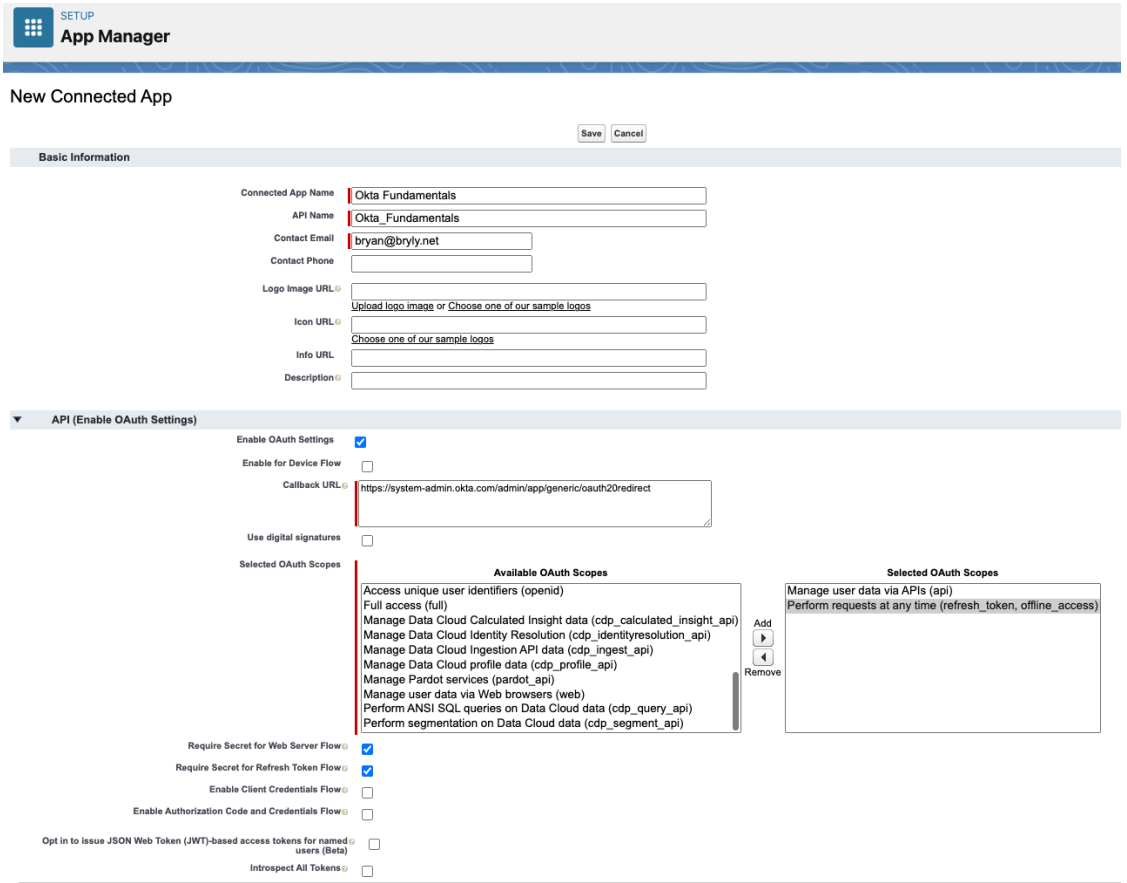
1.3 - (OAuth Consumer Key and OAuth Consumer Secret)

By using Provisioning you can create users in Salesforce using Okta or update them when they are updated in Okta. To configure Salesforce with Provisioning, follow the instructions below:

1. Go to the Salesforce application settings in Okta.
2. Click on the **Provisioning** tab and click on **Configure API Integration.**
3. **Enable** API Integration

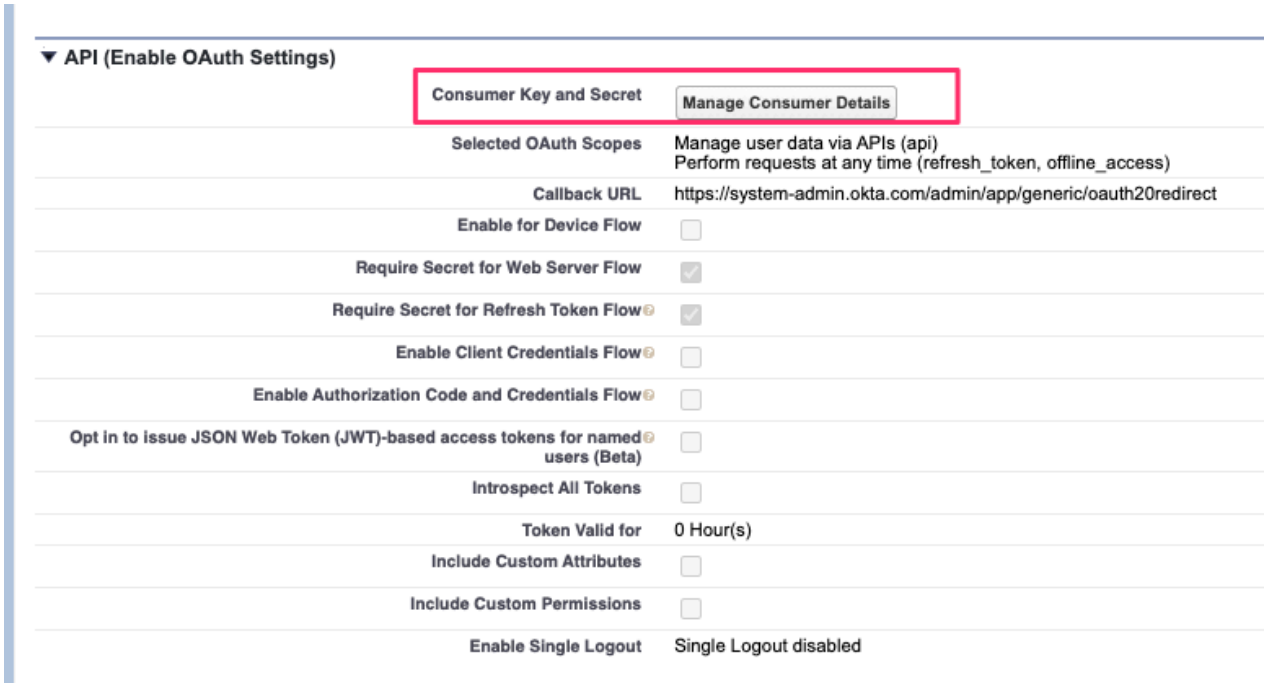
4. You will be asked to provide the OAuth Consumer Key & Secret. Follow the steps below to create the OAuth consumer key and consumer secret used in Salesforce REST integration.
5. In Salesforce, create a connected app & enable OAuth Settings for API Integration:
    a. Create a Connected App: Configure Basic Connected App Settings.
    b. Enable OAuth Settings for API Integration:
        - **Enable for Device Flow**: uncheck
        - **Callback URL**: https://system-admin.okta.com/admin/app/generic/oauth20redirect
        - **Use digital signatures**: uncheck
        - **Selected OAuth scopes**:
            - Manage user data via APIs (api)
            - Perform requests at any time (refresh_token, offline_access)
        - **Require Secret for Web Server Flow**: check
        - **Require Secret for Refresh Token Flow**: check
        - **Introspect All Tokens**: uncheck
        - **Configure ID Token**: uncheck
        - **Enable Asset Tokens**: uncheck

- **Enable Single Logout**: uncheck



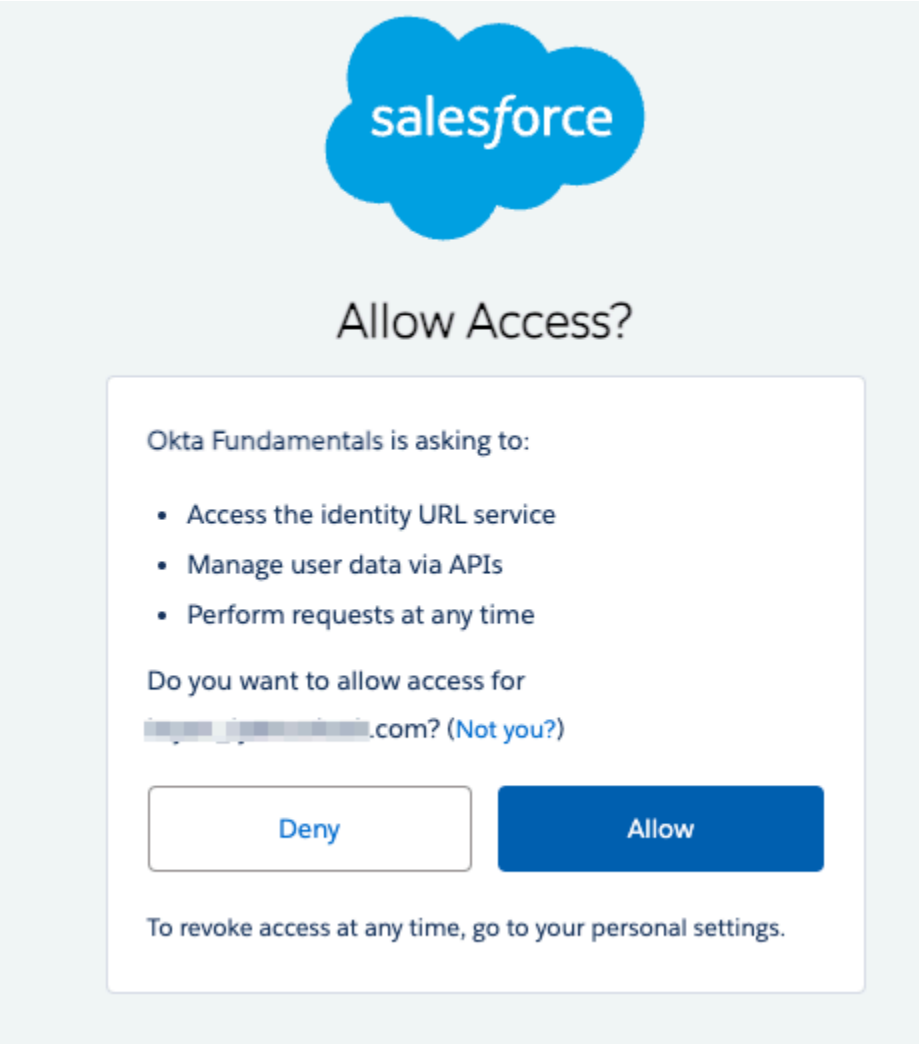
6. Once saved, get your Consumer Key and Consumer Secret under API (Enable OAuth Settings) section and use them for enabling provisioning for Salesforce in

Okta.

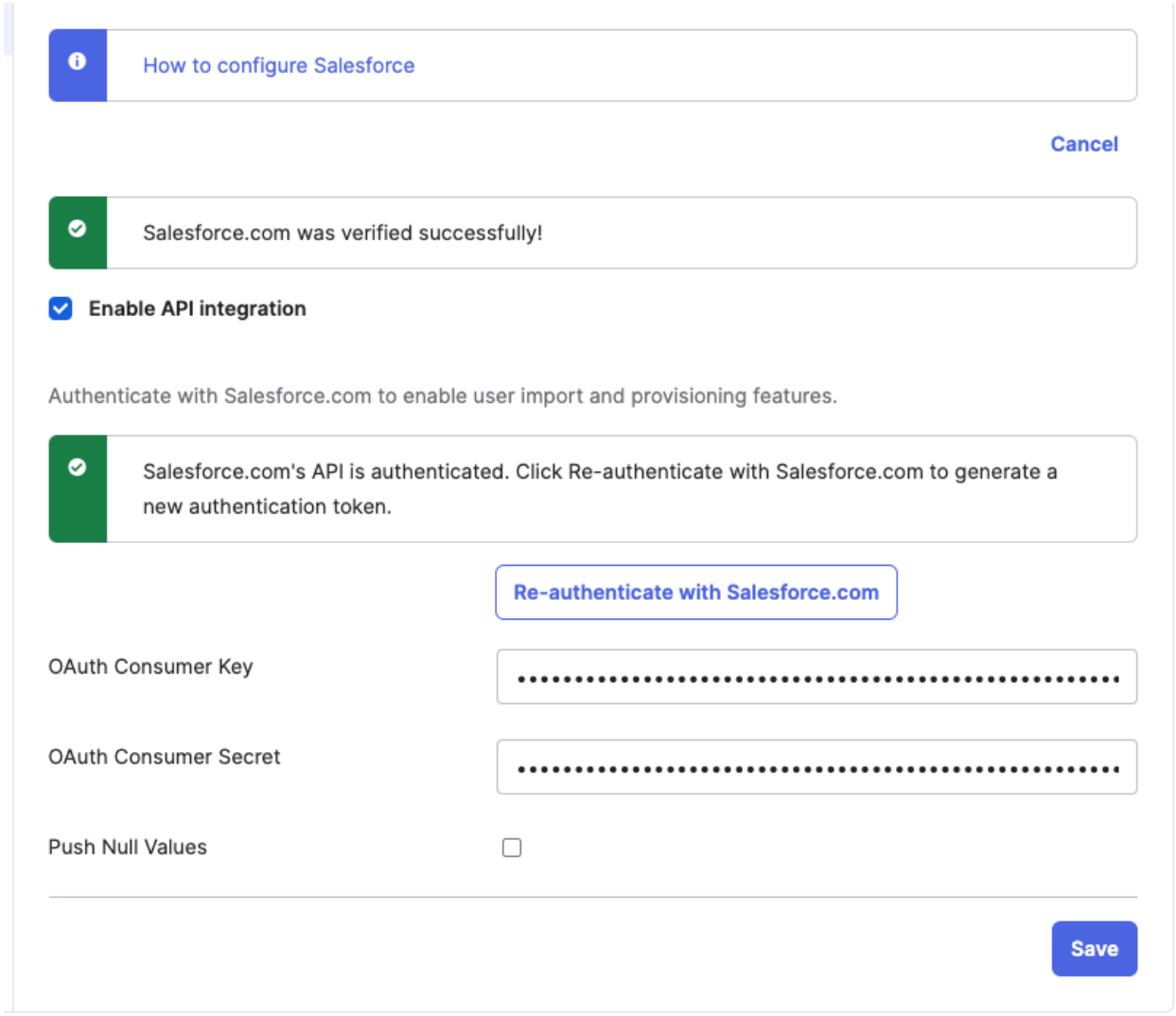


7. In the Okta Admin Console go to **Provisioning** > **Integration**.
8. Enter the following:
    a. OAuth Consumer Key: *Consumer Key from your Salesforce OAuth settings*
    b. OAuth Consumer Secret: *Consumer Secret from your Salesforce OAuth settings*
9. Click Authenticate with Salesforce.com.
10. In the new Salesforce.com window, enter the *administrator username and password that you used to create the Connected OAuth App*. If you previously entered SOAP credentials, you don't need to enter them again.

11. Click Allow to permit access to your Connected App.



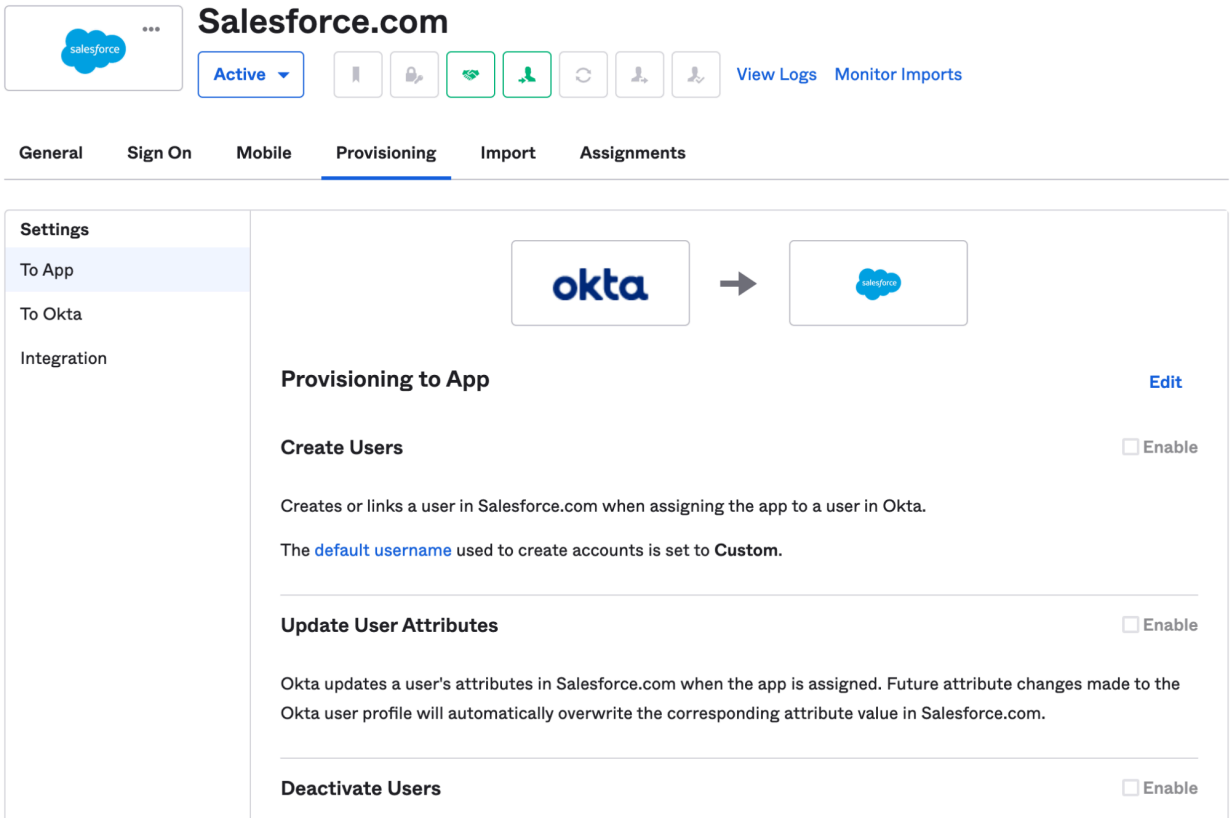
12. Click Save.



Note: If you received a credential error when performing **Re-authenticate with Salesforce.com,** try using an Incognito / Private Window.

13. You should now have provisioning options for the Salesforce app in Okta.

Enable **Create Users, Update User Attributes, Deactivate Users**.



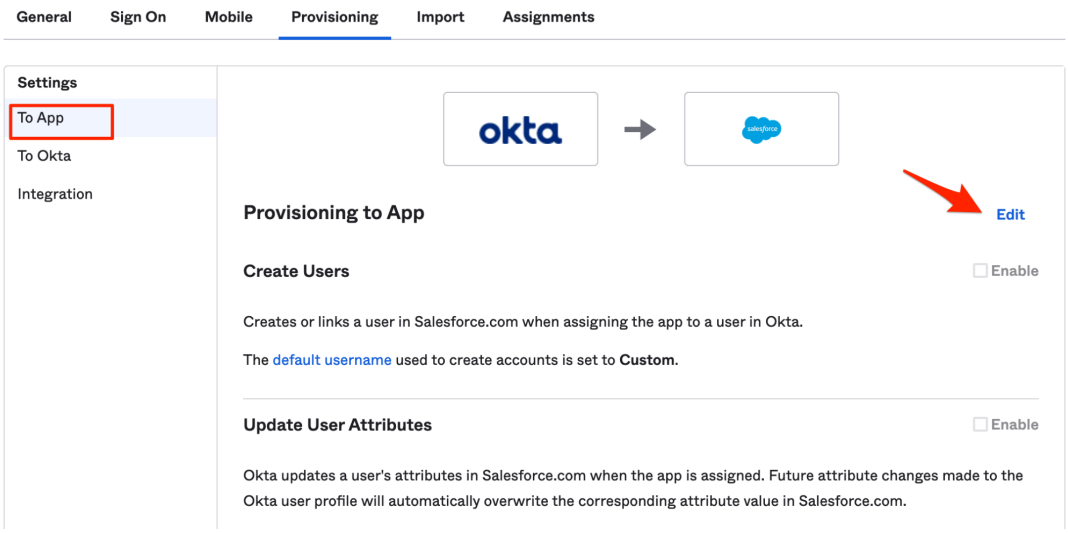
14. Test provisioning by assigning an account to the Salesforce application where Profile URL > Chatter Free User

Lab 1-7: Configure User Lifecycle Management in Okta

Objective	To configure User Lifecycle Management in Okta
Procedures	• Configure Salesforce with Lifecycle Management
Duration	30-45 minutes

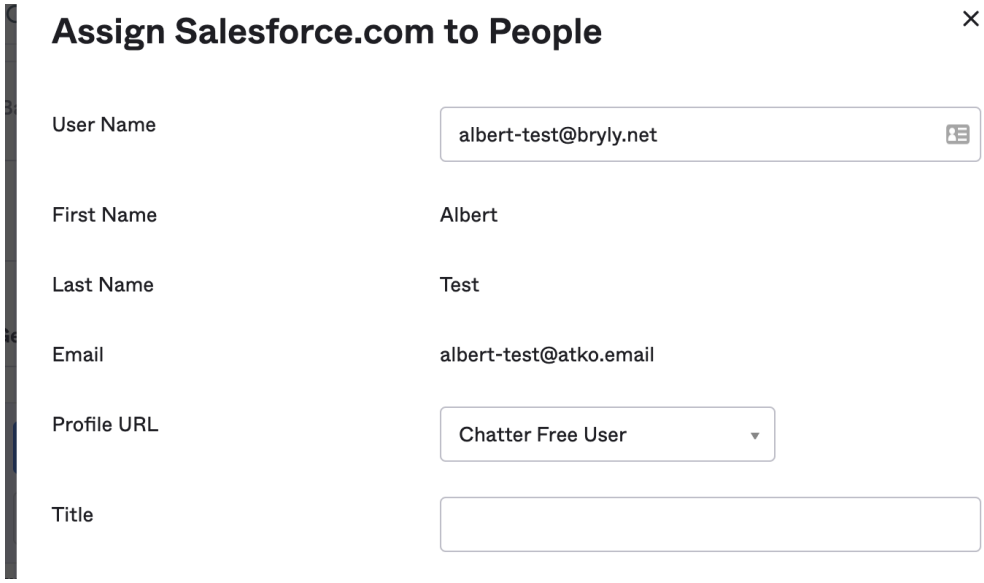
1.1 - Configure Salesforce with Lifecycle Management

1. You should have completed labs 6.3 for Salesforce provisioning. If not, please go back and complete this lab now. Proceed to the next steps if you have completed it.
2. Navigate to **Applications** > **Applications** > **Salesforce** and go to the **Provisioning** tab.
3. Double check that **Enable API Integration** has been enabled.
4. Under **Settings** > **To App** section, click **Edit** and enable **Create Users, Update User Attributes** and **Deactivate Users.**

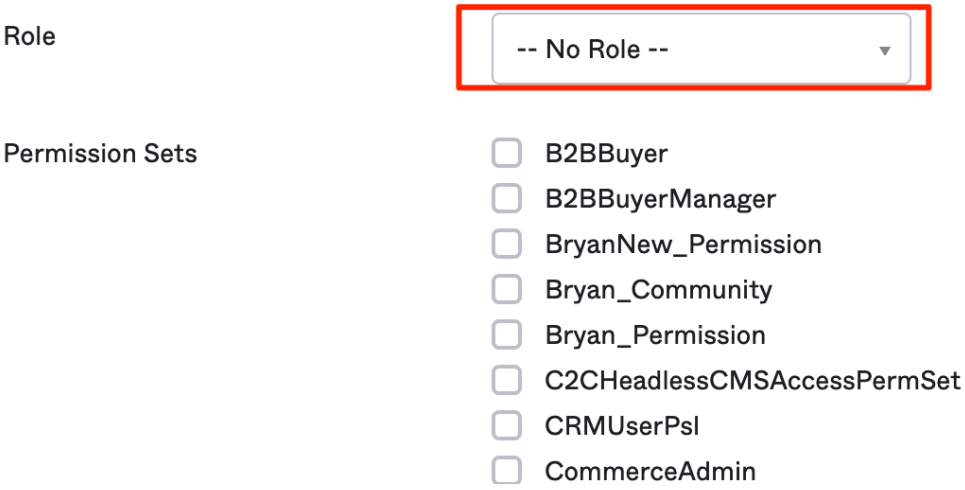


5. Click **Save**.
6. Go to the **Assignments** tab.
7. Assign the application to an Okta user that requires a Salesforce account.

8. For the Profile URL, select '**Chatter Free User**' (*no license limit for this profile type).*

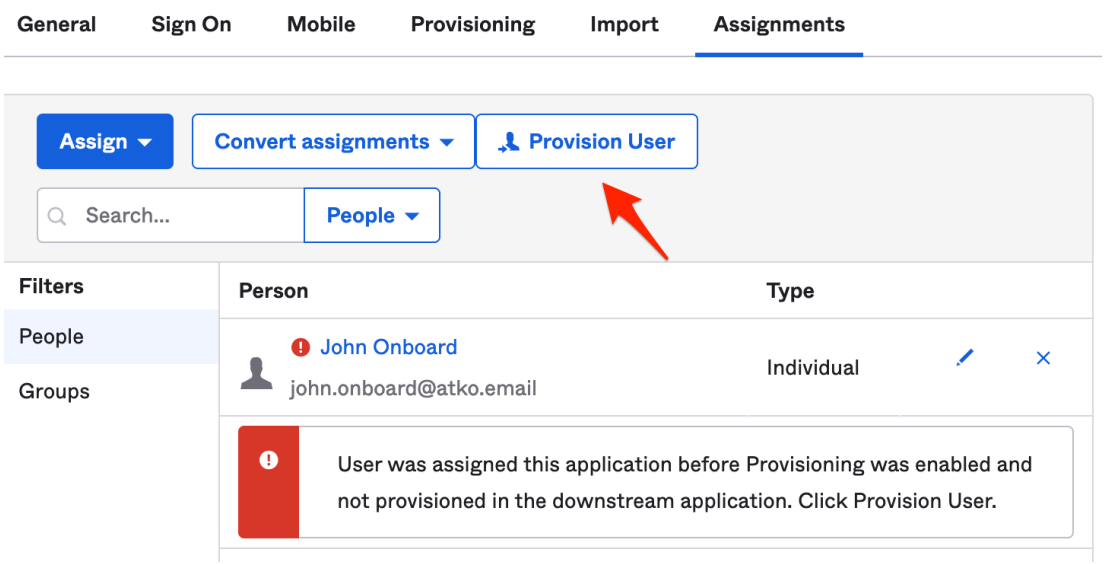


9. For Role, select '**No Role**'.

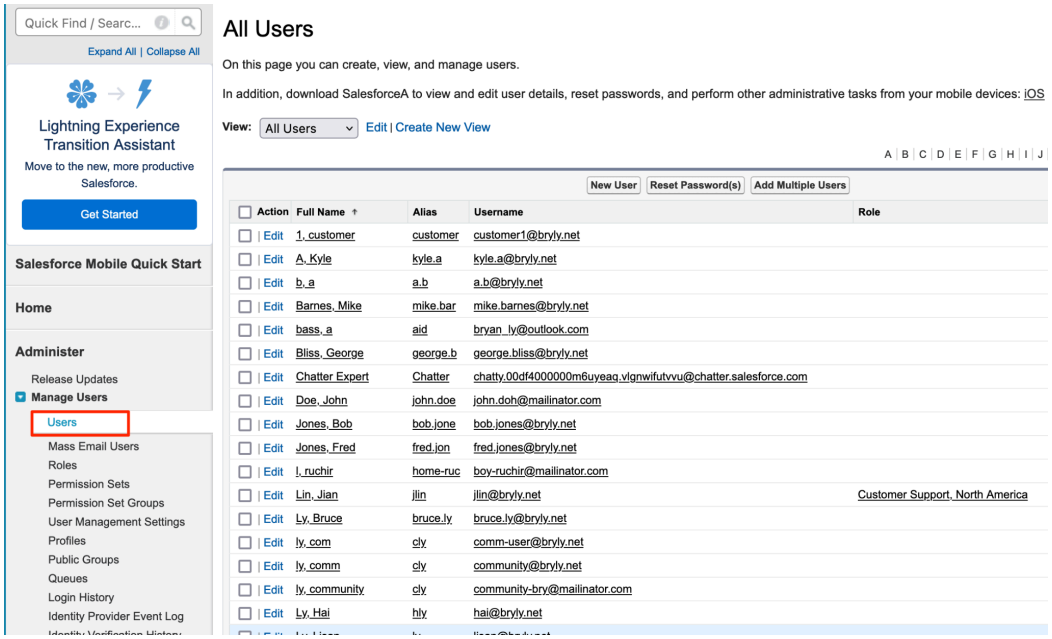


10. Click **Save and Go Back**.

11. If you see a red exclamation mark, it means there is an error. Click to see the error.



12. Click **Provision User**. This will trigger a provisioning job to Salesforce. If you do not see the Provision User button, proceed to the next steps.
13. You should now see the user assigned to Salesforce. To confirm, in Salesforce navigate to **Setup** > **Users** and search for the user.



14. Repeat Step 6 to assign one more user.
15. Log in to Okta with both users who were assigned to Salesforce to verify the SAML authentication flow and the profile assignment.

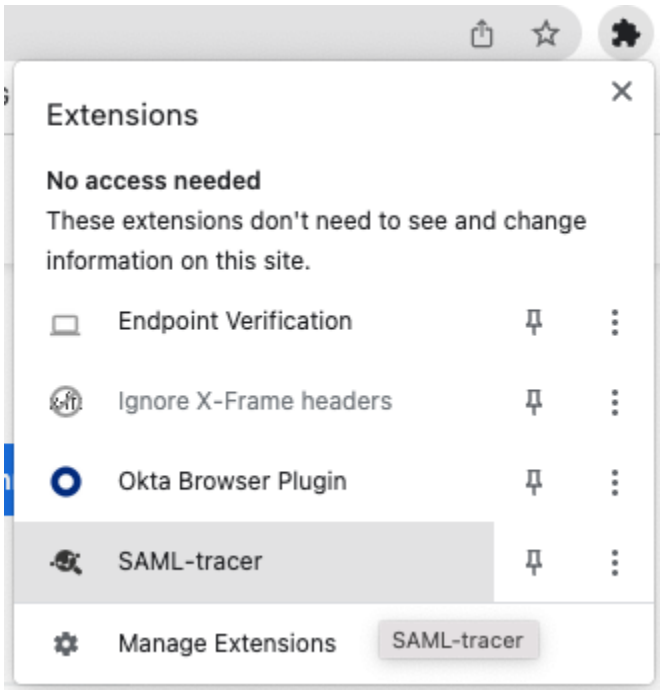
Lab 1-8: Set Up SAML Tracer for Troubleshooting

Objective	To configure troubleshooting options with SAML.
Procedures	• Configure SAML Tracer for Firefox & Chrome
Duration	10-20 minutes

1.1 - Configure SAML Tracer for Firefox & Chrome

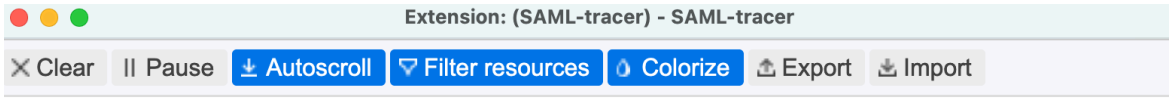
1. If you do not have Firefox, download it here. For Chrome, download here.
2. Get the SAML Tracer extension from the Firefox Add-Ons store. For Chrome, download the SAML tracer here.
3. Once installed, the SAML tracer tool can be accessed from the Firefox or Chrome toolbar.

Chrome:

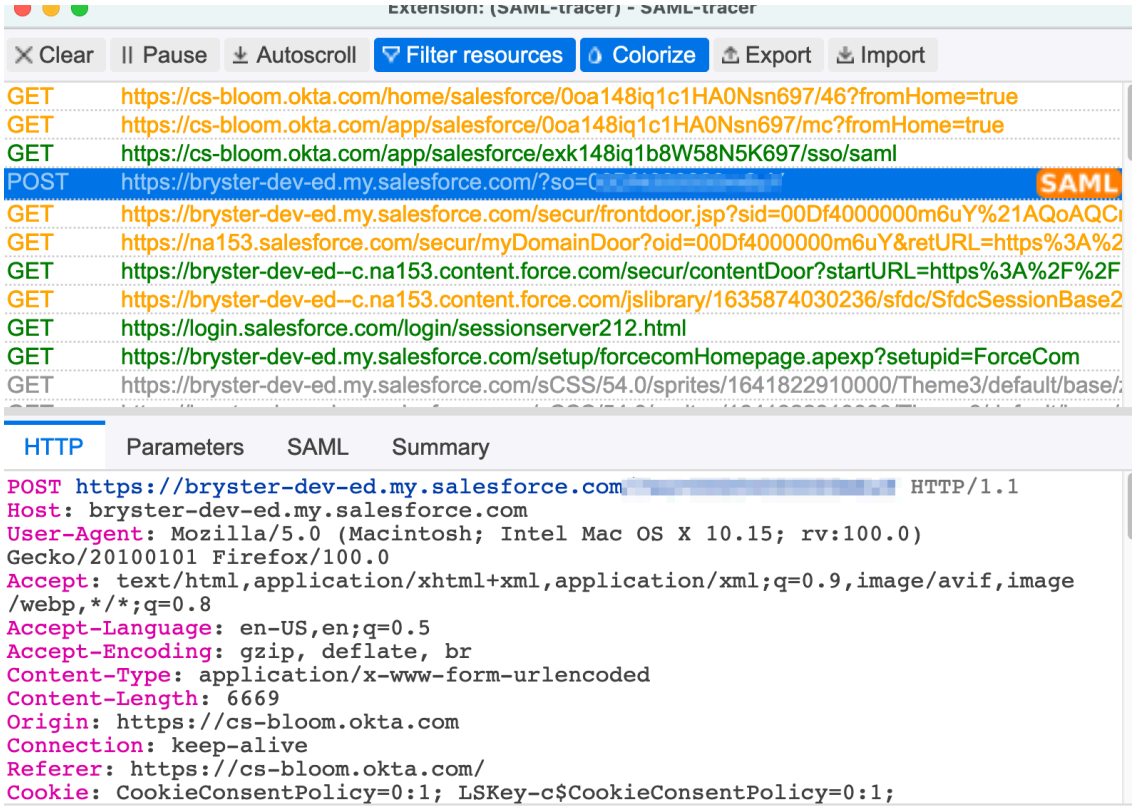


4. Open Firefox or Chrome and **log in to Okta**.

5. Start SAML Tracer (*the tool opens in a Firefox separate window*).

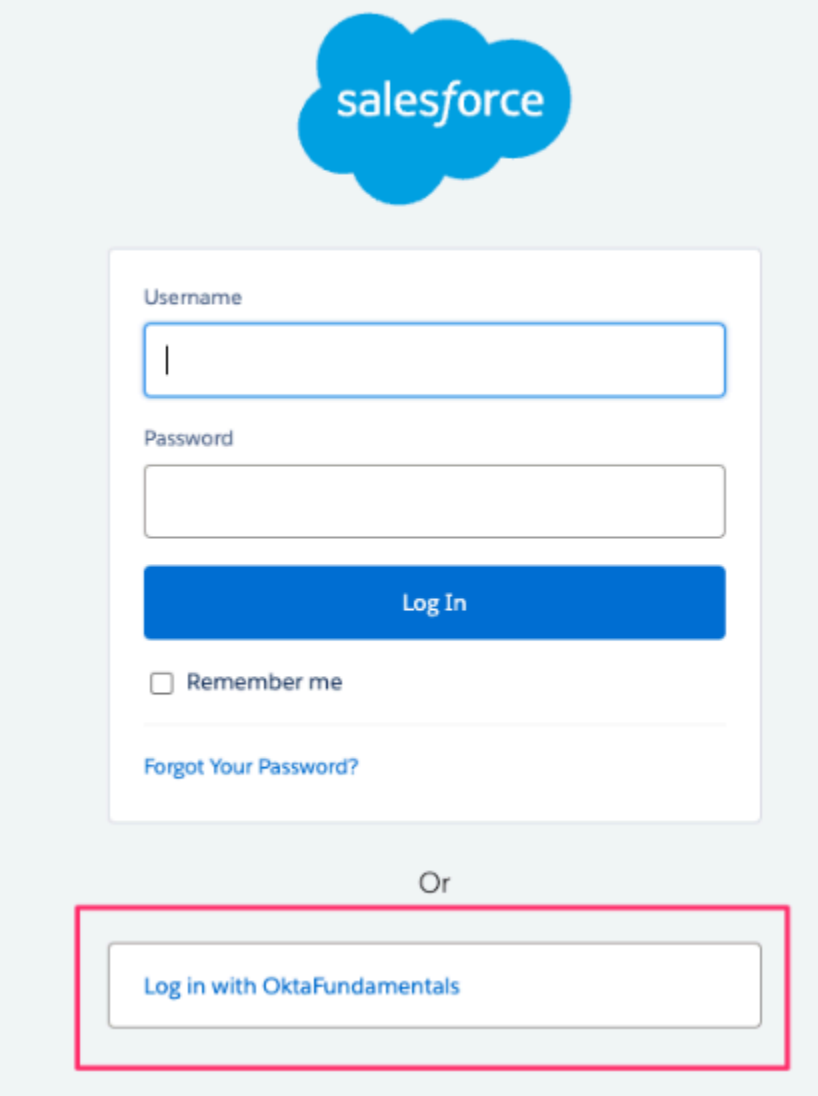


6. From your End-User dashboard, click **Salesforce**.
7. After being authenticated to Salesforce, switch to the **SAML Tracer** window.
8. Scroll through the contents and look for the **SAML** label.
9. To view the SAML assertion, click the **SAML POST** and select the **SAML tab**.



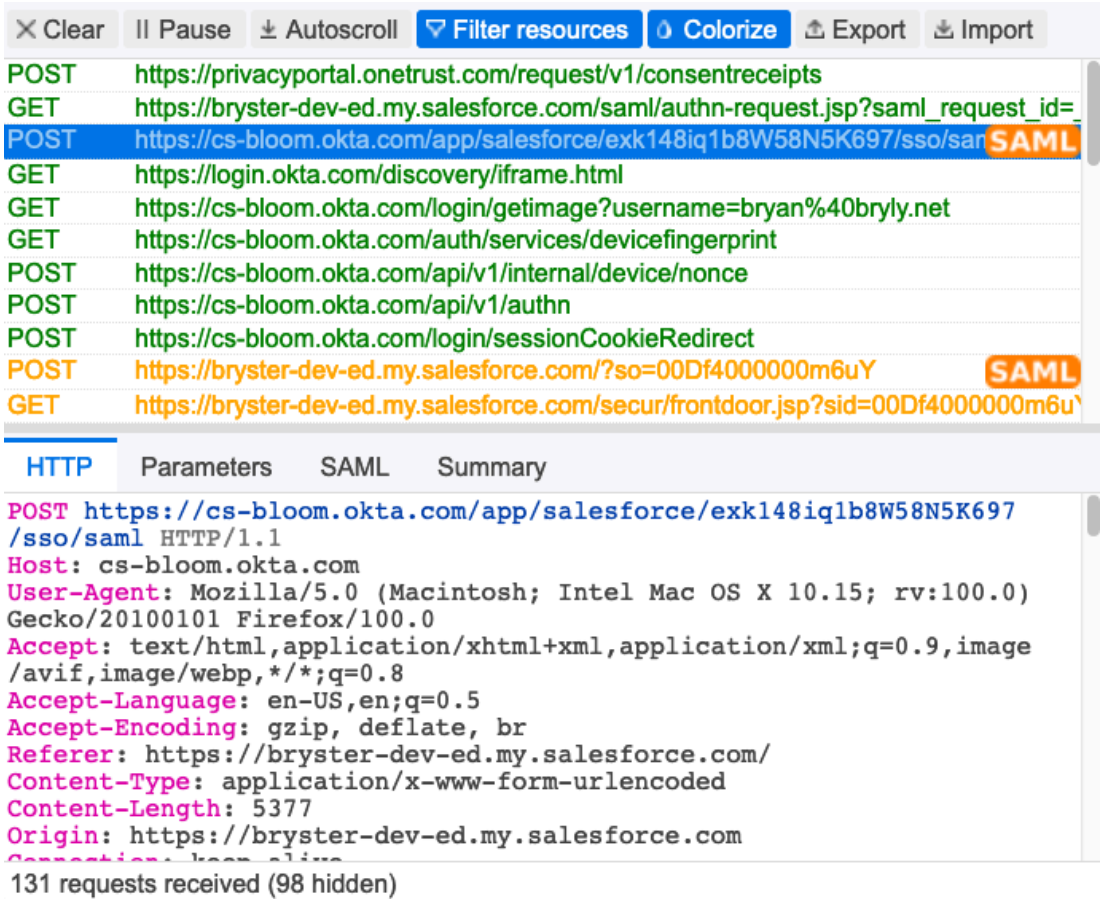
10. You can now validate the Destination URL, Audience, NameID and other attributes.
11. **Log out** of Salesforce.
12. Click **Clear** to remove previous network traffic, but do not close the SAML Tracer window.

13. In order to capture an **SP-Initiated SAML flow**, navigate to your Salesforce custom domain.



14. Select your **Identity Provider**, in this case 'Log in with OktaFundamentals'

15. Switch back to your SAML Tracer window



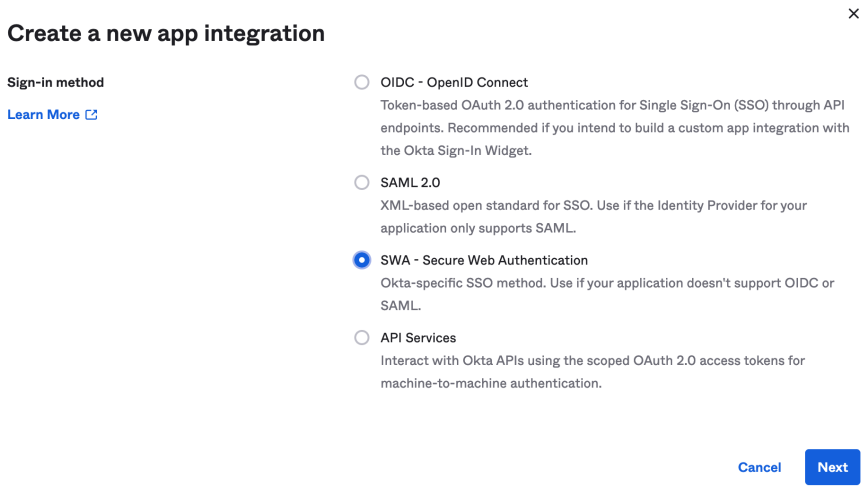
16. You can now see two SAML labels *(one for the **SAML Request** and the other for the **SAML Response**)*. Review both.
17. Use the **Export** option to save the web traffic flow.
18. Capture and review another SAML assertion from an application of your choice.

Lab 1-9: Configure Applications using the Application Integration Wizard (AIW)

Objective	To configure Applications using the Application Integration Wizard (AIW)
Procedures	• Configure a SWA application using the AIW – LinkedIn • Configure a SAML application using the AIW – Salesforce (metadata file)
Duration	20-30 minutes

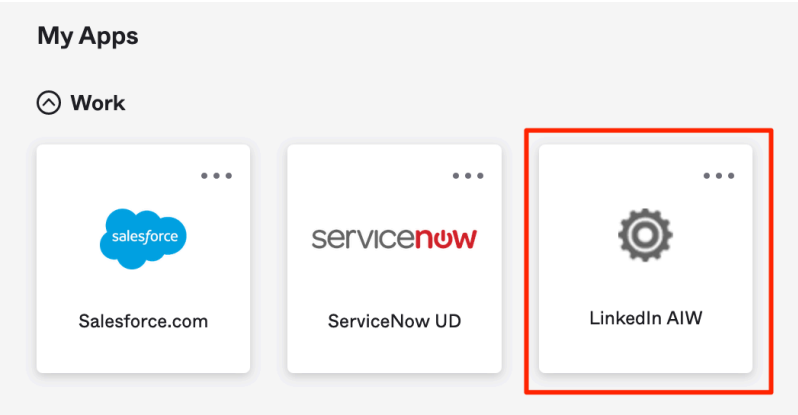
1.1 - Configure Linkedin using the Application Integration Wizard

1. Go to the **Okta Admin dashboard** > **Applications** > **Applications** > **Create App Integration**.
2. Select **SWA - Secure Web Authentication.**

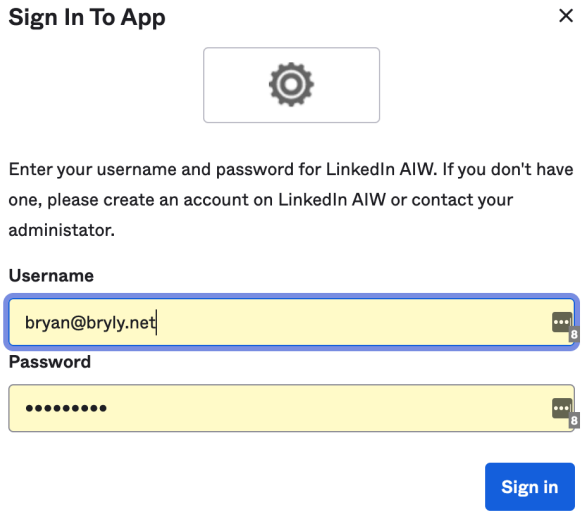


3. Click **Next**. Type **LinkedIn AIW** for the App name.
4. Enter the **App's login page URL**: https://www.linkedin.com/uas/login?
5. Click **Finish**.
6. Assign the application to your username.
7. Click **Save and Go Back**. Click **Done**.

8. Switch back to your End-User dashboard and open the LinkedIn AIW app.



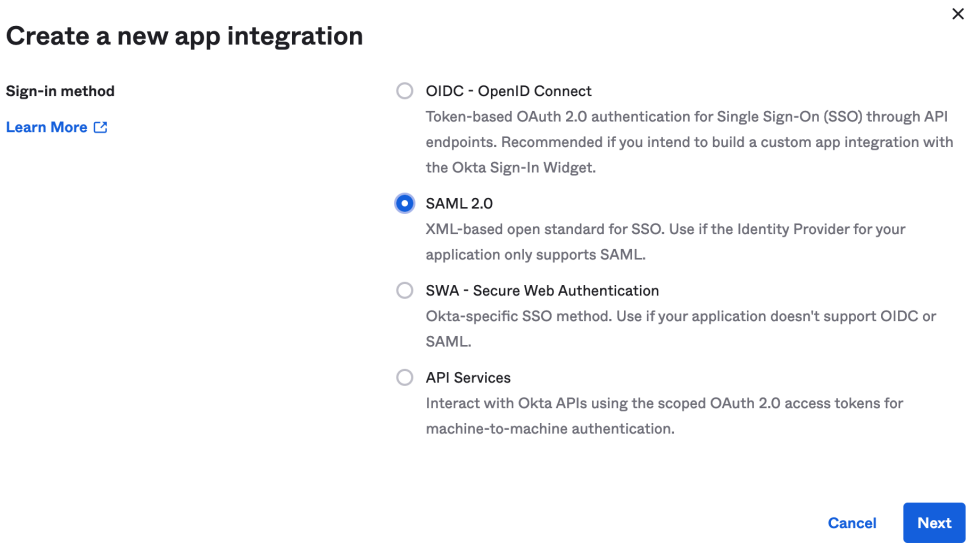
9. Enter your LinkedIn username and password and click **Sign in**.



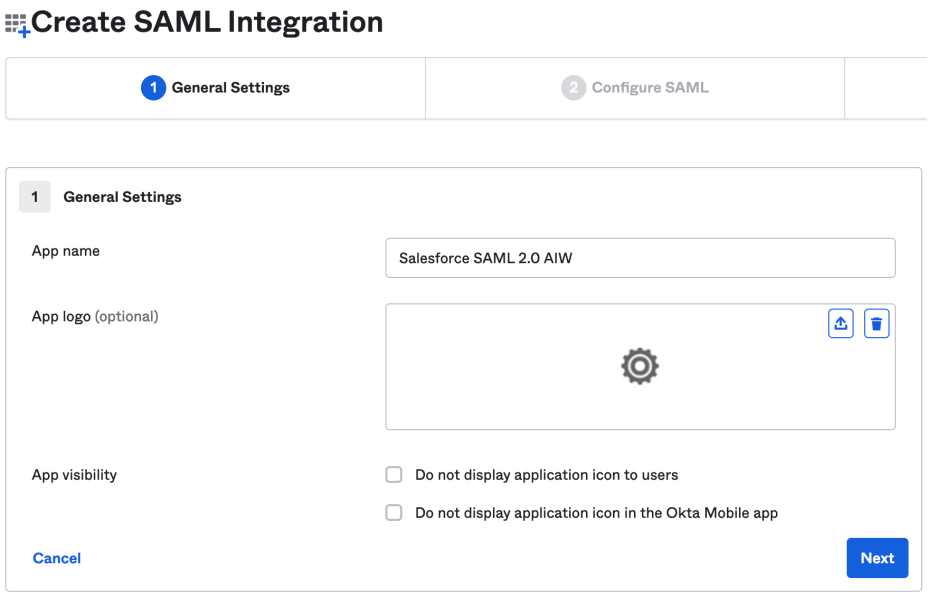
10. You should now be logged in to your LinkedIn profile.

1.2 - Configure a SAML application using the AIW – Salesforce (metadata file)

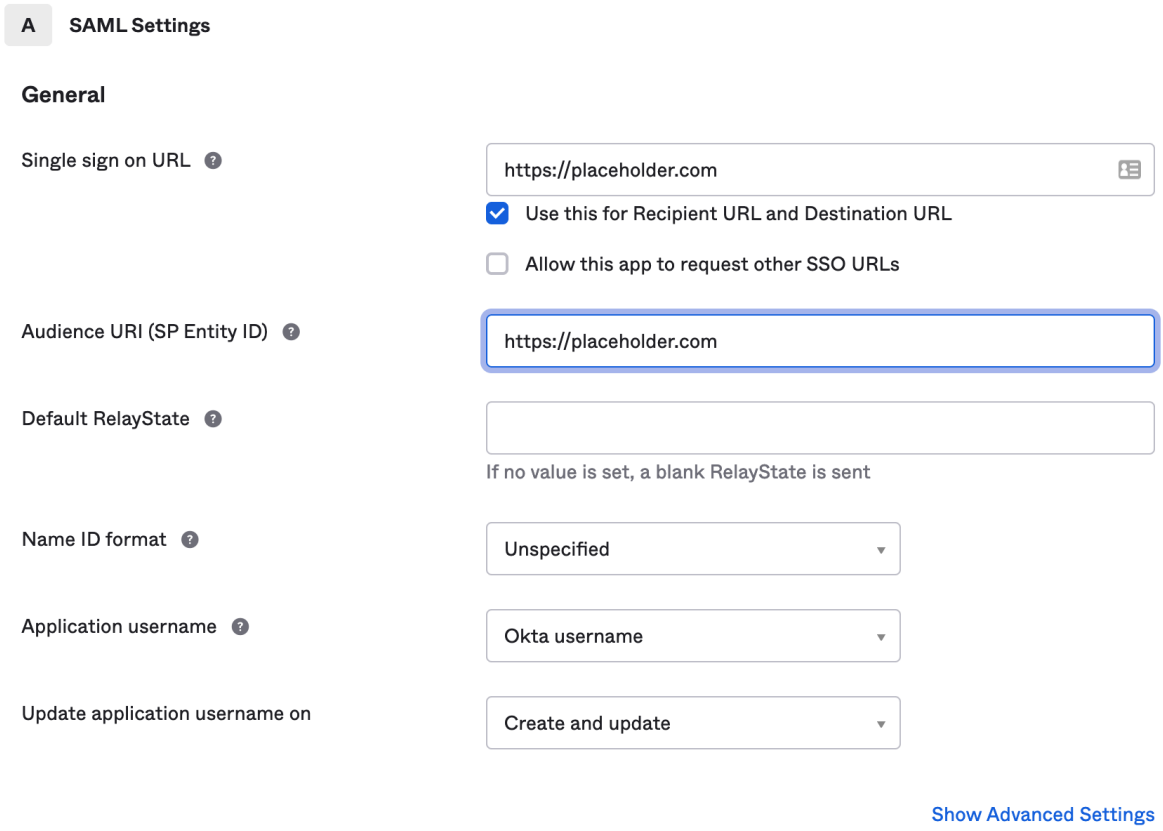
1. Go to the **Okta Admin dashboard** > **Applications** > **Applications** > **Create App Integration**.



2. Click **Next**.
3. Enter **Salesforce SAML 2.0 AIW** as the App name. Click **Next**.

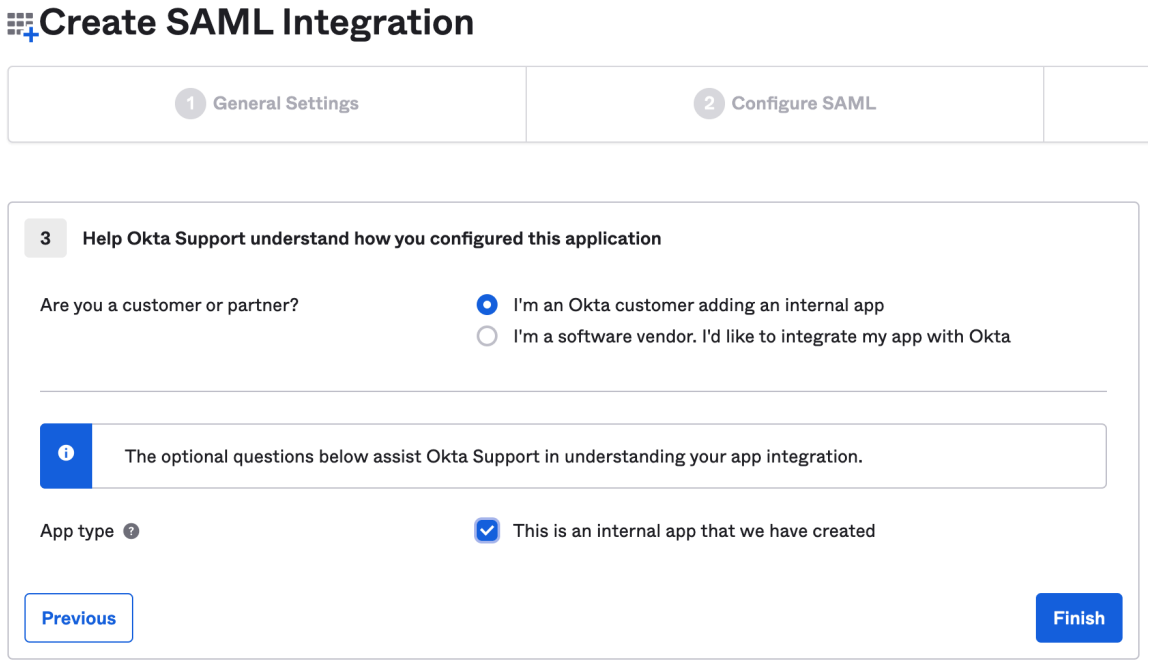


4. Add **https://placeholder.com** as the **Single sign on URL** and **Audience URI** (SP Entity ID).

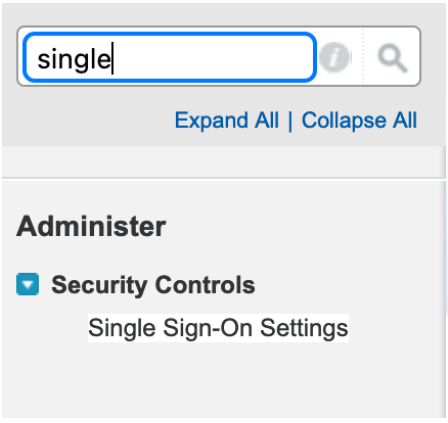


5. Leave the default values for the other fields and click **Next**.

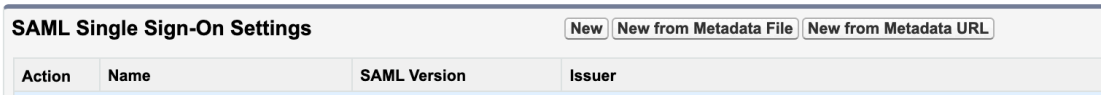
6. Select **I'm an Okta customer adding an internal app**. Check **This is an internal app that we have created**.



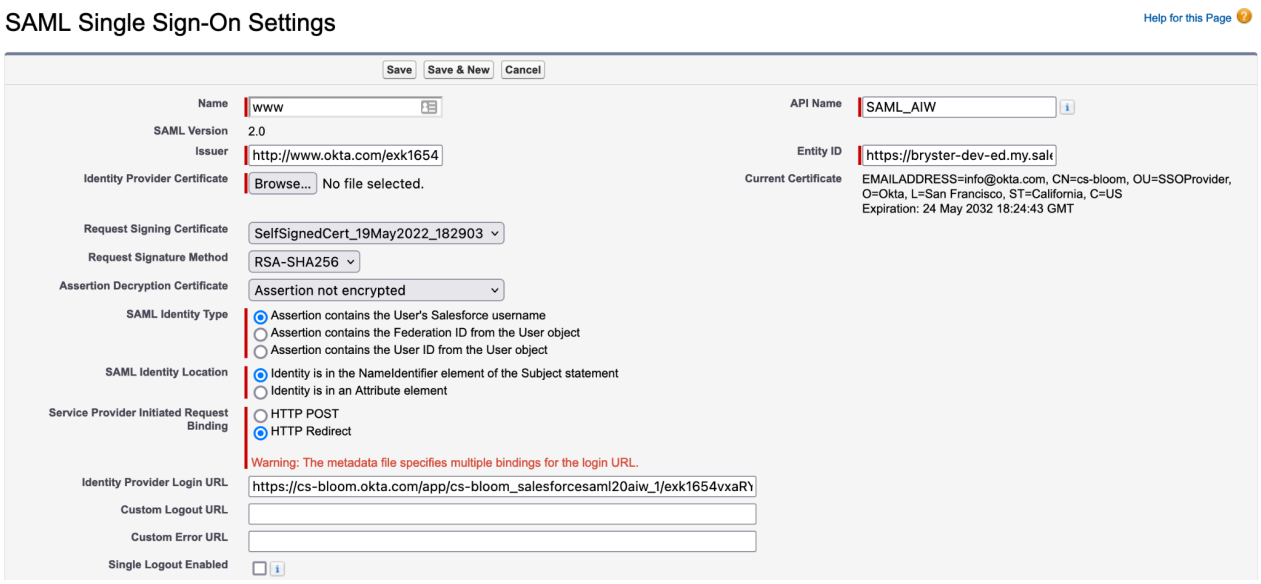
7. Click **Finish**.
8. On the **Sign On** tab, scroll to the middle section of the page, click on **View SAML setup instructions**. This will launch a new window.
9. Scroll towards the bottom of the page. Under Optional, select all on the metadata provided, paste it into a text editor and save it as metadata.xml.
10. Sign in to your existing Salesforce developer account as an administrator.
11. Navigate to **Single Sign-On Settings** from the Quickfind.



12. Under SAML Single Sign-On Settings, click **New from Metadata File**.

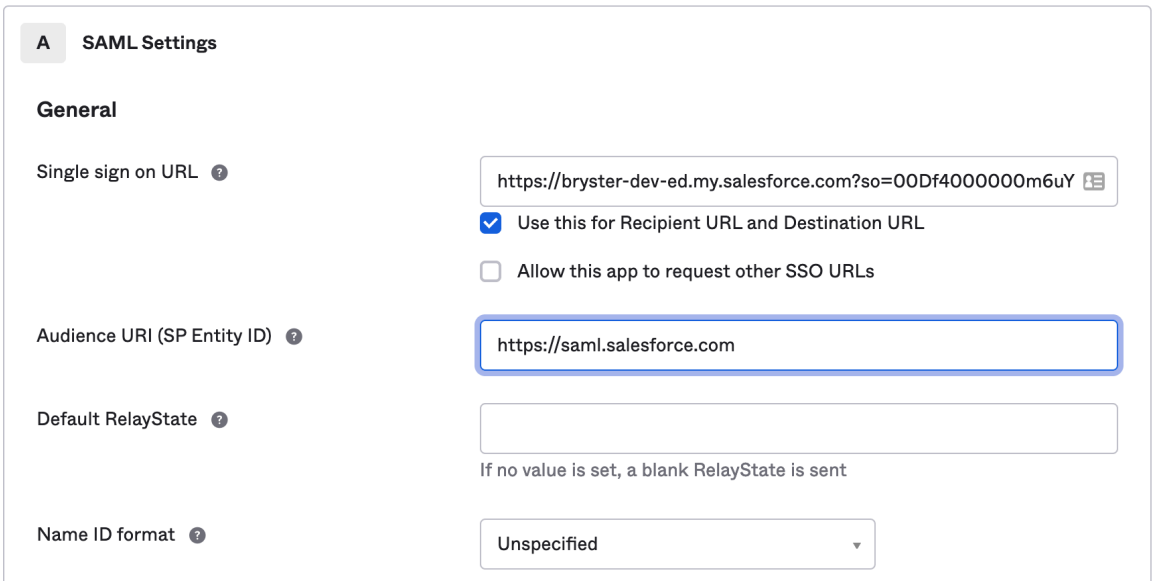


13. Choose the metadata file you saved earlier and click **Create**.
14. Add **SAML_AIW** as the Name and API Name and click **Save**.



15. We need the **Entity ID** and the Salesforce **Login URL** to update the SAML Settings in the Salesforce SAML 2.0 AIW app in Okta. Copy them.
16. Switch back to the **Salesforce SAML 2.0 AIW** app in Okta.
17. Go to the **General** settings.
18. Click **Edit** under SAML Settings.
19. Click **Next**.

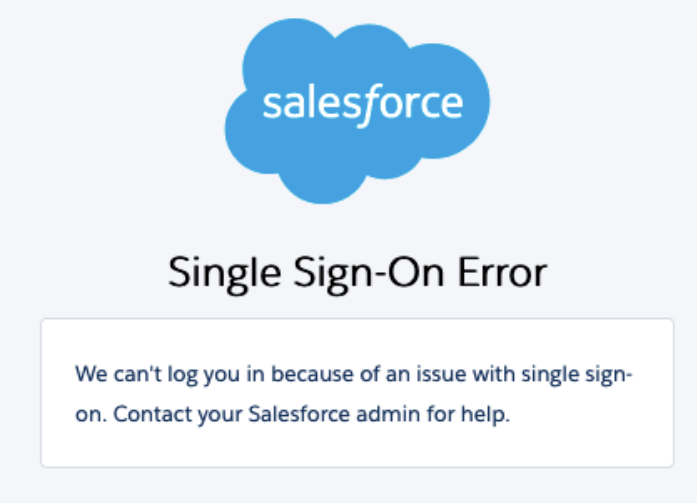
20. **Replace the placeholder** with the values from the Salesforce SAML profile.



21. Click **Next**.
22. Click **Finish**.
23. Go to the **Assignments** tab.
24. Assign the application to one of your existing Salesforce users.
25. **Edit** the username to match the Salesforce username.

26. Click **Save and Go Back**.
27. Click **Done**.
28. Log out of your Salesforce instances.
29. Switch to the Okta End-User dashboard (*the user assigned to the app in step 24*).
30. Click on the 'Salesforce SAML 2.0 AIW' app and should be successfully logged in. If you received this error, make sure the username assigned in Okta matches a

username in Salesforce.



31. Great work !!! You have configured a custom SAML integration with Salesforce.

BONUS LAB Exercises

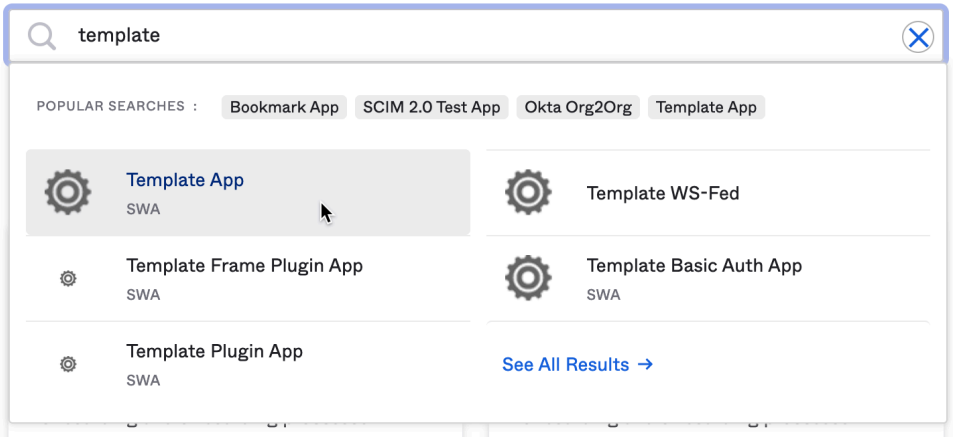
Lab 1-10: Configure Applications using the OIN Templates

Objective	To configure Applications using the OIN Templates
Procedures	• Configure a SWA application using the Template Plugin App 3 Fields – Ready Tech Admin
Duration	15-20 minutes

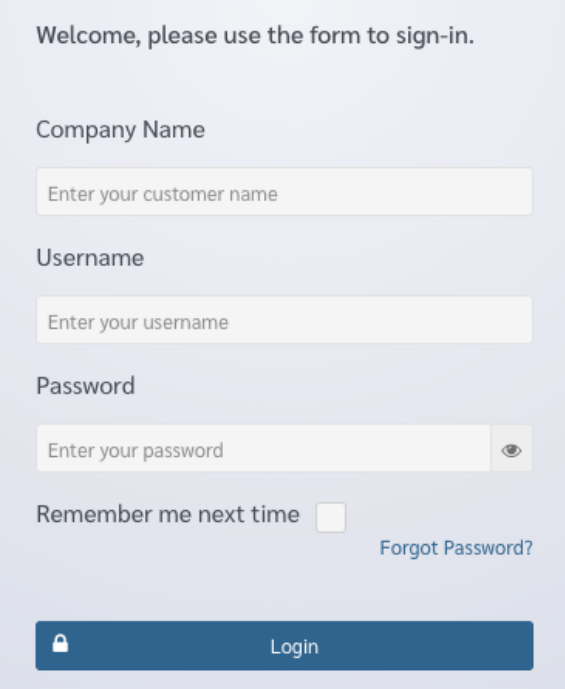
1.1 - Configure a SWA application using the Template Plugin App 3 Fields – Ready Tech Admin

1. Log in to your Okta Admin dashboard.
2. Navigate to **Applications** > **Applications** > **Browse App Catalog.**

3. Type **template plugin** in the **Search for an application** field. Select *Template App*.

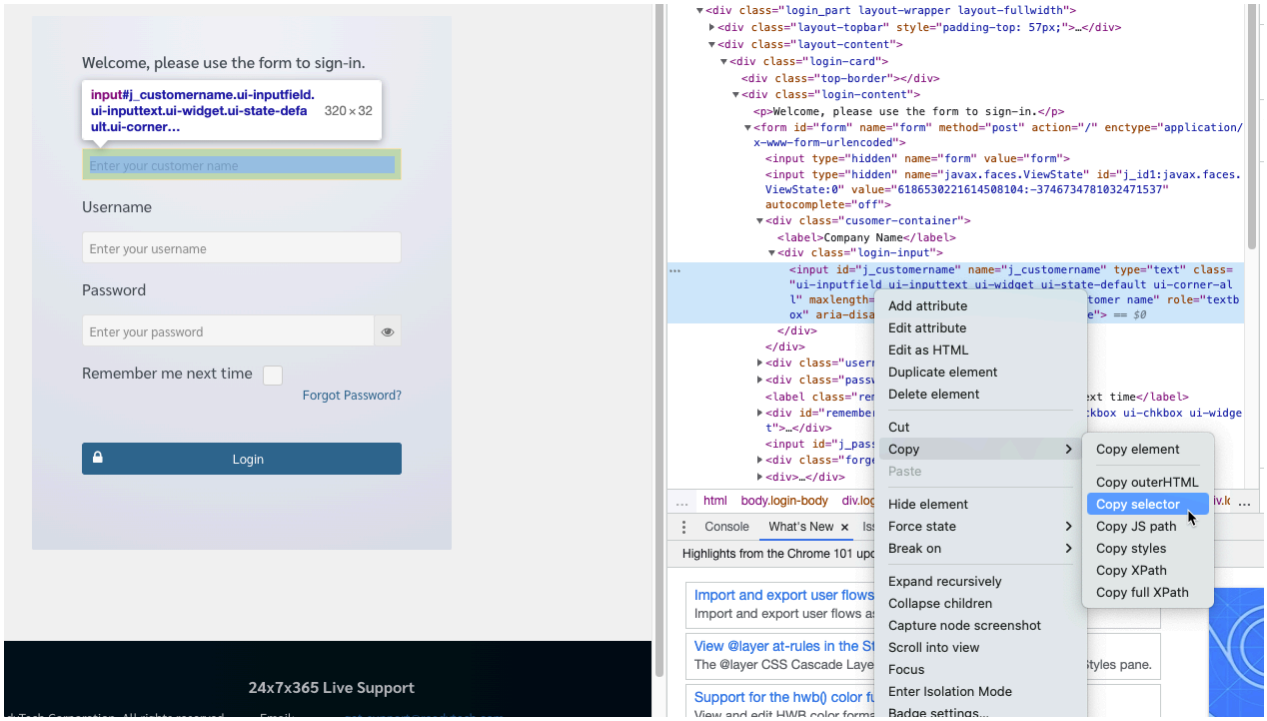


4. Click **Add Integration**.
5. Enter **ReadyTech Template Plugin App 3 Fields** as Application Label.
6. We need to define the parameter values for the Username, Password and Login button.
7. Go to the URL: https://admin.readytech.com/ in your browser



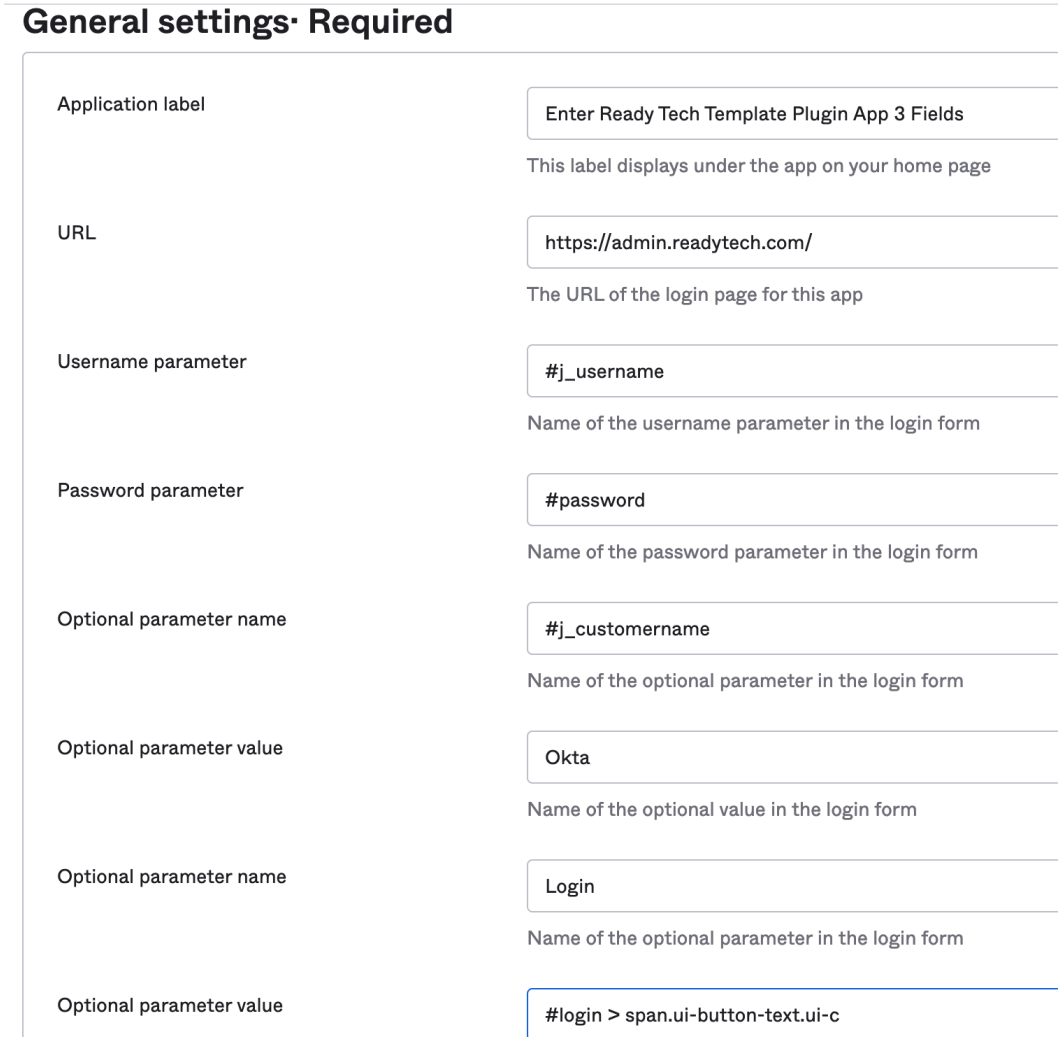
8. Right click the Company Name field and click **Inspect**.

9. Right click the highlighted text and **Copy selector.**



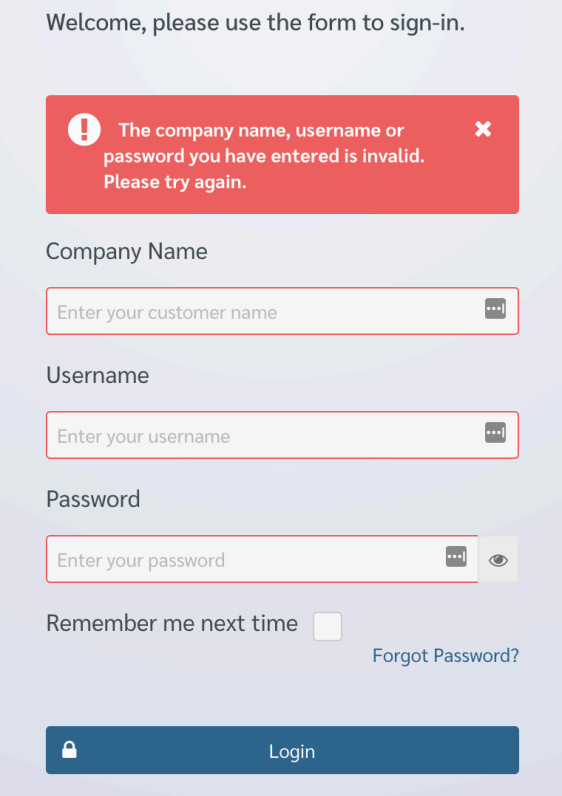
10. Repeat the steps to capture the CSS selectors for the **username**, **password** and **login** button fields.
11. Add **OKTA** as the value for the Extra Field (e.g. the name of your company).

12. You should now have the following configuration:



13. Click **Next**.
14. In the Sign-On Options, leave **Secure Web Authentication** selected.
15. Click **Done**.
16. Assign the application to your username. Click **Save and Go Back**.
17. Click **Done**.
18. For the purpose of this exercise, we do not require an actual account for the application. Our configuration is successful if the site returns an invalid credentials message.
19. Switch back to your **End-user dashboard**.
20. Click on the ‘Ready Tech Template Plugin App 3 Fields’ app. Enter random credentials and click Sign in to Ready Tech Template Plugin App 3 Fields.

21. Our configuration is successful even if we're missing a valid account to login with. The application authentication flow works.



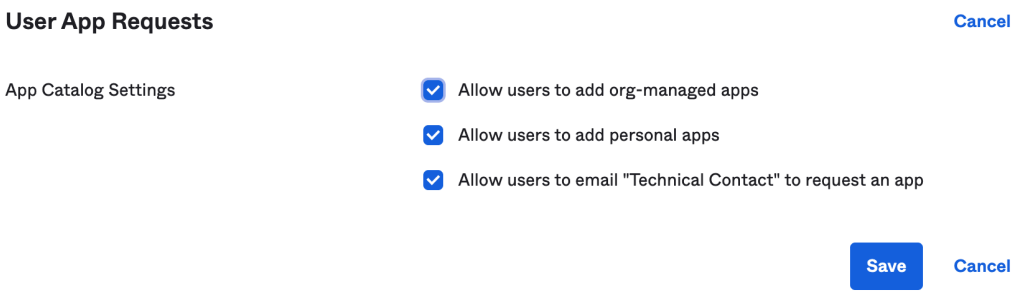
Lab 1-11: Configure the Application Approval Workflow.

Objective	To configure the Application Approval Workflow.
Procedures	• Configure Self-Service for Salesforce. • Submit and Approve Requests. • Review Application Access Reports
Duration	15-20 minutes

1.1 - Configure Self-Service for Salesforce

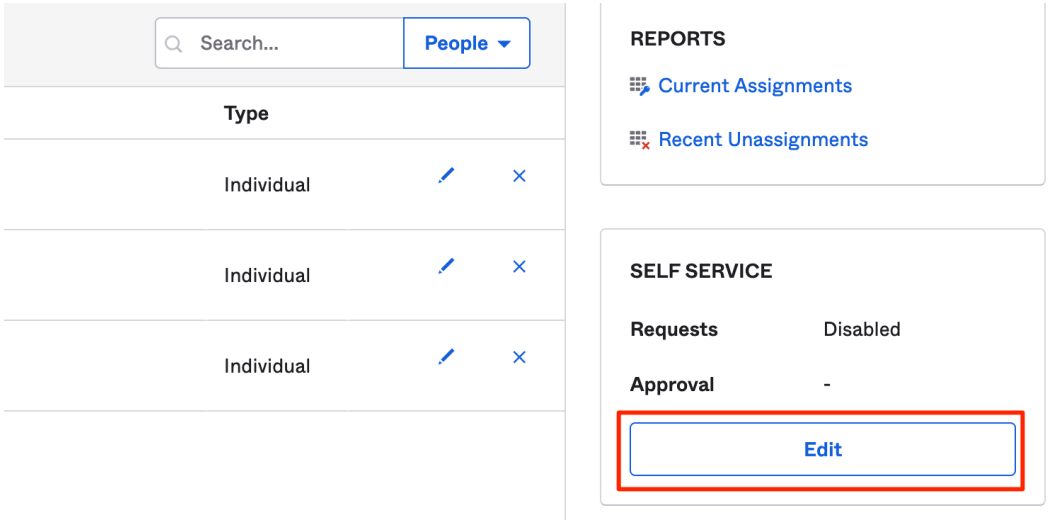
1. From your Okta Admin dashboard, navigate to **Directory** > **Groups**.
2. Create a group called **Approval Group**.

3. Add 3 users to the Approval Group.
4. Navigate to **Applications** > **Self-Service**.
5. Click **Edit** for User App Requests.
6. Check **Allow users to add org-managed apps**.



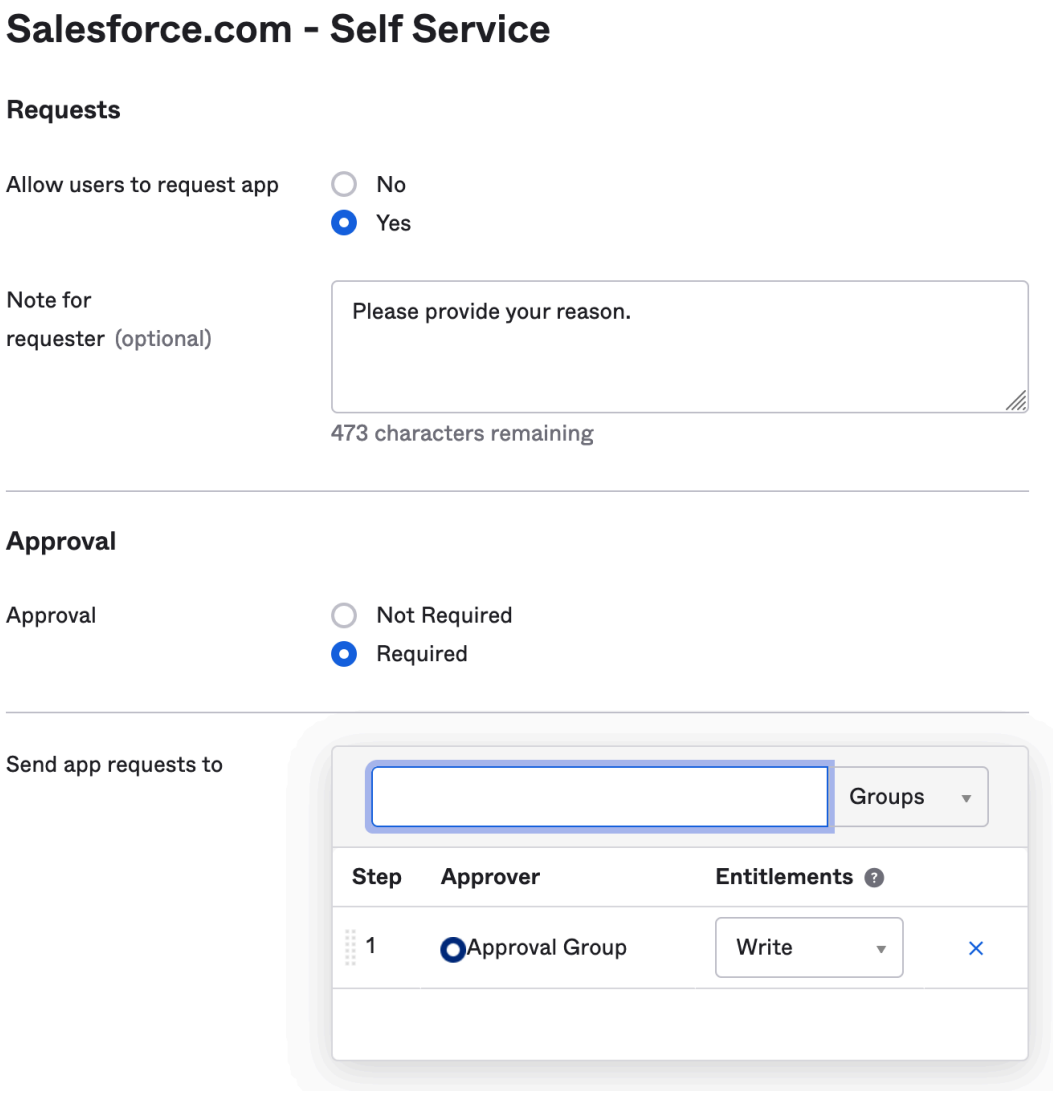
7. Click **Save**.
8. Navigate to **Applications**.

9. Select **Salesforce.com**
10. Go to the **Assignments** tab.
11. Click **Edit** under Self-Service.

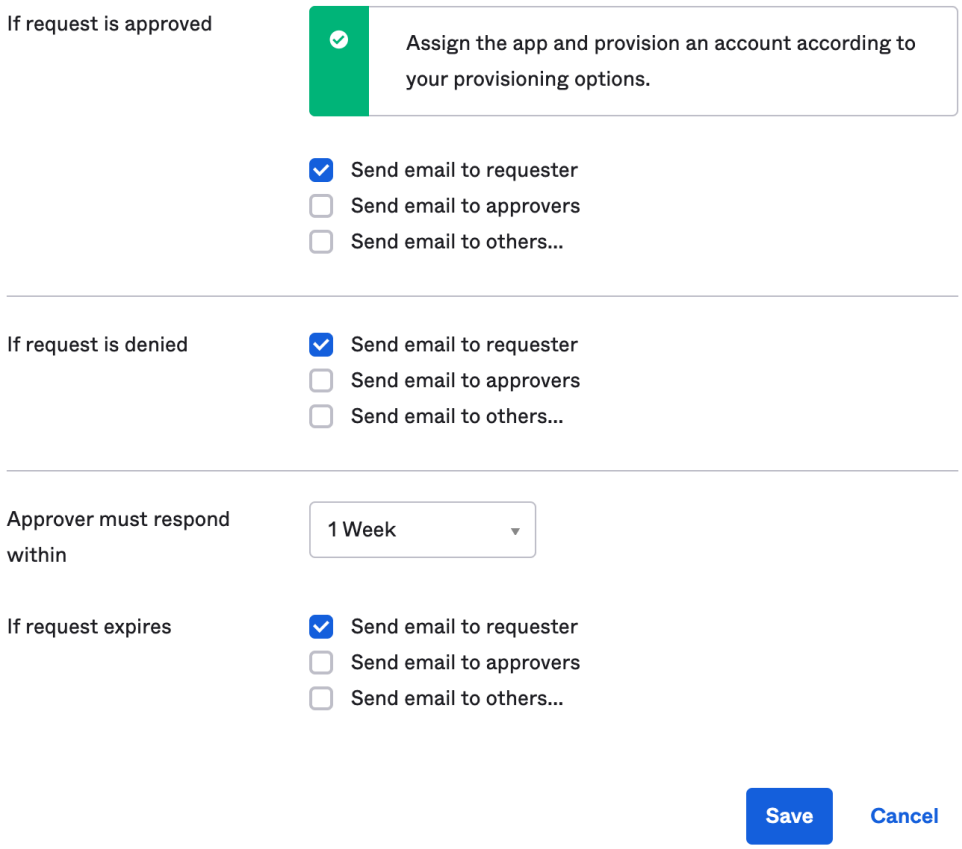


12. Select **Yes** to **Allow users to request app**.
13. Optional - Add a message to request details.
14. Select Approval **Required**.

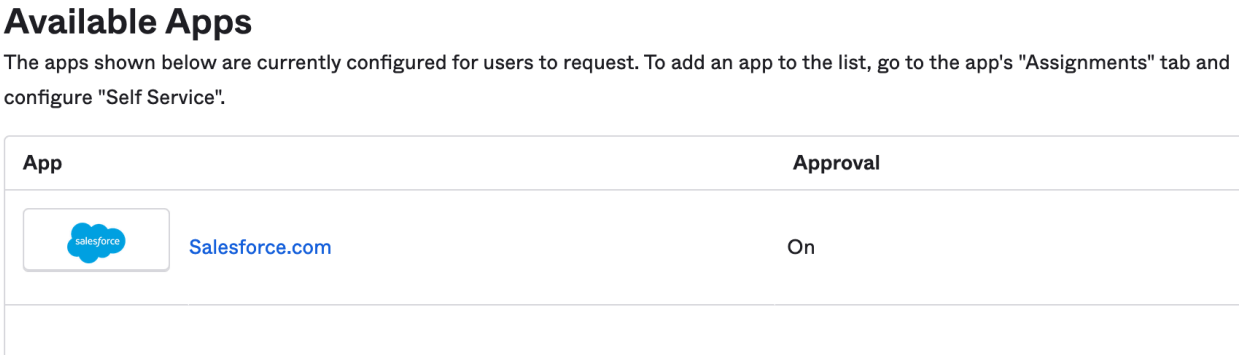
15. Send app requests to your **Approval Group** (**Write** permissions).



16. Review the available options for approvals and denials and click **Save**.

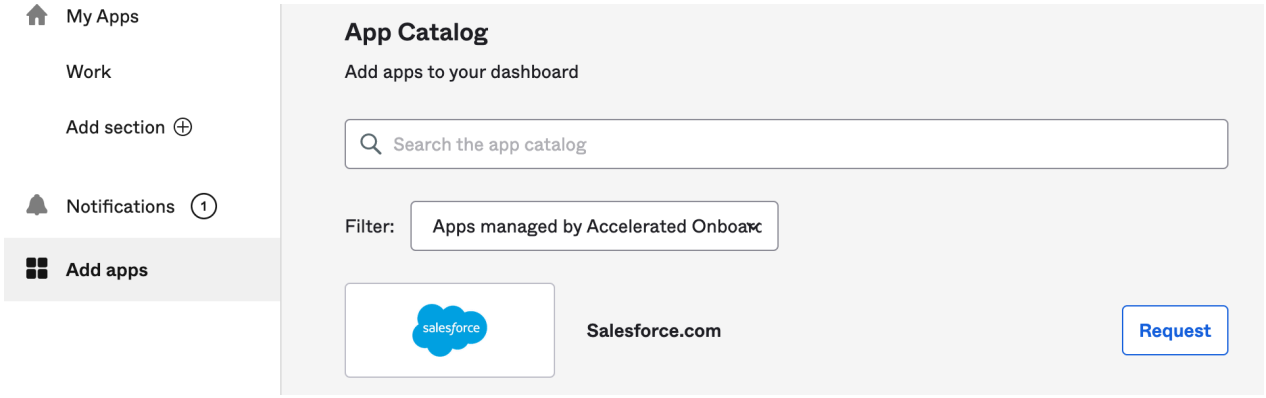


17. Navigate to **Applications** > **Self Service** and verify the Available Apps.

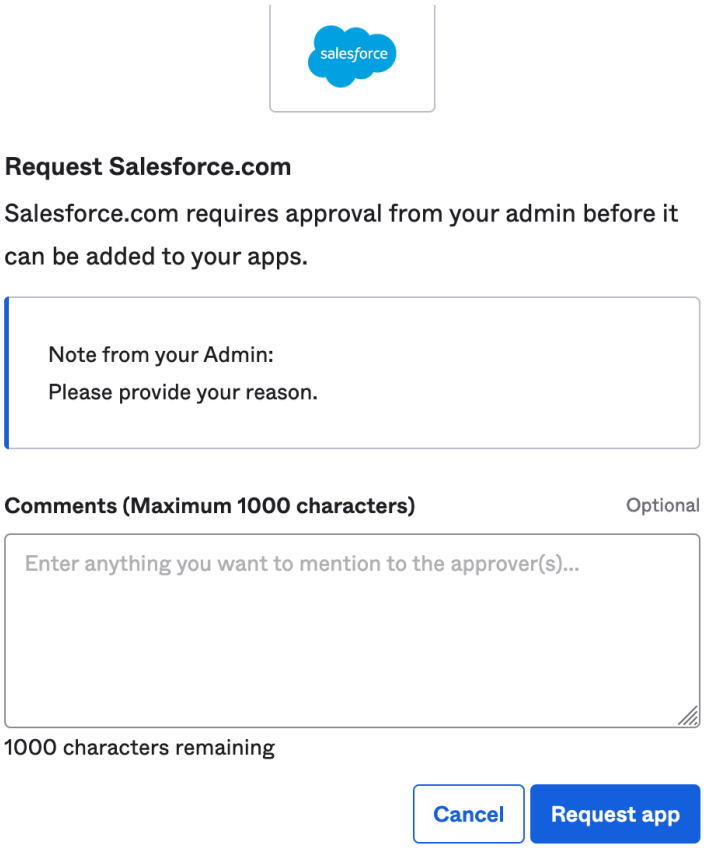


18. Log out of Okta session and log in with an end-user which hasn't been provisioned to Salesforce yet.

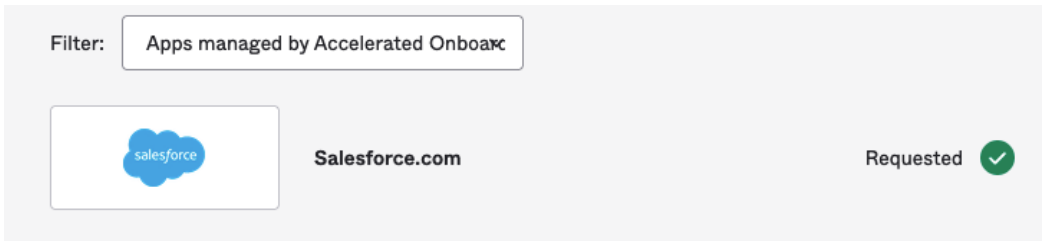
19. Click **Add Apps**.



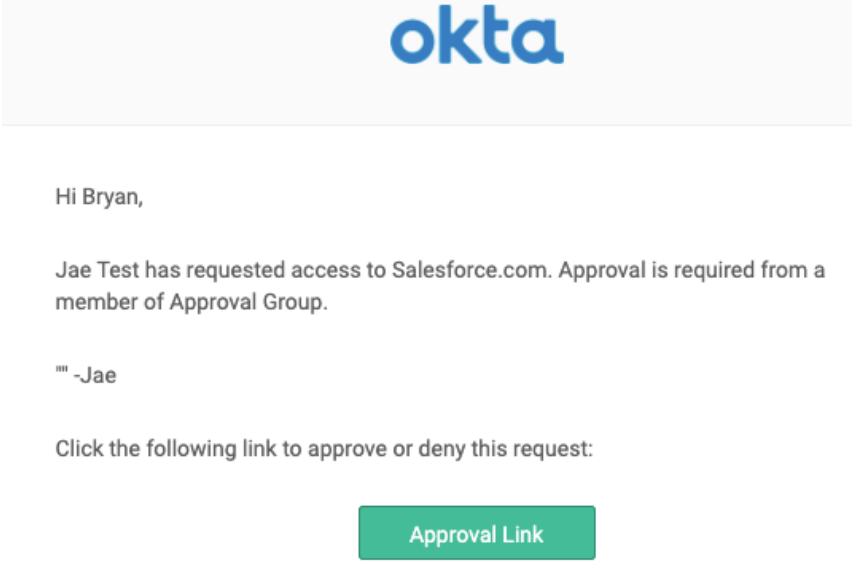
20. Click **Request**.
21. Provide the necessary details. Click **Request App**.



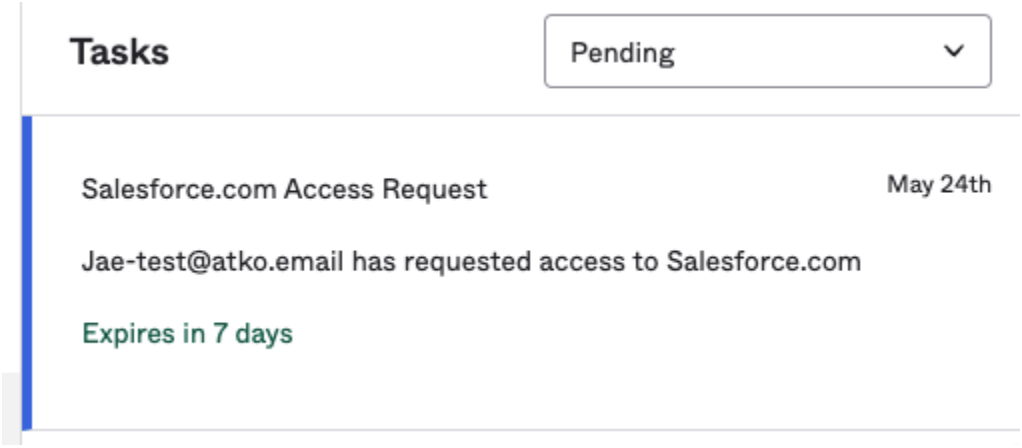
22. The application request has been sent.



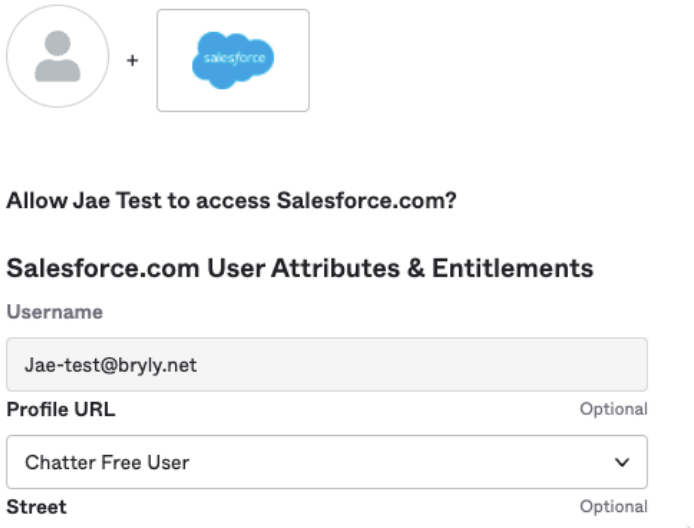
23. The approvers will receive an email notification. Open the message.
24. Click the **Approval Link**.



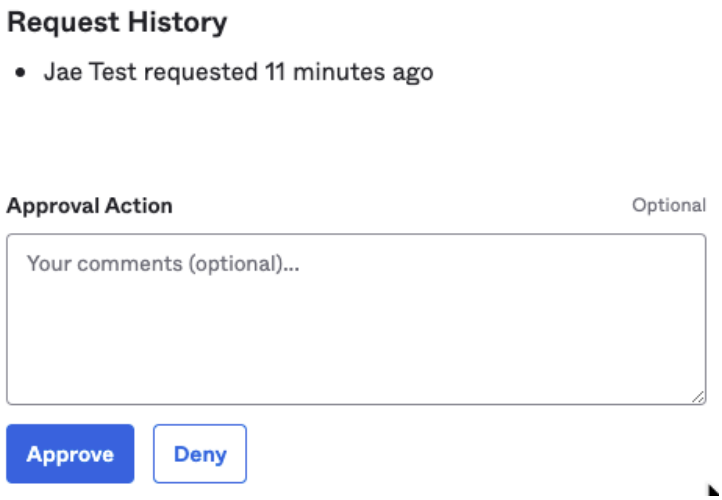
25. You will be redirected to the Tasks page and you will have one Pending **Salesforce.com Access Request**.



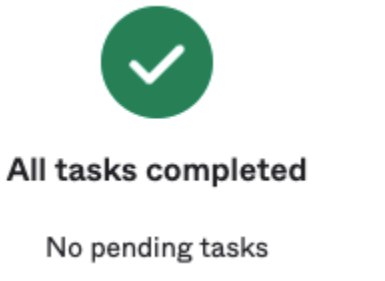
26. Under Salesforce.com User Attributes & Entitlements, select the dropdown under Profile URL and choose **Chatter Free User**.



27. (Optional) You can add a comment in the Approval Action section.
28. Click **Approve**.

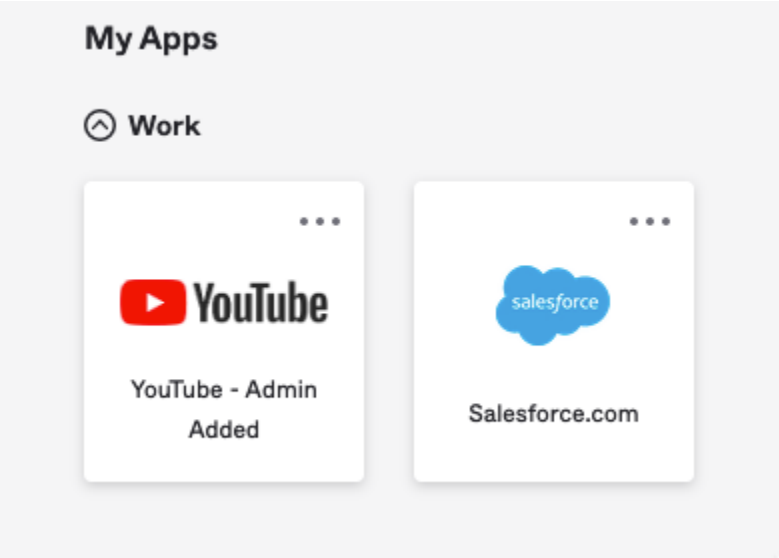


29. You will receive a task confirmation.



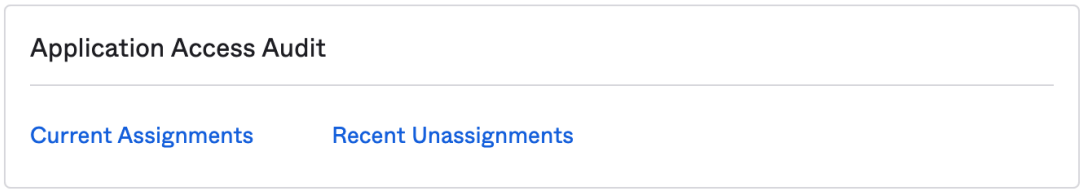
30. Navigate to your **Admin console** > **Applications** > **Applications> Salesforce.com** and verify the assignment of the user under the **Assignment** tab.

31. Log in to Okta as the requested end-user.
32. Verify if the user can see the Salesforce.com chiclet and if he can log in successfully.



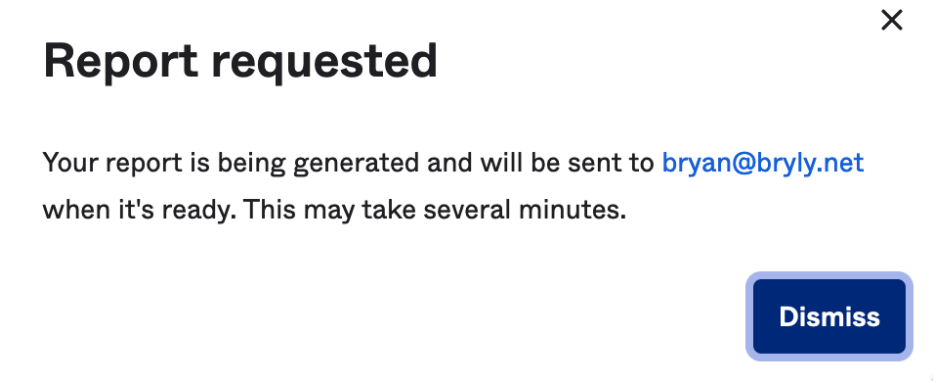
1.2 - Review Application Access Reports

1. Log in to **Okta Admin** dashboard.
2. Navigate to **Reports** > **Reports**.
3. Scroll down to the **Application Access Audit** section.

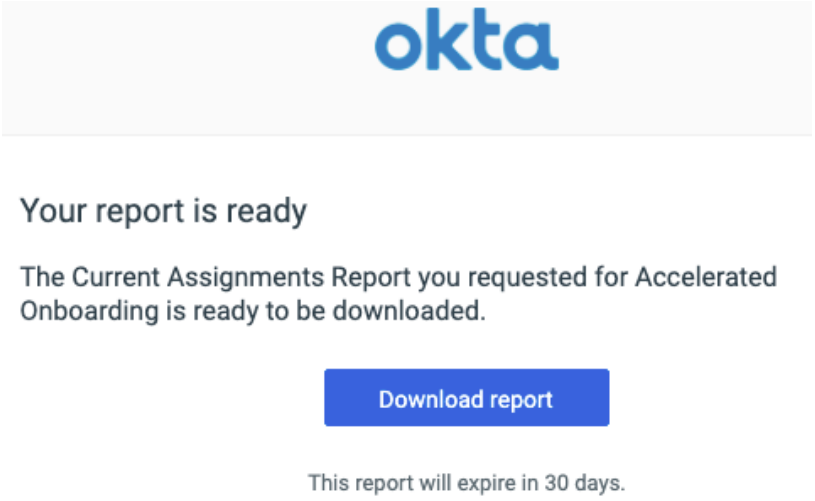


4. Click **Current Assignments**.
5. You can filter the report by Date Range, User, Application or Group. Enter **Salesforce.com** in the Application field.

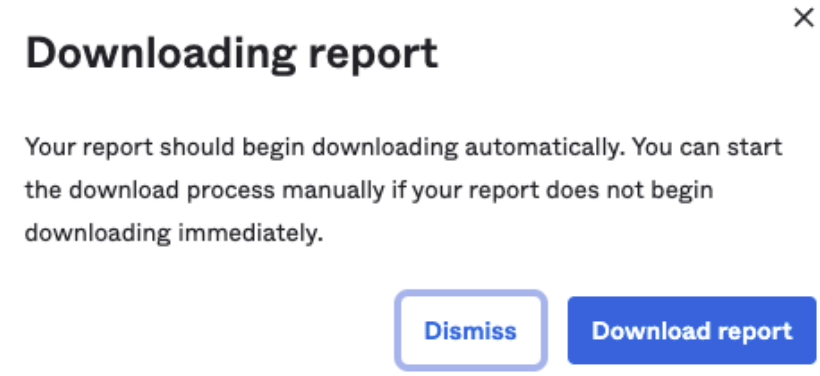
6. Click **Request Report**. You'll be presented with the below message:



7. Click **Dismiss**.
8. Check the email and you should you see the below email:



9. Click on Download Report and you will be provided with a **csv** file.



10. You can also list all applications assigned to a user.
11. Click **Request Report**.
12. Select **Recent Unassignments**.

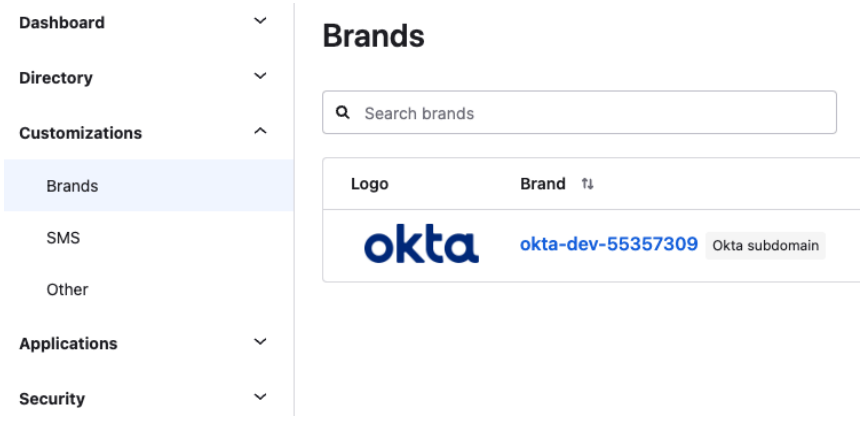
13. Add Salesforce.com as the Application.
14. Click **Run Report**. You should see users' unassignment status.

Lab 1-12: Personalize Your Okta Tenant

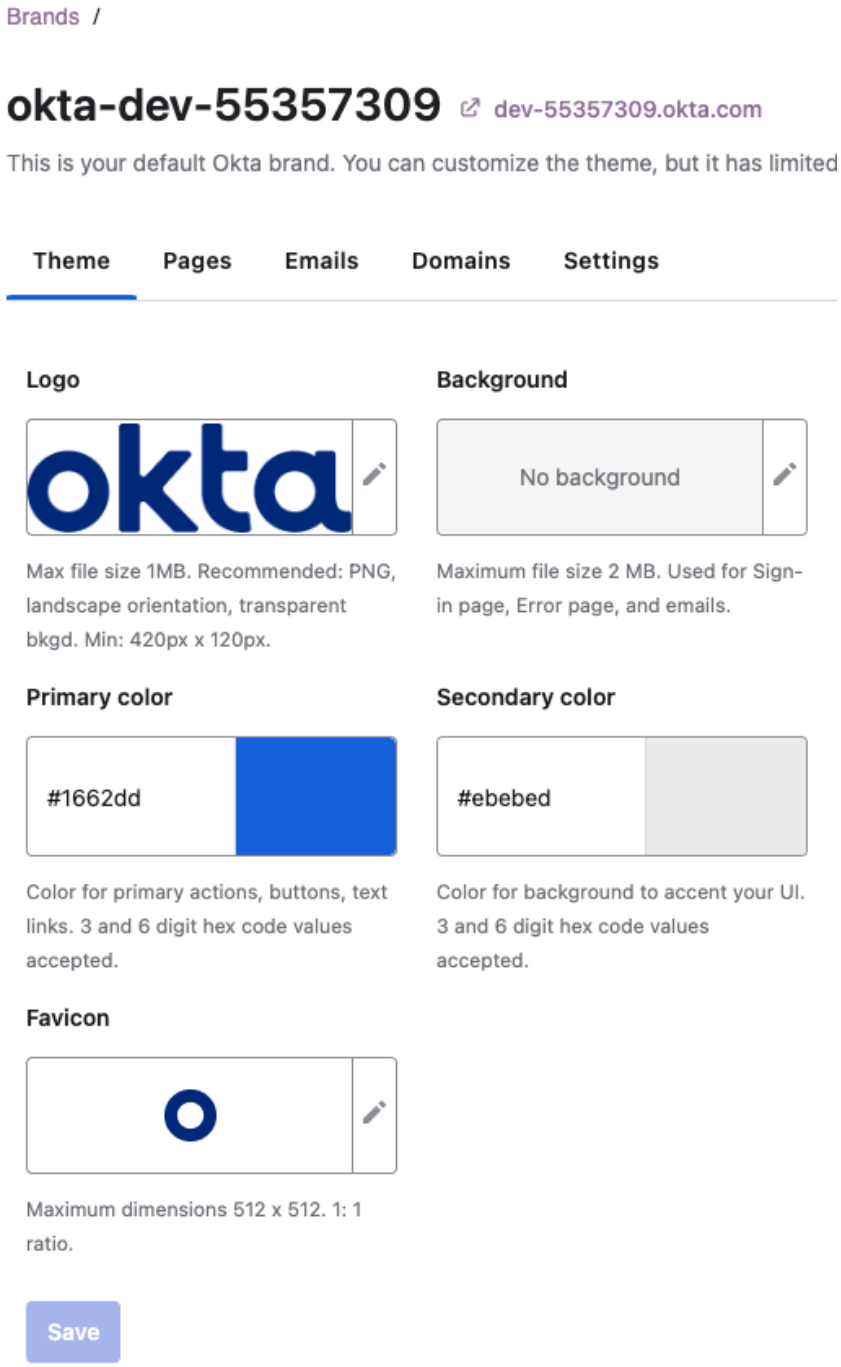
Objective	To personalize your Okta tenant
Procedures	• Change the Color, Logo and Background Image. • Customize the Sign-In Page. • Customize the User Activation Email.
Duration	15-30 minutes

1.1 - Change the Color, Logo and Background Image

1. Login to your **Okta Admin** dashboard.
2. Navigate to **Customizations** > **Brands**. Click on your subdomain.

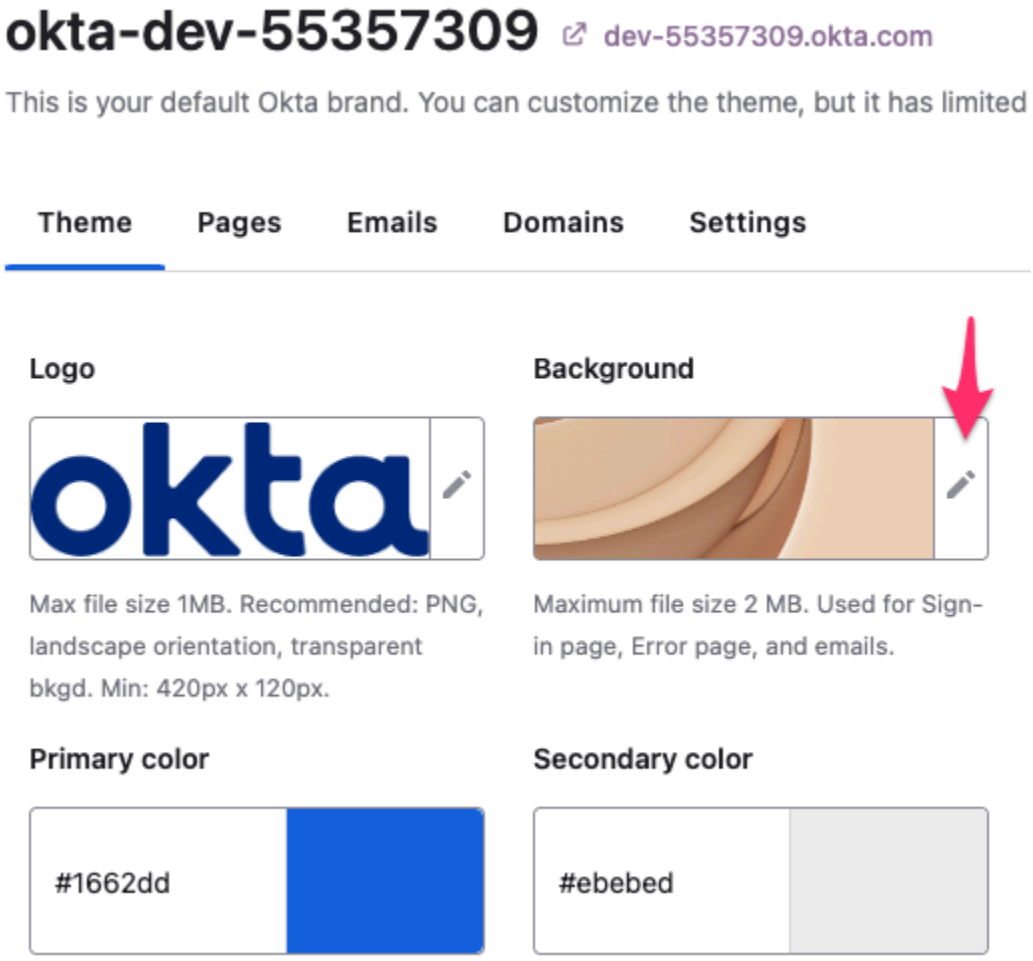


3. Change the primary color, secondary color, logo, favicon and background image to your liking.

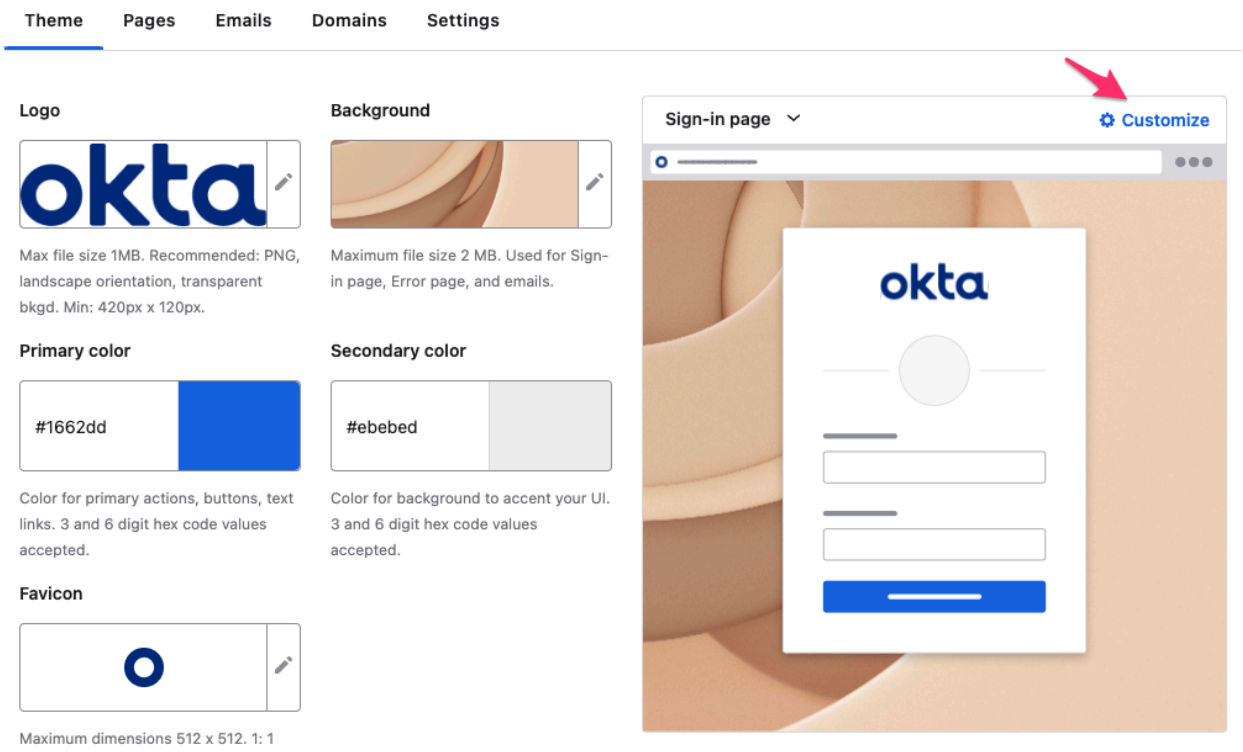


4. Click **Save**.
5. Click on **Edit** on the Okta-hosted Sign-In page section.

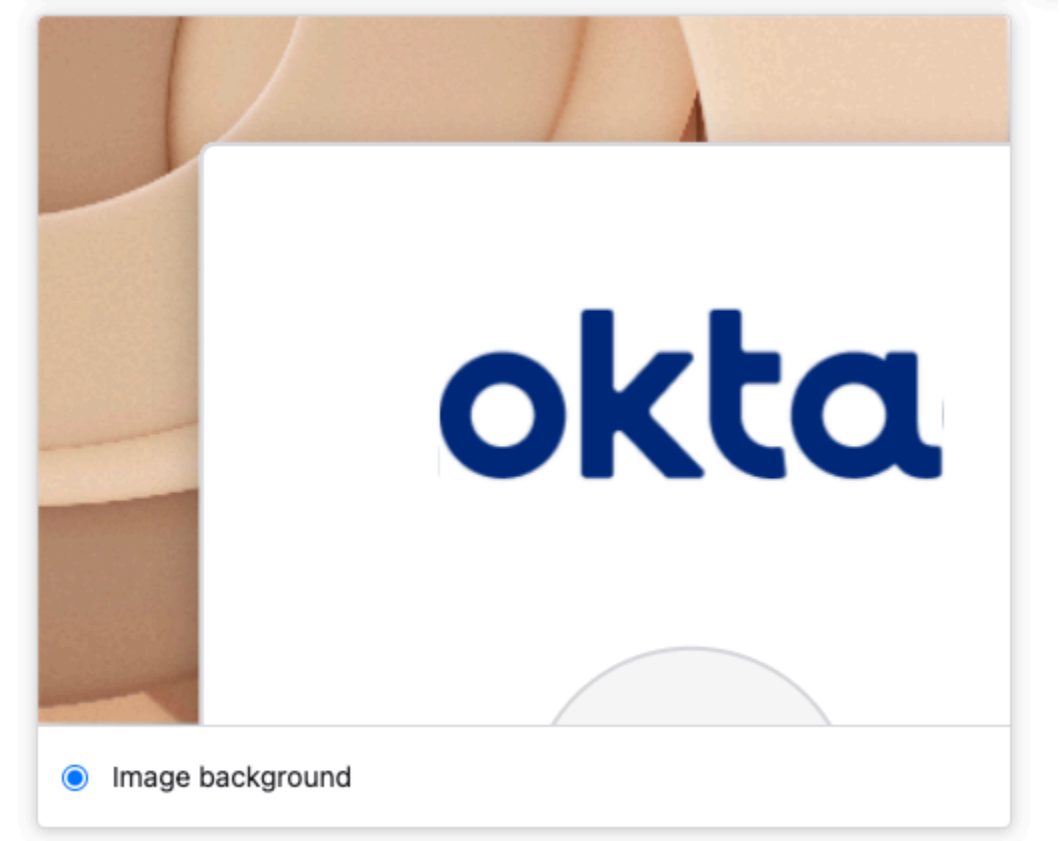
6. In the Theme tab, select the pencil icon to change the background image. Upload a file less than 2 mb. Click **Save**.



7. In the ‘sign-in page’ to the right, click on Customize



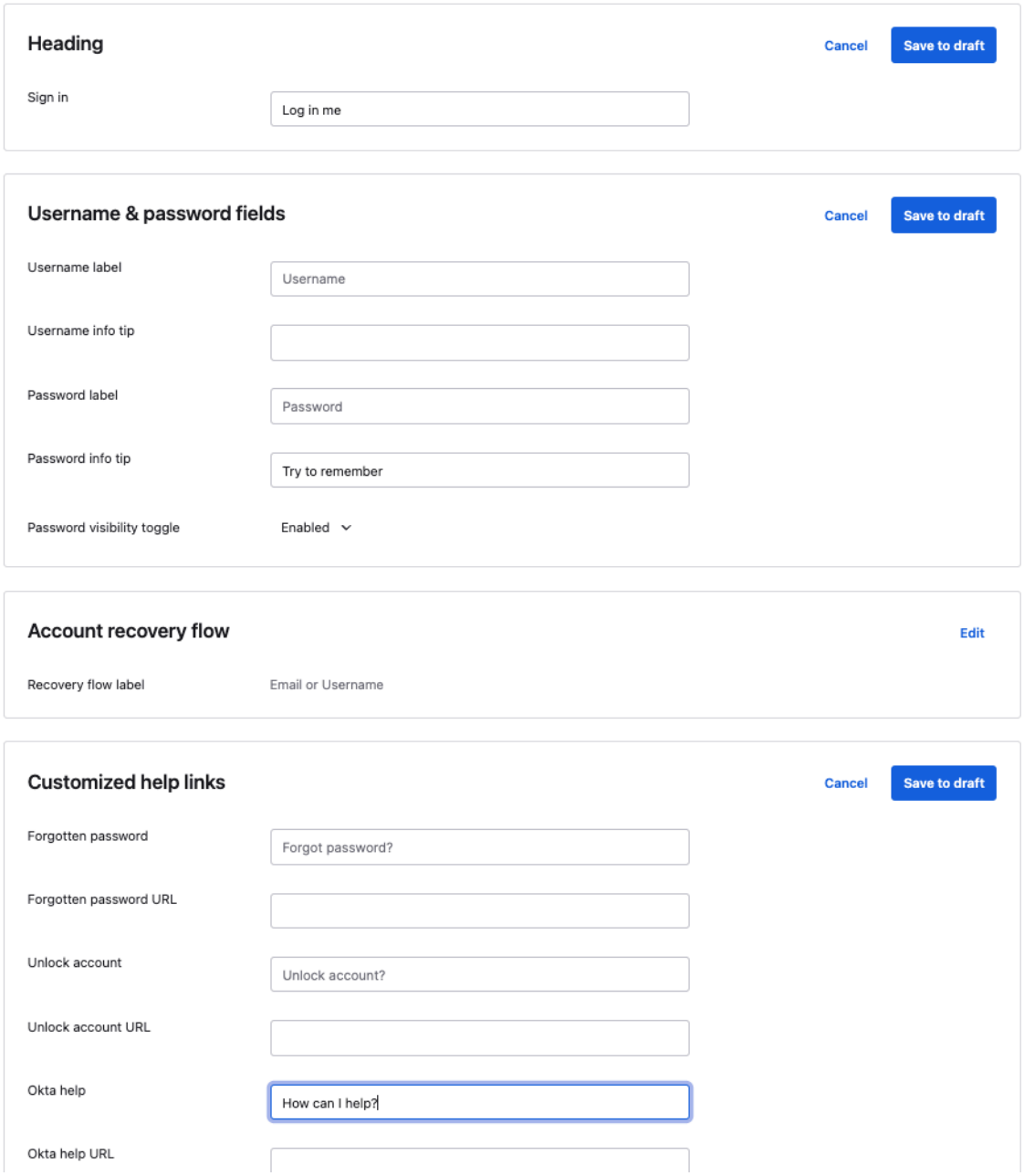
8. In the ‘Page Design’ tab, select ‘image background’ towards the bottom. Click **Save and Publish**.



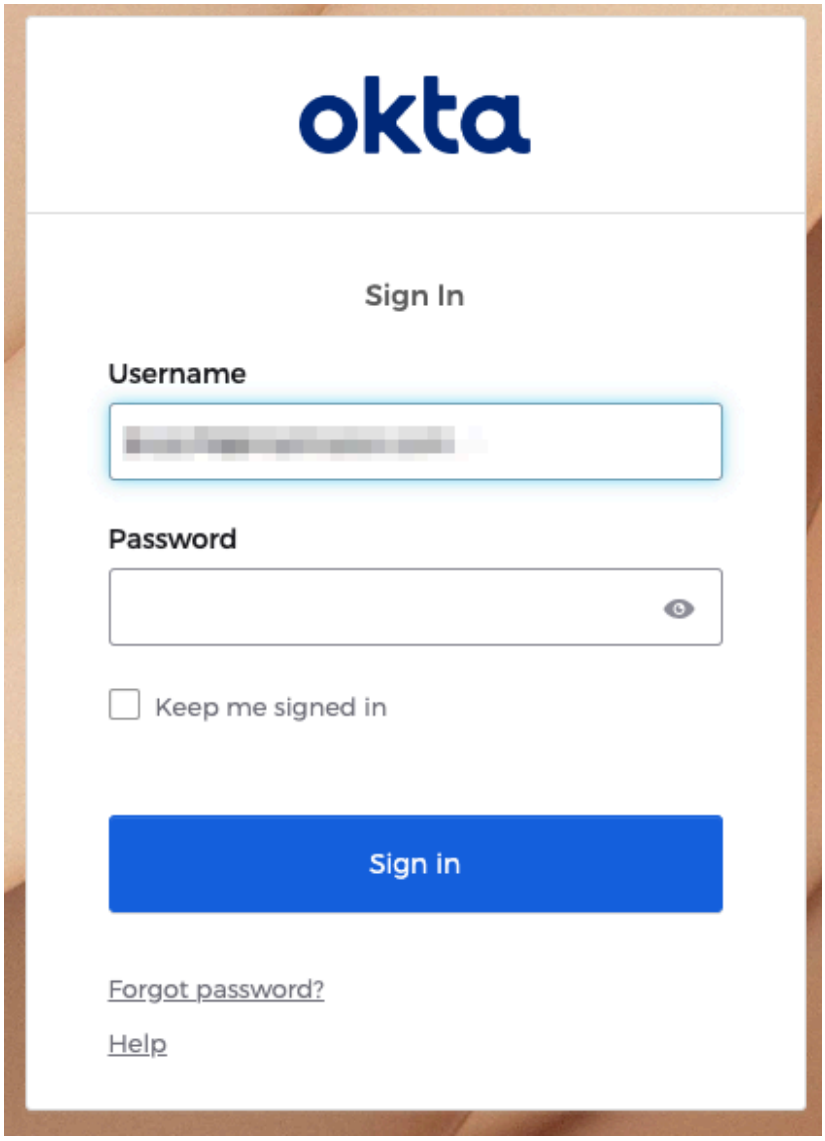
9. Log out and log in again. Notice the change.

1.2 - Customize the Sign-In Page

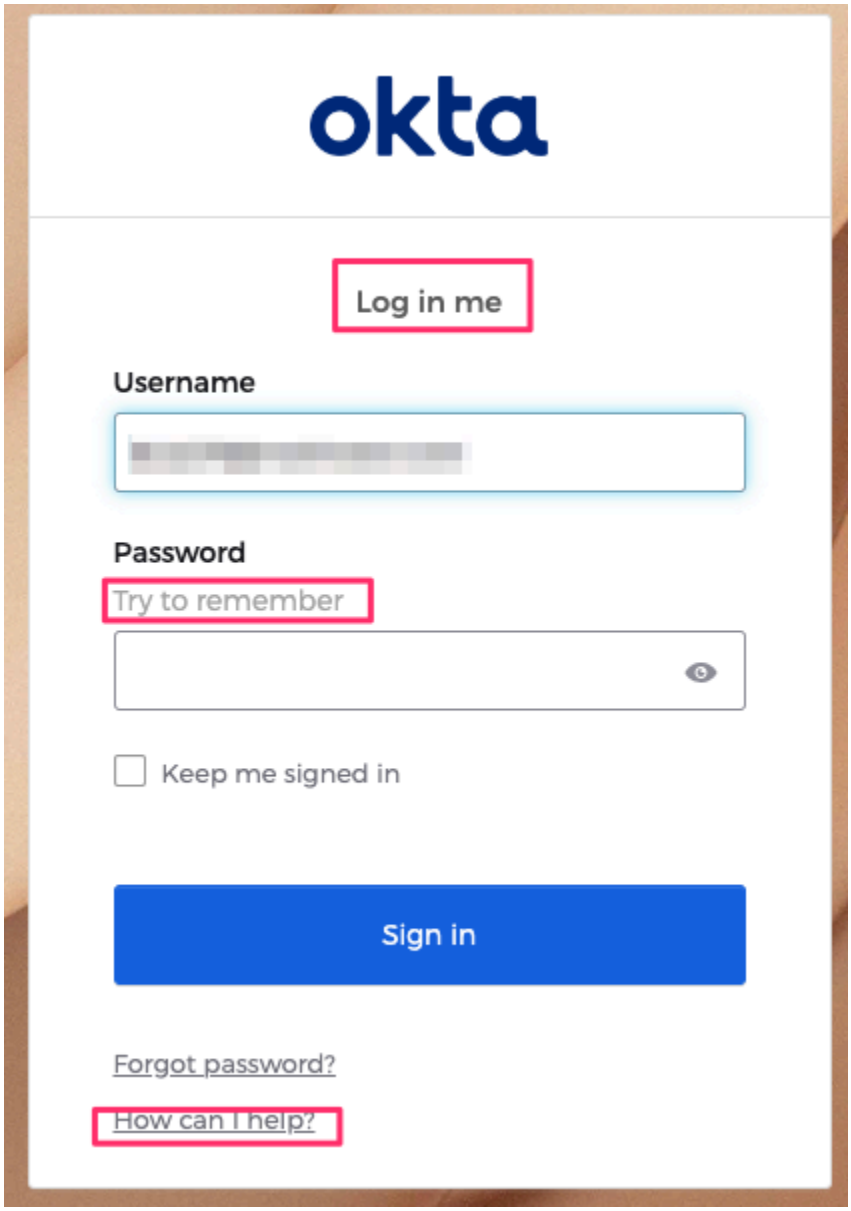
1. From your **Okta Admin** dashboard, navigate to **Customizations** > **Brands.**
2. Click on your subdomain.
3. In the 'sign-in page', click Customize. Then click on the 'Labels' tab.
4. Change the 'Sign In' heading, 'Password info tip' and 'Okta Help'.



5. Click **Save to draft** to all 3. Click **Publish**.
6. Sign out of Okta and confirm the updates.
   Before:


okta
Sign In
Username
Password
Keep me signed in
Sign in
Forgot password?
Help

After:



7. Log back into your **Okta Admin** dashboard, navigate to **Customizations** > **Brands.**
8. Click on your subdomain.
9. In the ‘sign-in page’, click Customize. Then click on the ‘Labels’ tab.
10. Click **Edit** in the ‘Sign In’ heading, ‘Password info tip’ and ‘Okta Help’
11. Put back in original values. Click **Save to Draft** and **Publish** the changes.
12. Confirm the changes by logging out and logging in again.

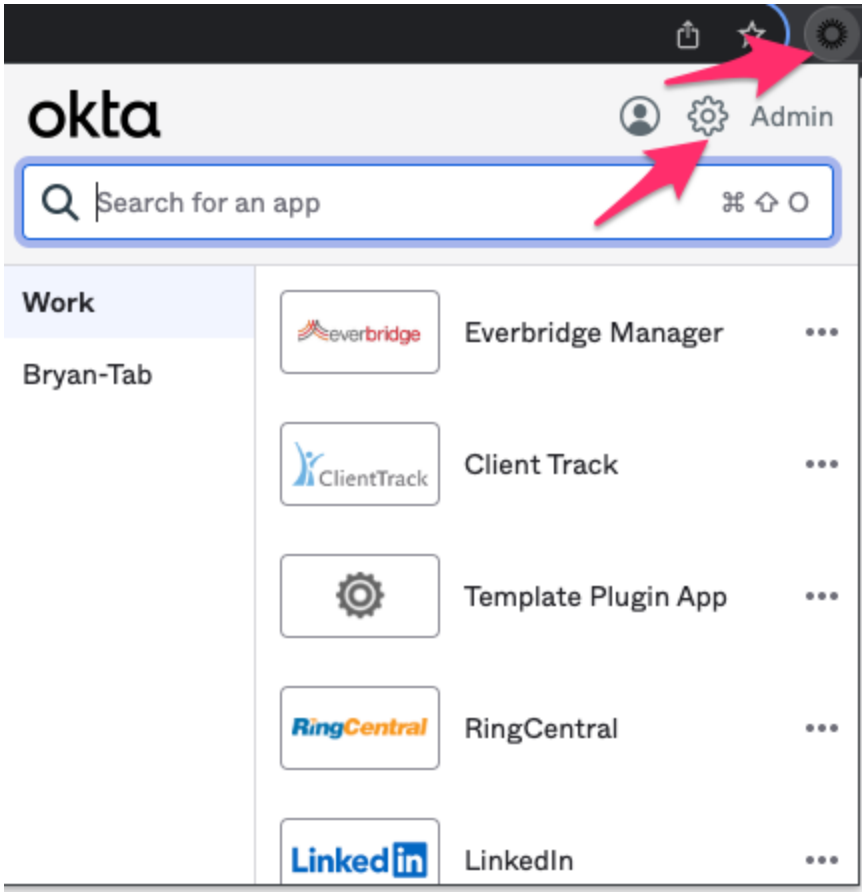
Lab 1-13: Configure the Okta Browser Plugin

Objective	To configure the Okta Browser plugin
Procedures	• Configure the Okta Browser Plugin (End-User settings). • Configure the Okta Browser Plugin (Admin settings). • Switch between multiple Okta accounts using the Plugin.
Duration	15-20 minutes

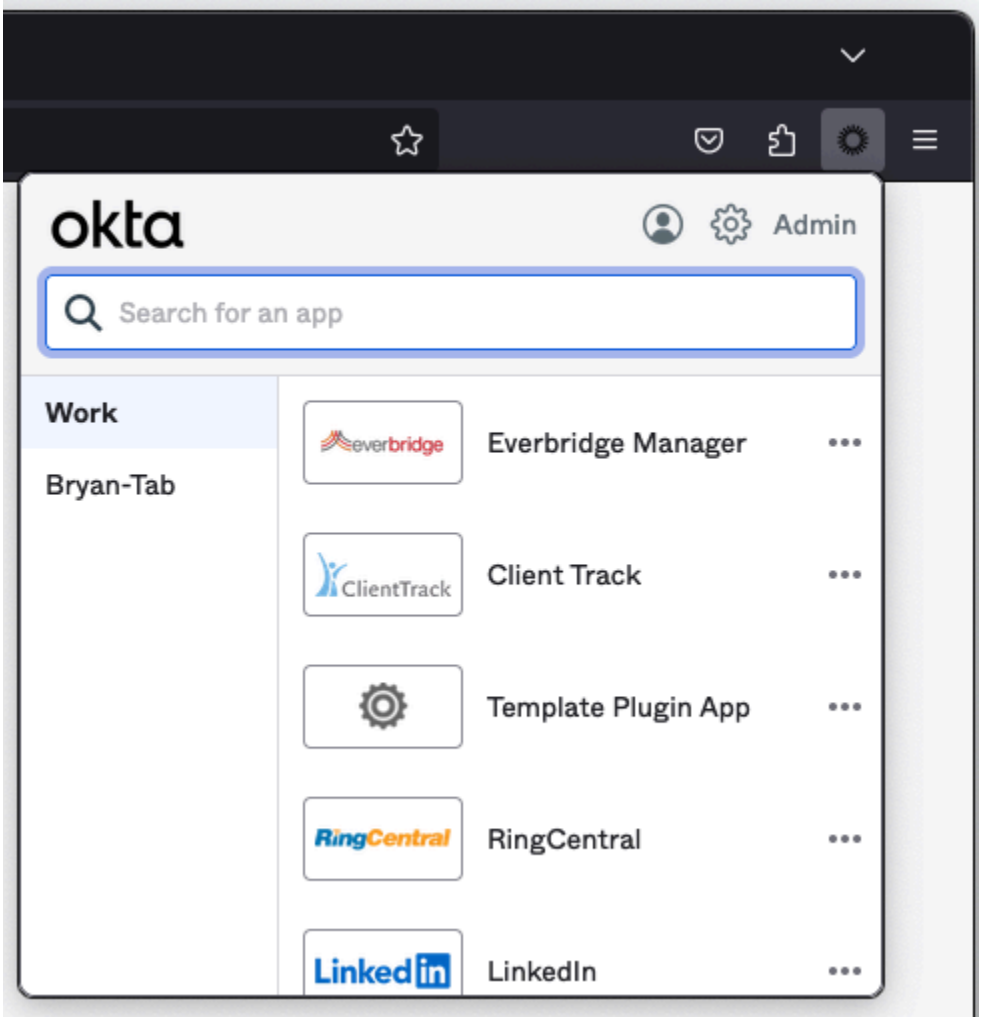
1.1 - Configure the Okta Browser Plugin (End-User settings)

The Okta Browser Plugin enables you to automatically sign into applications that would otherwise require you to manually enter your credentials (e.g., applications that do not support SAML or a direct form POST to a URL). Using the plugin enables you to use SSO for a broader range of applications.

1. To configure the Okta browser plugin, click on the blue O icon and the gear icon in the plugin.
   Chrome:

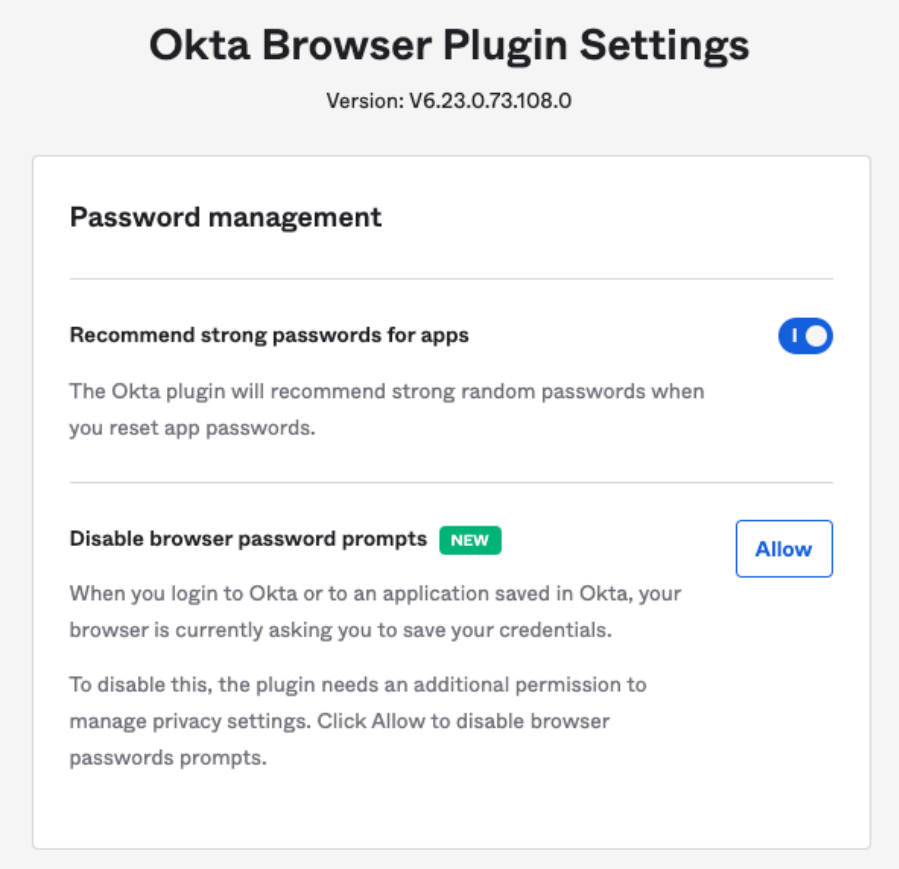

okta
Admin
Search for an app
⌘ ⇧ O
Work
Bryan-Tab
everbridge
Everbridge Manager
ClientTrack
Client Track
Template Plugin App
RingCentral
RingCentral
LinkedIn
LinkedIn

Firefox:

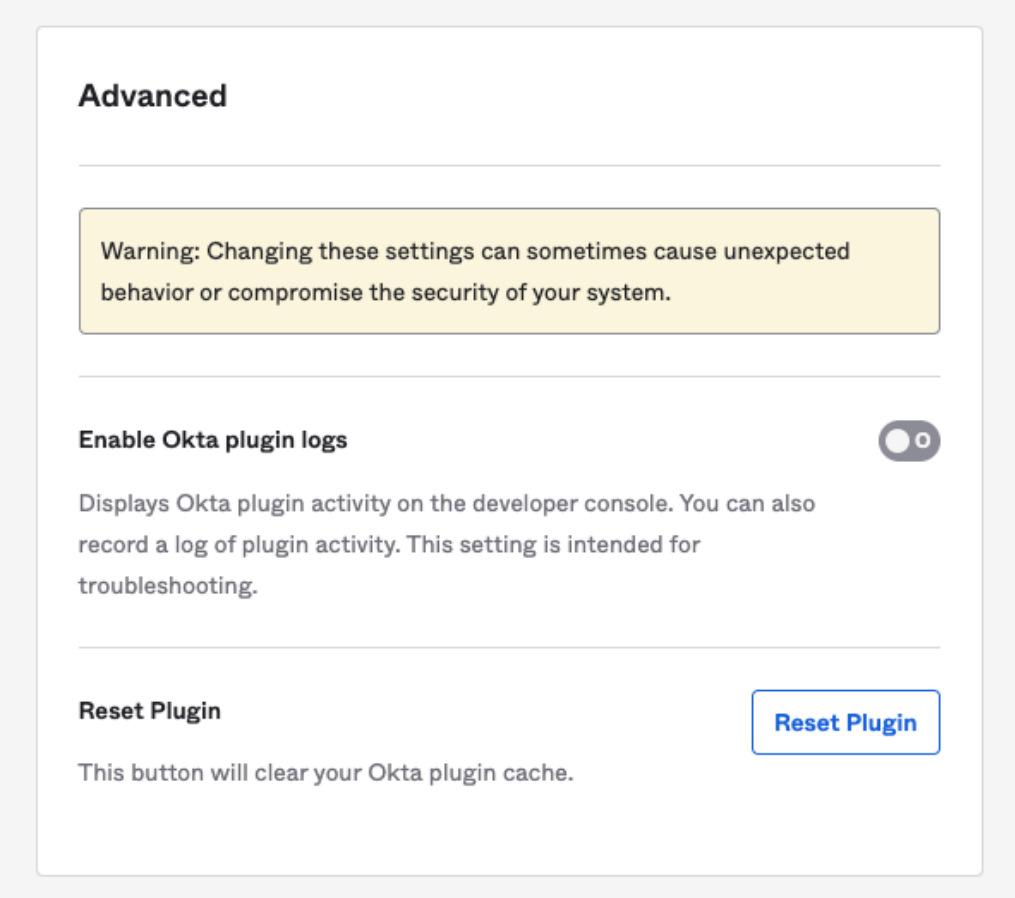


2. This will launch a new browser tab. If you don't want the Okta Browser plugin to recommend secure passwords or to prompt you to save apps to your dashboard,

untoggle the options.



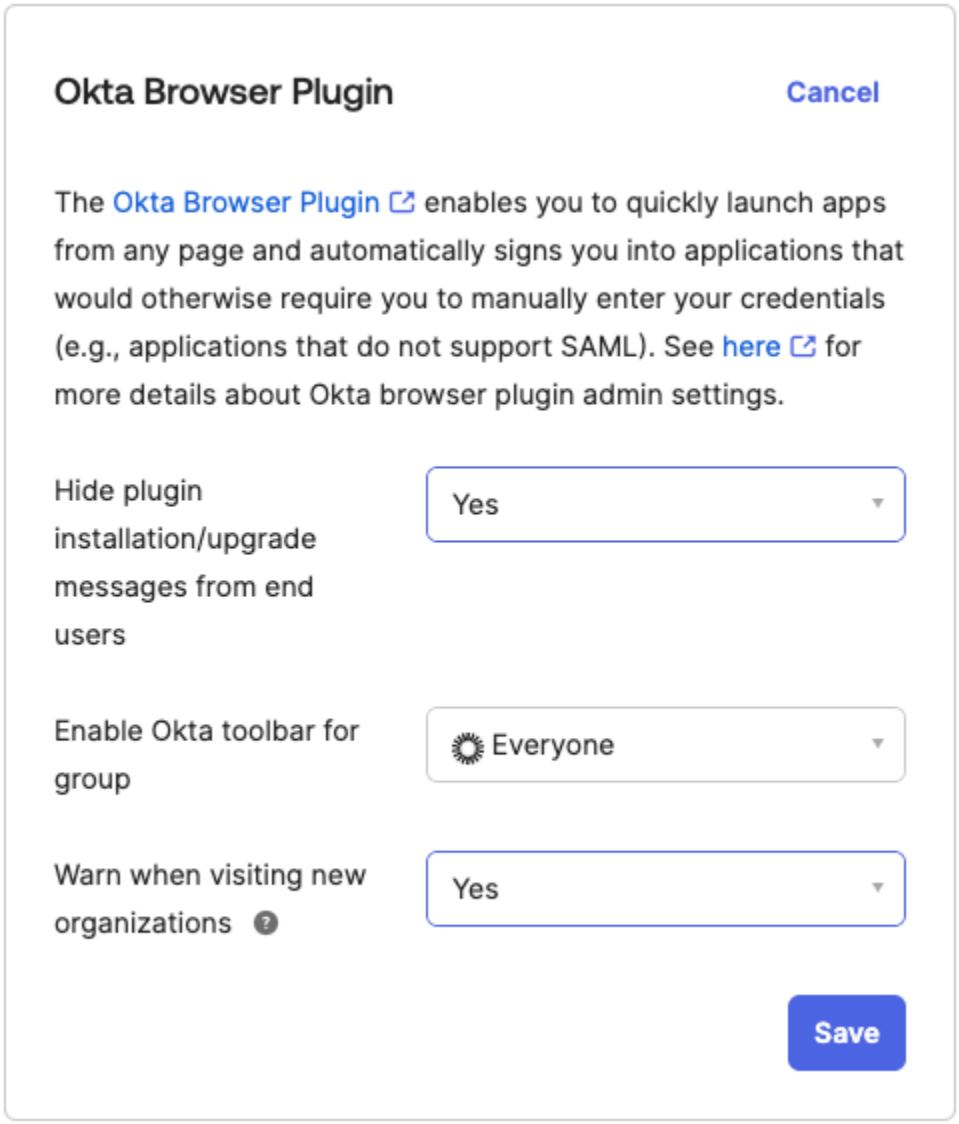
3. Scroll further down and click **Reset Plugin** to refresh the Okta browser plugin cache.



1.2 - Configure the Okta Browser Plugin (Admin settings)

1. Login to your **Okta Admin** dashboard.
2. Navigate to **Customization** > **Other** > scroll to the Okta Browser Plugin section.
3. Click **Edit**.
4. Selecting **Yes** for 'Hide plugin installation/upgrade messages from end users' will hide messages related to installation or upgrade of the plugin.

5. If you want your users to receive a warning message when attempting to login to a different org, select Yes for **Warn when visiting new organizations**.

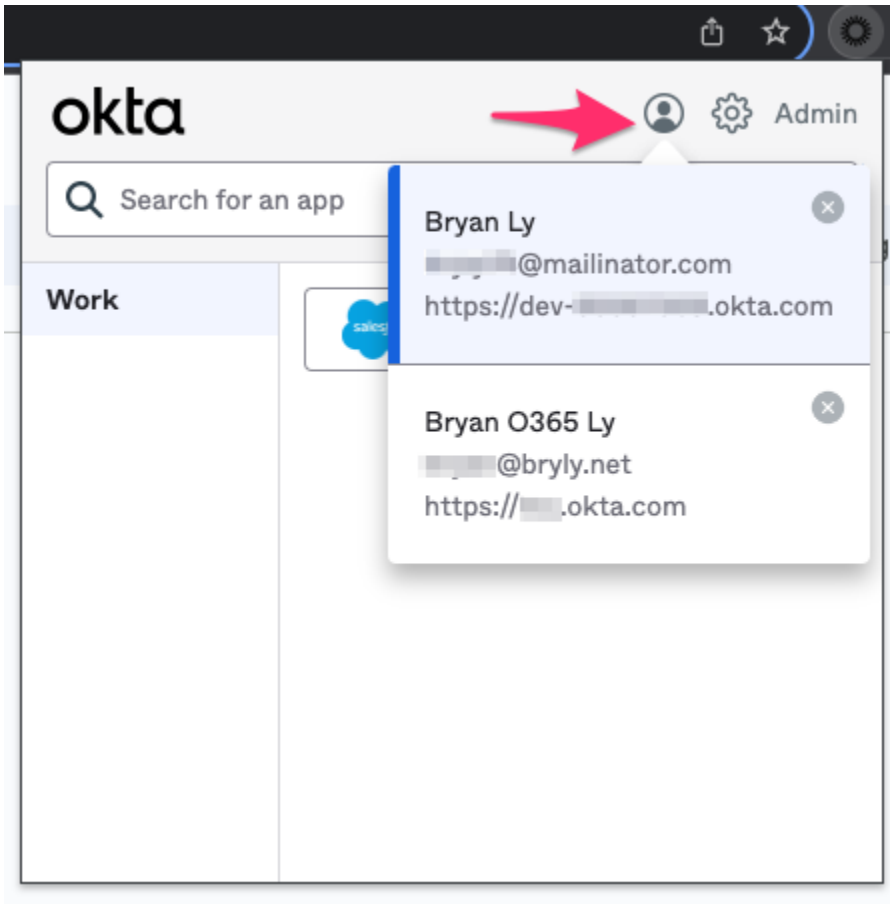


6. Click **Save**.

1.3 - Switch between multiple Okta accounts using the Plugin

You can easily switch between multiple Okta accounts through the Okta browser plugin.

1. You may be prompted to trust or reject subsequent Okta accounts the first time you access those accounts.



2. Switch Okta accounts by clicking the Account Chooser icon.
3. To remove an account from the account chooser, click the X icon.

WELL DONE !!! You've completed the Okta Fundamental Introduction Lab