

Lab Guide:

Okta Fundamentals - Intro Labs

Table of Contents

Prerequisites	3
Lab 1-1: Create an Account and Access your Okta Tenant	3
Create an Okta developer account	3
Lab 1-2: Create Okta Sourced Users	5
1.1 Create and activate two accounts in the Okta Admin portal	5
1.2 Import a list of users from a CSV file	
Another way to create users is through a CSV import	7
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.	10
Lab 1-3: Create and Manage Groups in Okta	11
1.1 Create Groups via the admin UI	11
1.2 Assign Users to Groups	12
1.3 Configure Group Membership Rules	13
Lab 1-4: Add and Configure SWA Applications	15
1.1 - Add and configure a SWA Application - Youtube (End-User flow)	15
1.2 - Add and configure a SWA Application - Youtube (administrator flow)	17
1.3 - Add and configure a SWA Application - Linkedin	20
Lab 1-5: Delete Applications	21
1.1 - Delete the Youtube application (end-user flow)	21
1.2 - Delete the Linkedin application (admin flow)	22
Lab 1-6: Configure SAML Applications in Okta	24
1.1 - Configure Salesforce application with SAML	24
1.2 - Configure SP-Initiated SAML between Salesforce and Okta	31
1.3 - (OAuth Consumer Key and OAuth Consumer Secret)	36
Lab 1-7: Configure User Lifecycle Management in Okta	43
1.1 - Configure Salesforce with Lifecycle Management	43
Lab 1-8: Set Up SAML Tracer for Troubleshooting	46
1.1 - Configure SAML Tracer for Firefox & Chrome	46
Lab 1-9: Configure Applications using the Application Integration Wizard (AIW)	50
1.1 - Configure Linkedin using the Application Integration Wizard	50
1.2 - Configure a SAML application using the AIW – Salesforce (metadata file)	52

BONUS LAB Exercises	57
Lab 1-10: Configure Applications using the OIN Templates	57
1.1 - Configure a SWA application using the Template Plugin App 3 Fields – Ready Tech Admin	57
Lab 1-11: Configure the Application Approval Workflow.	62
1.1 - Configure Self-Service for Salesforce	62
1.2 - Review Application Access Reports	69
Lab 1-12: Personalize Your Okta Tenant	71
1.1 - Change the Color, Logo and Background Image	71
1.2 - Customize the Sign-In Page	76
Lab 1-13: Configure the Okta Browser Plugin	79
1.1 - Configure the Okta Browser Plugin (End-User settings)	79
1.2 - Configure the Okta Browser Plugin (Admin settings)	83
1.3 - Switch between multiple Okta accounts using the Plugin	84

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.

The screenshot shows the Okta landing page with three main service offerings:

- Customer Identity Cloud**: FREE tier for developers. It secure my customers or SaaS applications. Call-to-action: Try Customer Identity Cloud →.
- Workforce Identity Cloud**: FREE TRIAL for IT admins. It secure my employees, contractors, & partners. Call-to-action: Try Workforce Identity Cloud →.
- Developer Edition Service**: FREE tier for developers. It access the Okta Developer Edition Service. Test your code and apps, as well as manage and automate Okta for employees and partners. Call-to-action: Sign up free for Developer Edition.

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.

The screenshot shows the Okta end-user dashboard with the following interface elements:

- Header:** Shows the URL as dev-! .okta.com/app/UserHome and a navigation bar with back, forward, search, and other browser controls.
- User Profile:** Shows "Bryan" and "okta-dev-".
- Sidebar:** Shows "My Apps", "Notifications", and "Add apps".
- Main Content:**
 - A modal dialog titled "Trust this account in the Okta browser plugin" with instructions to open the Okta browser plugin and click "Trust". It includes a "Need help?" link and a close "X" button.
 - The "My Apps" section displays a placeholder message: "Add apps to your launcher" with a rocket icon, followed by "Please contact your admin for assistance."

Lab 1-2: Create Okta Sourced Users

Objective	To create and import users into Okta
Procedures	<ul style="list-style-type: none">• 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:

Add Person

User type  User

First name John

Last name Ly

Username john.ly99@mailinator.com

Primary email john.ly99@mailinator.com

Groups (optional) You haven't added any [groups](#)

Activation  Activate now

I will set password
.....
To create new users with password, enrollment policy must set password as required

User must change password on first login

Do not send unsolicited or unauthorized activation emails. [Read more](#)

[Save](#) [Save and Add Another](#) [Cancel](#)

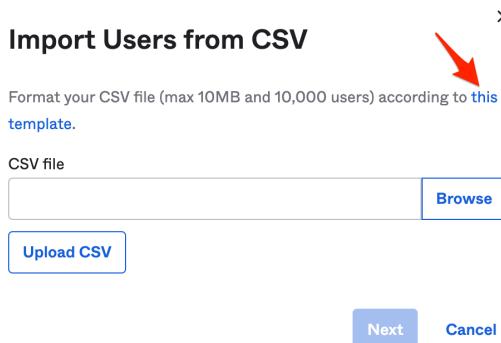
If you'd like to use a free email service, check out <https://www.mailinator.com>. You can use this to create your test users.

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.



Import Users from CSV

Format your CSV file (max 10MB and 10,000 users) according to [this template](#).

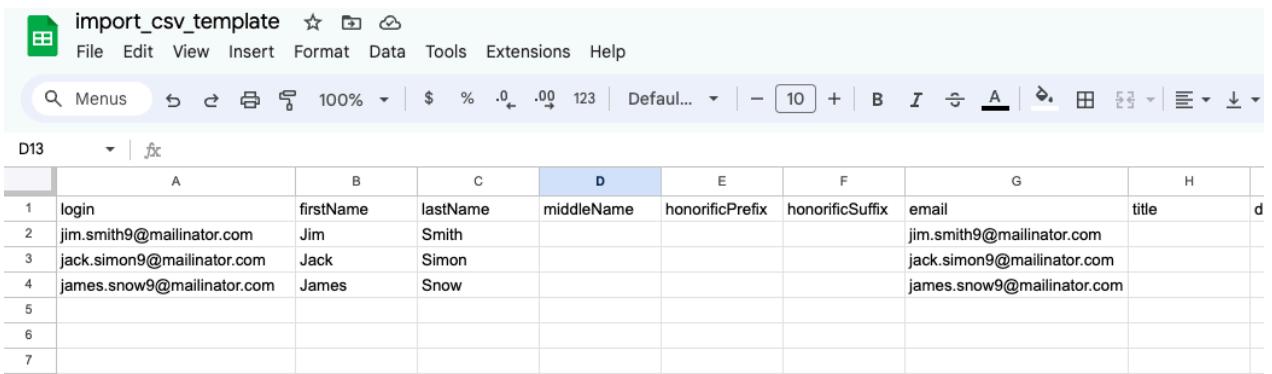
CSV file

[Browse](#)

[Upload CSV](#)

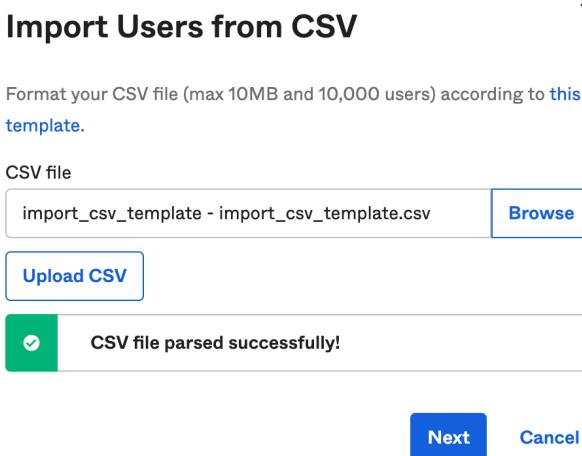
[Next](#) [Cancel](#)

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	d
1	login	firstName	lastName	middleName	honorificPrefix	honorificSuffix	email		
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**.



Import Users from CSV

Format your CSV file (max 10MB and 10,000 users) according to [this template](#).

CSV file

[Browse](#)

[Upload CSV](#)

CSV file parsed successfully!

[Next](#) [Cancel](#)

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

Import Users from CSV

X

Click Import Users to start importing your users.

- Automatically activate new users

When selected, new imported users will be automatically activated.

- Do not create a password and only allow login via Identity Provider

Only use this option for users who will authenticate via an external Identity Provider. When selected, users will not be sent activation emails and will not set up an Okta password.

Import Users

Cancel

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

Import Users from CSV

X

3 users imported!

- 3 new users
- 0 updated users
- 0 users unchanged
- 0 users with errors

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-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**.

The screenshot shows the Okta Admin Console interface. At the top, there is a navigation bar with tabs: Overview, Roles, Resources, and Admins. The Admins tab is highlighted with a red box and a blue underline. Below the tabs, there are two filter options: 'View by type' (with 'Users' selected) and 'Filter by admin' (an empty input field). To the right of these filters is a large blue button labeled 'Add administrator' with a red arrow pointing towards it. The main table below has columns for Admin, Roles, and Action. One row is visible, showing 'Bryan Ly' as the Admin, 'Super Administrator' as the Role, and an 'Edit' button in the Action column.

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

Administrator assignment by admin

This screenshot shows a dropdown menu titled 'Admin'. The placeholder text 'Select a user or group' is visible inside the dropdown. A small downward arrow icon is at the bottom right of the dropdown box.

4. Select the user.

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

Administrator assignment by admin

Select admin

John Ly (john.ly99@mailinator.com)

Complete the assignment

Create role assignments by selecting roles and resource sets that you want to constrain the given admin to.

This role cannot be further constrained and will be active for the entire org

Role	Preview	Remove
Super Administrator		

- 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	<ul style="list-style-type: none"> 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

- Navigate to **Directory > Groups**.

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

Add group

Name	Support
Description (optional)	CS Support
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

Groups [Help](#)

All	Rules			
<input type="button" value="Add Group"/> <input type="text" value="Search..."/>				
Source	Name	People	Apps	Directories
<input checked="" type="radio"/>	Everyone All users in your organization	5	0	0
<input checked="" type="radio"/>	Managers CS Managers	0	0	0
<input checked="" type="radio"/>	Sales Sales Group	0	0	0
<input checked="" type="radio"/>	Support CS Support	0	0	0

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:

Groups

The screenshot shows the 'Groups' page in Okta. At the top, there are tabs for 'All' and 'Rules'. Below the tabs is a search bar with the placeholder 'Search...'. A blue button labeled '+ Add Group' is visible. The main area displays a table with four rows:

Source	Name	People	Apps	Directories
Everyone	All users in your organization	5	0	0
Managers	CS Managers	0	0	0
Sales	Sales Group	2	0	0
Support	CS Support	2	0	0

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**.

Add Rule

The screenshot shows the 'Add Rule' configuration page. It includes fields for 'Name' (set to 'Managers'), 'IF' conditions, 'THEN' actions, and 'EXCEPT' users. At the bottom, there are 'Preview' and 'Save' buttons.

IF conditions:

- Use basic condition (selected)
- User attribute
- title | string
- Equals
- Manager

THEN Action:

- Assign to: Managers

EXCEPT Users:

This rule will not add users to a group they've been manually removed from.

Buttons at the bottom:

- Preview
- Enter an Okta user to preview this rule
- Save
- Cancel

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.

Add Rule

User matches rule

Name: Managers

IF

Use basic condition (radio button selected) Use Okta Expression Language (advanced)

User attribute: title | string Equals: Manager

THEN Assign to: Managers

This rule will not add users to a group they've been manually removed from.

EXCEPT The following users:

Preview: John Ly Save Cancel

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.

Managers

Actions ▾

Created: 10/2/2023 Last modified: 10/2/2023 View logs

People Applications Profile Directories Admin roles

People

Person & username	Status	Managed
John Ly john.ly99@mailinator.com	Active	By rule Managers

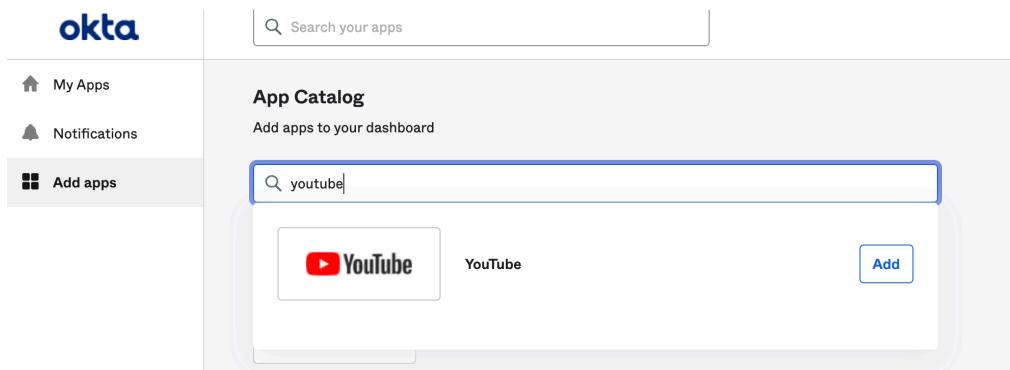
Showing 1 of 1

Lab 1-4: Add and Configure SWA Applications

Objective	To add and configure SWA applications in Okta
Procedures	<ul style="list-style-type: none">• Create SWA apps• Assign Applications to users• Test Single Sign-On• Reveal Password
Duration	30-45 minutes

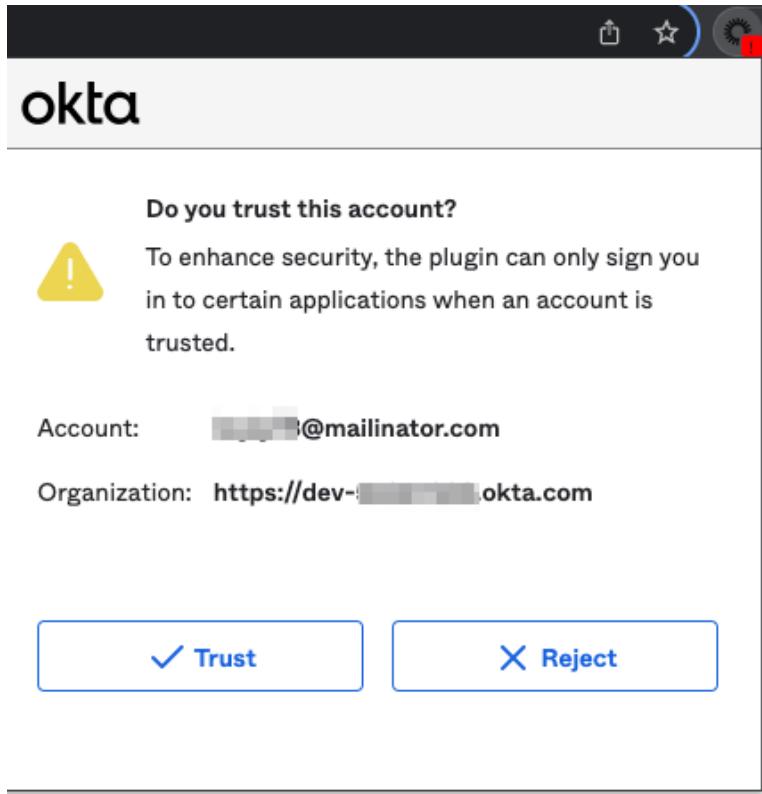
1.1 - Add and configure a SWA Application - Youtube (End-User flow)

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**.

< Back to My Apps

YouTube

Setup access to your YouTube account in Okta

Enter your username and password for YouTube. If you don't have one, please create an account on YouTube or contact your administrator.

Username

[REDACTED]@mailinator.com

Password

[REDACTED]

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.

Browse App Integration Catalog

[Create New App](#)

Use Case	
All Integrations	7684
Apps for Good	10
Automation	105
Centralized Logging	27
Directory and HR Sync	49
Bot or Fraud Detection	5
Identity Proofing	28
Identity Governance and Administration (IGA)	30

Search: youtube
X

POPULAR SEARCHES : Bookmark App SCIM 2.0 Test App Okta Org2Org Template App

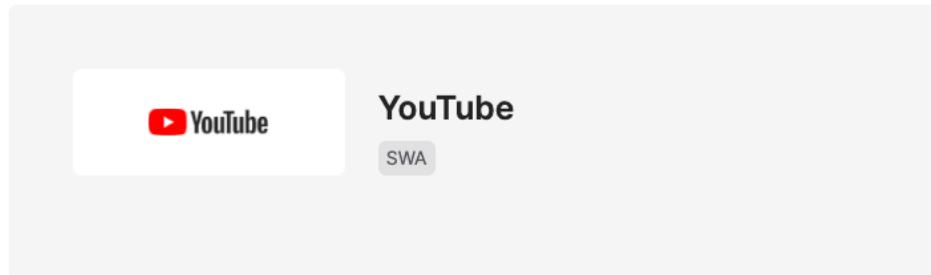
YouTube SWA	easystub SWA
Uber SWA	Cube19 SWA
Cube OIDC	See All Results →

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

Applications > Catalog > Single Sign-On > YouTube

Last updated: September 22, 2022

+ Add Integration



Okta Verified Overview

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

Add YouTube

General Settings

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

General settings
All fields are required to add this application unless marked optional.

Cancel **Next**

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

Add YouTube

The screenshot shows the 'Sign-On Options' configuration page for the YouTube app. At the top, there are two tabs: 'General Settings' (numbered 1) and 'Sign-On Options' (numbered 2, which is highlighted). Below the tabs, the title 'Sign-On Options· Required' is displayed. Under the title, the section 'Sign on methods' is shown. A note states: '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.' It also mentions that 'Application username is determined by the user profile mapping. [Configure profile mapping](#)'. A blue info icon box contains the text: 'Secure Web Authentication is the only sign-on option currently supported for this application.' To the right of this box is a list of three options: 'Secure Web Authentication' (selected), 'User sets username and password', and 'Administrator sets username and password'. The 'User sets username and password' option is also highlighted with a blue circle.

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.

Browse App Integration Catalog

Create New App

Use Case	
All Integrations	7374
Apps for Good	13
Automation	12
Centralized Logging	10
Directory and HR Sync	12
Bot or Fraud Detection	2
Identity Proofing	5
Identity Governance and	2

POPULAR SEARCHES : Bookmark App SCIM 2.0 Test App Okta Org2Org Template App

LinkedIn SWA

LinkedIn Learning SAML

LinkedIn Talent Solutions SAML

LinkedIn IdP Inbound Federation

LinkedIn Sales Navigator SWA

See All Results →

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**.

i Secure Web Authentication is the only sign-on option currently supported for this application.

Secure Web Authentication

User sets username and password

Administrator sets username and password

Administrator sets username, user sets password

Administrator sets username, password is the same as user's Okta password

Users share a single username and password set by administrator

Shared Username

Shared Password

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.

The screenshot shows the Okta Assignments page for the LinkedIn application. At the top, there's a LinkedIn logo and navigation links for Active, View Logs, and Monitor Imports. Below that, tabs for General, Sign On, Import, and Assignments are present, with Assignments being the active tab. A search bar and a Groups dropdown are also at the top. The main area displays a table with columns for Priority, Assignment, and Actions (Edit and Delete). Two entries are listed:

Priority	Assignment	
1	Managers No description	Edit Delete
2	Support CS Support	Edit Delete

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.

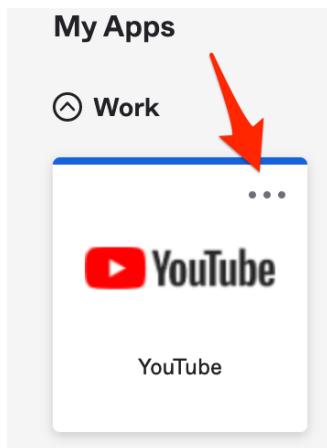
Lab 1-5: Delete Applications

Objective	To delete applications in Okta
Procedures	<ul style="list-style-type: none"> Delete the end-user flow app Delete the administrator flow app
Duration	5-10 minutes

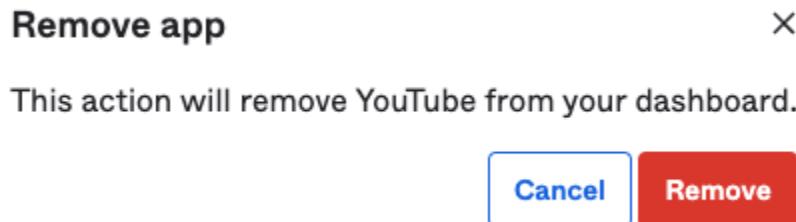
1.1 - Delete the Youtube application (end-user flow)

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.



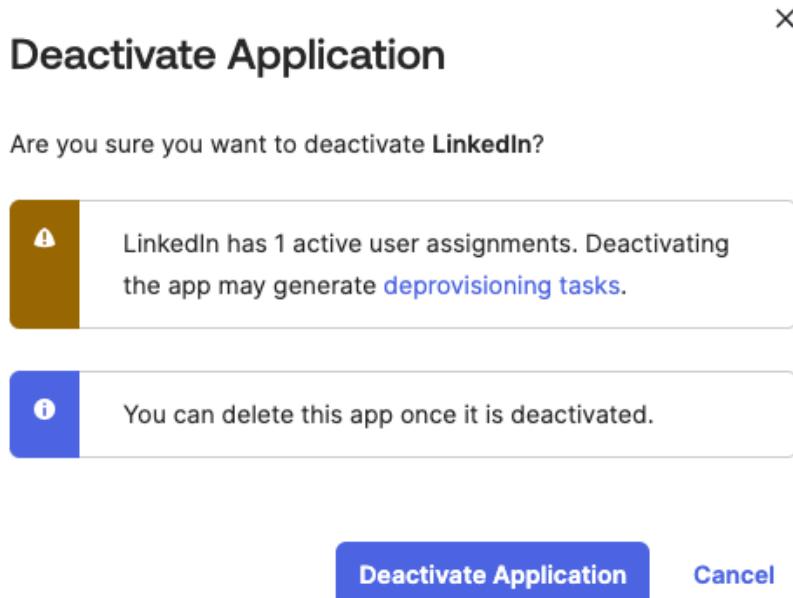
3. On the right side of the screen, click on **Remove**.
4. Click **Remove** to confirm removal of the app.



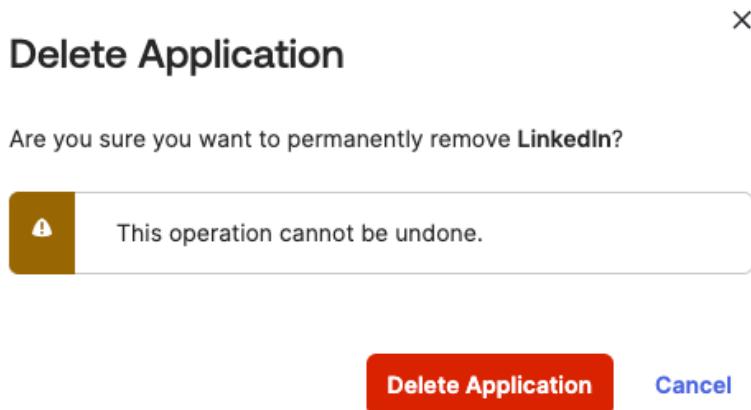
1.2 - Delete the LinkedIn application (admin flow)

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 drop-down on the gear icon.

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



5. Select **Inactive** on the main applications page. Click the drop-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	<ul style="list-style-type: none"> 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.

Browse App Integration Catalog

Create New App

Use Case	
All Integrations	7684
Apps for Good	10
Automation	105
Centralized Logging	27
Directory and HR Sync	49
Bot or Fraud Detection	5
Identity Proofing	28
Identity Governance and	30

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

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

General settings· Required

Application label This label displays under the app on your home page

Instance Type Select the type of Salesforce instance that you want to connect to.

Custom Domain Enter your custom domain. If your domain is `acme.my.salesforce.com`, enter `acme`. This field is only required if you are using your custom domain for your Entity Id in Salesforce or if you are using Salesforce Government Cloud. ([How to Configure](#))

User Profile & Type Select the type of user you wish to provision to or import from Salesforce. "Standard" will create normal Salesforce users and is the default. If you have a Portal or Community in Salesforce then you can instead choose to have Okta provision these as "external users". Use multiple Salesforce.com application instances to handle both "Standard" users as well "Portal" and "Community" users.

Seats (optional) If you enter the number of licenses purchased for this app, we can provide a seat utilization report.

Application Visibility Do not display application icon to users
 Do not display application icon in the Okta Mobile App

Browser plugin auto-submit Automatically log in when user lands on login page

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

SAML 2.0

Default Relay State All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

Preview SAML

Enable Single Logout

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.

Credentials Details

Application username format

Custom

Expression Language Reference

substringBefore(user.email, '@')+"@bry.com"

To maintain security, do not use fields which can be edited by users.

Update application username on

Create and update

Allow users to securely see their password
(Recommended)

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

Previous Cancel Done

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.

The screenshot shows a search interface with a search bar containing the text 'single'. Below the search bar are two buttons: a magnifying glass icon and a question mark icon. Underneath the search bar is a link labeled 'Expand All | Collapse All'. The main content area has a title 'Administer' and a section titled 'Security Controls' which contains a checked checkbox and a link labeled 'Single Sign-On Settings'.

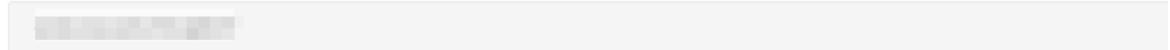
16. Click **Edit** and check SAML Enabled under 'Federated Single Sign-On Using SAML'.
17. Click **New**.

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:



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

[https://dev-\[REDACTED\]-admin.okta.com/admin/org/security/0oabrhnx94wN6yBI5d7/cert](https://dev-[REDACTED]-admin.okta.com/admin/org/security/0oabrhnx94wN6yBI5d7/cert)

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

[https://dev-\[REDACTED\].okta.com/app/salesforce/exkbrhenx8a39UuqW5d7/sso/saml](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](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](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:

SAML Single Sign-On Settings

20. Click **Save**.

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

Endpoints

View SAML endpoints for your org, Experience Cloud sites, or custom domains.

Your Organization

Login URL https://bryster-dev-ed.my.salesforce.com?so=00Df400000m6uY

Logout URL https://bryster-dev-ed.my.salesforce.com/services/auth/sp/saml2/logout

OAuth 2.0 Token Endpoint https://bryster-dev-ed.my.salesforce.com/services/oauth2/token?so=00Df400000m6uY

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.

Advanced Sign-on Settings

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

Login URL

`https://bryster-dev-ed.my.salesforce.com?so=0ODf400`

Enter the Salesforce Login URL specified in your single-sign on settings in Salesforce.

Logout URL

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

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.

Assign Salesforce.com to People

User Name	john.onboard@bry.com	
Save and Go Back		Cancel

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

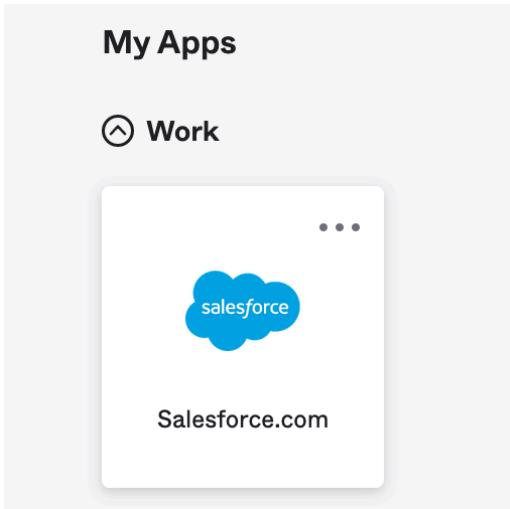
Person	Type
John Onboard john.onboard@atko.email	Individual

Edit User Assignment

User Name	bryan@bryly.net	
Save		Cancel

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.

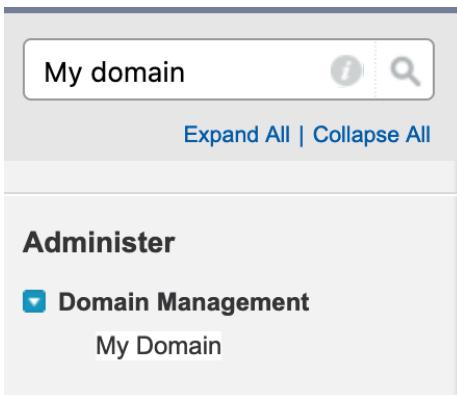
29. Click on the **Salesforce.com** app from the user dashboard to SSO.

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.

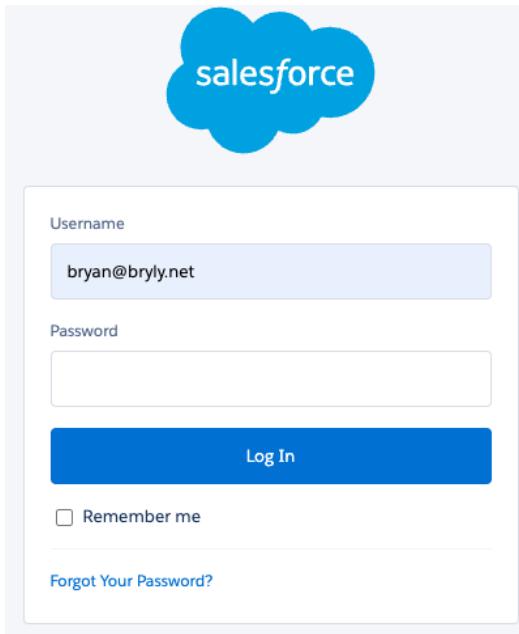
1.2 - Configure SP-Initiated SAML between Salesforce and Okta

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](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](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**.

Advanced Sign-on Settings

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

Login URL
 Enter the Salesforce Login URL specified in your single-sign-on settings in Salesforce.

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

20. Click **Save**.

21. Navigate to **Applications > Applications > Salesforce > General** tab and click **Edit**.

Enter in the custom domain.

General Sign On Mobile Provisioning Import Assignments

App Settings Cancel

Application label
 This label displays under the app on your home page

Instance Type
 Select the type of Salesforce instance that you want to connect to.

Custom Domain
 Enter your custom domain. If your domain is acme.my.salesforce.com, enter acme. This field is only required if you are using your custom domain for your Entity Id in Salesforce or if you are using Salesforce Government Cloud. ([How to Configure](#))

User Profile & Type

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**.

Authentication Configuration	
Edit	
Authentication configuration settings apply to all deployed and provisioned domains for this org.	
Login Page Type	Standard
Authentication Service	Login Form Okta - Bry Ly
Logo File	
Background Color	<input type="color" value="#f4f6f9"/>
Right Frame URL	
Use the native browser for user authentication on iOS	<input type="checkbox"/>
Use the native browser for user authentication on Android	<input type="checkbox"/>

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**.

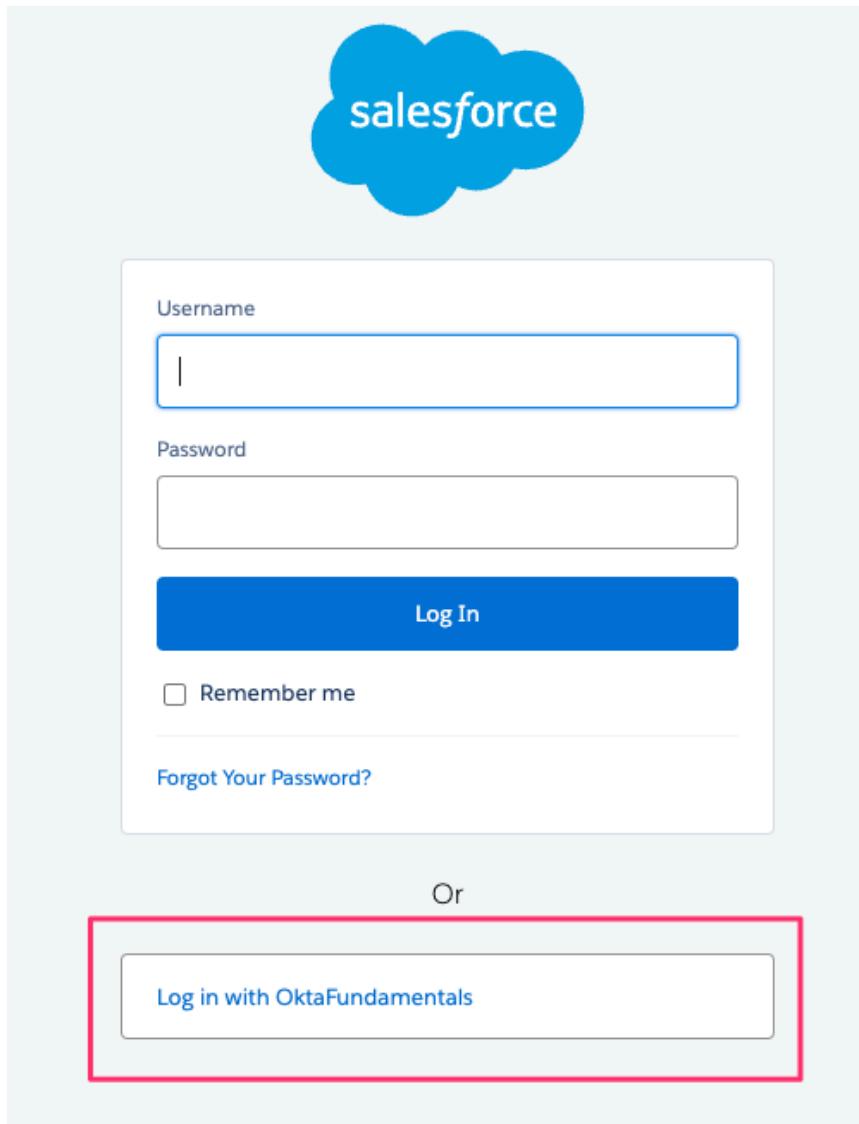
Login Page Type	Standard
Authentication Service	<input checked="" type="checkbox"/> Login Form <input type="checkbox"/> Okta - Bry Ly <input type="checkbox"/> Okta for Fed ID <input type="checkbox"/> Okta-Community <input checked="" type="checkbox"/> OktaFundamentals <input type="checkbox"/> Onboarding <input type="checkbox"/> SAML_AIW <input type="checkbox"/> Salesforce SLO <input type="checkbox"/> Veza <input type="checkbox"/> www

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.

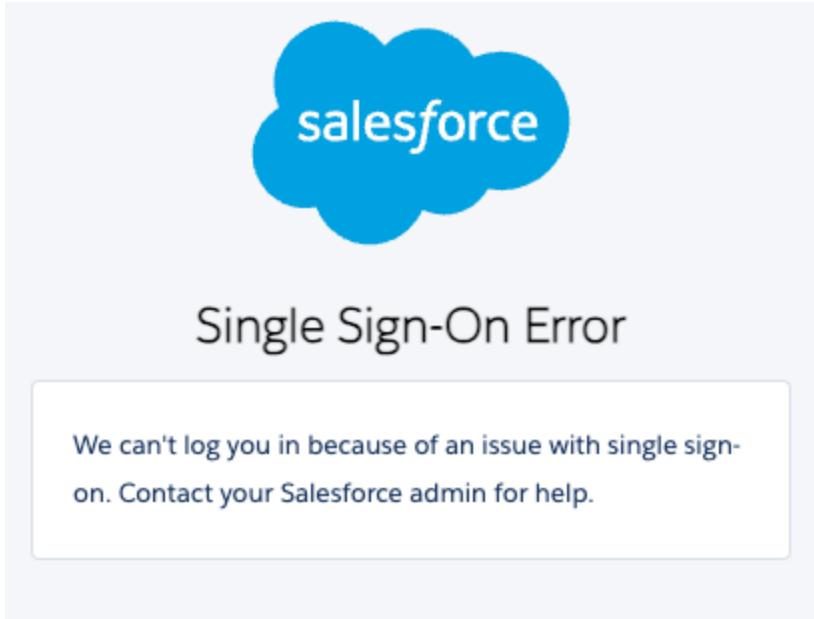
<https://bryster-dev-ed.my.salesforce.com>) and you should see the option to login

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.



The screenshot shows a Salesforce error page with a blue cloud icon containing the word "salesforce". The title is "Single Sign-On Error". A message box contains the text: "We can't log you in because of an issue with single sign-on. Contact your Salesforce admin for help." Below the message, a list of steps is shown:

- 7. Confirming Issuer matches **Ok**
- 8. Confirming a Subject Confirmation was provided and contains valid timestamps **Ok**
- 9. Checking that the Audience matches **Audience problems**
 - The audience in the assertion did not match the allowed audiences
 - Allowed audiences: [https://bryster-dev-ed.my.salesforce.com]
- 10. Checking the Recipient **Ok**
- 11. Validating the Signature **Is the response signed? true**

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/oauth2redirect>
 - **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

Basic Information

Connected App Name: Okta Fundamentals
 API Name: Okta_Fundamentals
 Contact Email: bryan@bryly.net
 Contact Phone:
 Logo Image URL: Upload logo image or Choose one of our sample logos
 Icon URL: Choose one of our sample logos
 Info URL:
 Description:

API (Enable OAuth Settings)

Enable OAuth Settings:
 Enable for Device Flow:
 Callback URL: https://system-admin.okta.com/admin/app/generic/oauth2redirect
 Use digital signatures:
 Selected OAuth Scopes

Available OAuth Scopes	Selected OAuth Scopes
Access unique user identifiers (openid) Full access (full) Manage Data Cloud Calculated Insight data (cdp_calculated_insight_api) Manage Data Cloud Identity Resolution (cdp_identityresolution_api) Manage Data Cloud Ingestion API data (cdp_ingest_api) Manage Data Cloud profile data (cdp_profile_api) Manage Pardot services (pardon_api) Manage user data via Web browsers (web) Perform ANSI SQL queries on Data Cloud data (cdp_query_api) Perform segmentation on Data Cloud data (cdp_segment_api)	Manage user data via APIs (api) Perform requests at any time (refresh_token, offline_access)

Add Remove

Require Secret for Web Server Flow:
 Require Secret for Refresh Token Flow:
 Enable Client Credentials Flow:
 Enable Authorization Code and Credentials Flow:
 Opt in to issue JSON Web Token (JWT)-based access tokens for named users (Beta):
 Introspect All Tokens:

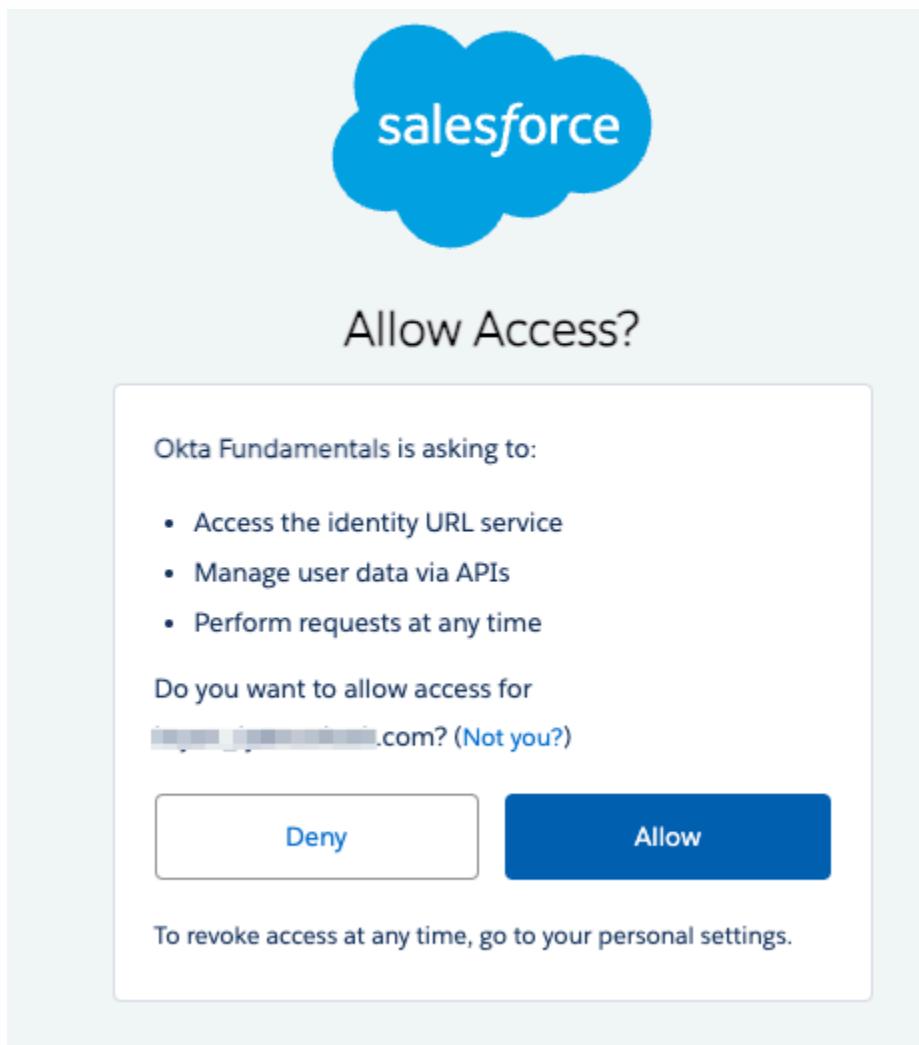
- Once saved, get your Consumer Key and Consumer Secret under API (Enable OAuth Settings) section and use them for enabling provisioning for Salesforce in

Okta.

▼ API (Enable OAuth Settings)	
Consumer Key and Secret	Manage Consumer Details
Selected OAuth Scopes	Manage user data via APIs (api) Perform requests at any time (refresh_token, offline_access)
Callback URL	https://system-admin.okta.com/admin/app/generic/oauth20redirect
Enable for Device Flow	<input type="checkbox"/>
Require Secret for Web Server Flow	<input checked="" type="checkbox"/>
Require Secret for Refresh Token Flow	<input checked="" type="checkbox"/>
Enable Client Credentials Flow	<input type="checkbox"/>
Enable Authorization Code and Credentials Flow	<input type="checkbox"/>
Opt in to issue JSON Web Token (JWT)-based access tokens for named users (Beta)	<input type="checkbox"/>
Introspect All Tokens	<input type="checkbox"/>
Token Valid for	0 Hour(s)
Include Custom Attributes	<input type="checkbox"/>
Include Custom Permissions	<input type="checkbox"/>
Enable Single Logout	Single Logout disabled

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.

The screenshot shows the configuration page for integrating Salesforce with Okta. At the top, a blue info icon says "How to configure Salesforce". On the right, there's a "Cancel" button. Below that, a green checkmark icon says "Salesforce.com was verified successfully!". Underneath, a checked checkbox labeled "Enable API integration" is followed by a note: "Authenticate with Salesforce.com to enable user import and provisioning features." A green checkmark icon next to this note says "Salesforce.com's API is authenticated. Click Re-authenticate with Salesforce.com to generate a new authentication token." To the right of this note is a blue "Re-authenticate with Salesforce.com" button. Below these sections are fields for "OAuth Consumer Key" (containing a redacted value) and "OAuth Consumer Secret" (containing a redacted value). There is also a checkbox for "Push Null Values" which is unchecked. At the bottom right is a blue "Save" button.

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**.

The screenshot shows the Okta Admin Console interface for managing the Salesforce.com application. The top navigation bar includes the Salesforce logo, a dropdown menu, and several icons. Below the navigation is a tabs bar with General, Sign On, Mobile, Provisioning (which is selected), Import, and Assignments. A horizontal line separates this from the main content area.

The main content area has a sidebar on the left labeled "Settings" with options To App, To Okta, and Integration. The "To App" option is selected. The main panel shows a diagram with the Okta logo pointing to the Salesforce logo, indicating the direction of provisioning.

Provisioning to App

Create Users Enable

Creates or links a user in Salesforce.com when assigning the app to a user in Okta.
The default username used to create accounts is set to Custom.

Update User Attributes Enable

Okta updates a user's attributes in Salesforce.com when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Salesforce.com.

Deactivate Users Enable

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	<ul style="list-style-type: none"> 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**.

The screenshot shows the Okta application configuration interface for the Salesforce app. The top navigation bar includes tabs for General, Sign On, Mobile, Provisioning (which is underlined), Import, and Assignments. On the left, a sidebar titled 'Settings' lists 'To App', 'To Okta', and 'Integration'. The main panel shows a diagram with 'okta' on the left and 'salesforce' on the right, connected by an arrow. Below this is the 'Provisioning to App' section. Under 'Create Users', there is a description: 'Creates or links a user in Salesforce.com when assigning the app to a user in Okta.' It notes that the default username is set to 'Custom'. An 'Edit' button is visible with a red arrow pointing to it. There is also an 'Enable' checkbox. Under 'Update User Attributes', there is a note about Okta updating attributes in Salesforce.com when assigned, with an 'Enable' checkbox.

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*).

Assign Salesforce.com to People ×

User Name	albert-test@bryly.net	
First Name	Albert	
Last Name	Test	
Email	albert-test@atko.email	
Profile URL	Chatter Free User	▼
Title		

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

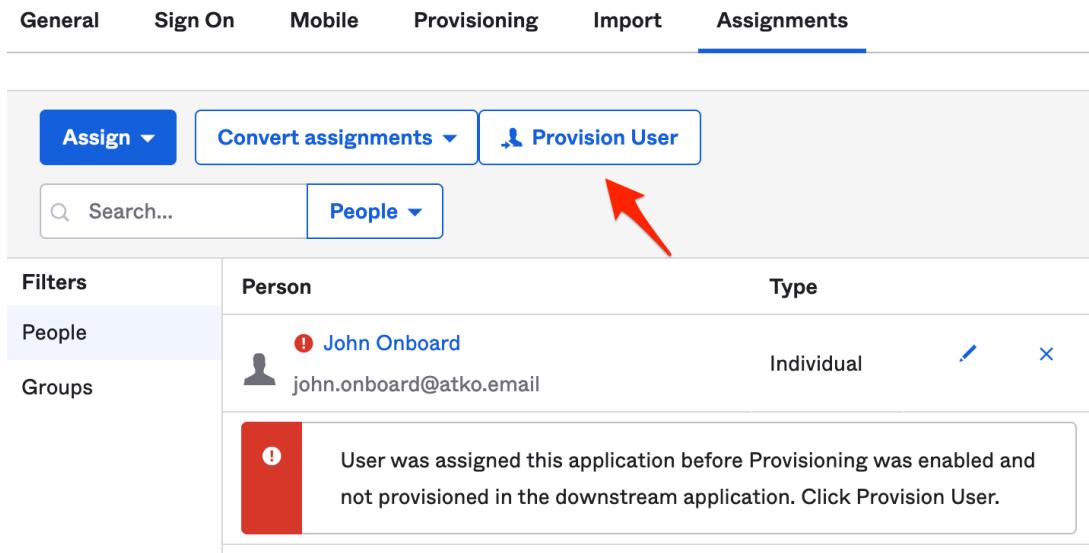
Role	-- No Role --	▼
------	---------------	---

Permission Sets

- B2BBuyer
- B2BBuyerManager
- BryanNew_Permission
- Bryan_Community
- Bryan_Permission
- C2CHeadlessCMSSAccessPermSet
- CRMUserPsi
- CommerceAdmin

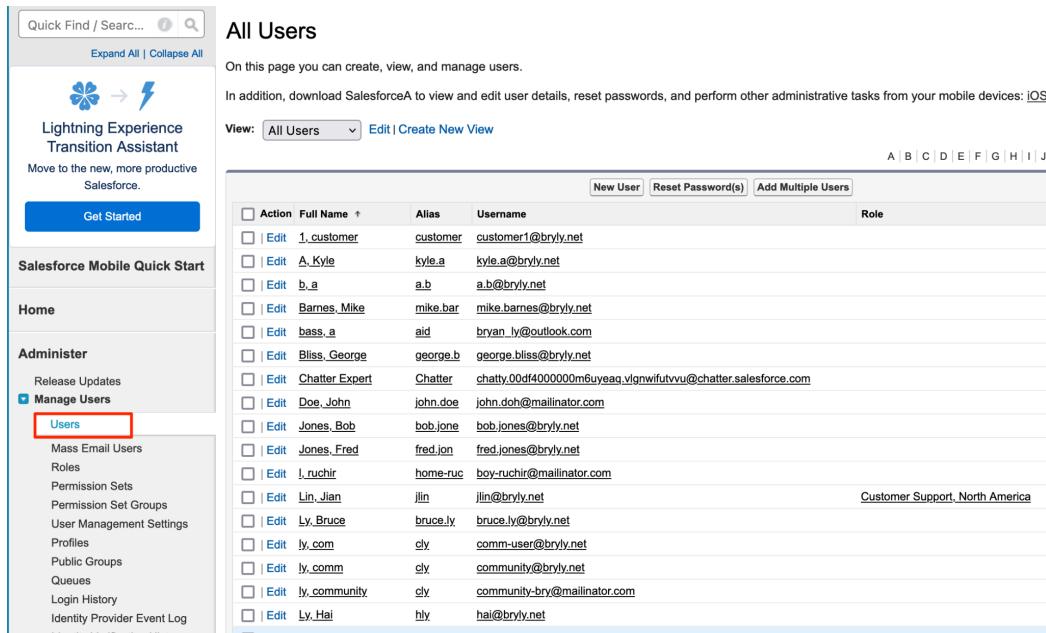
10. Click **Save and Go Back**.

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



The screenshot shows the Okta Assignments tab interface. At the top, there are buttons for 'Assign', 'Convert assignments', and 'Provision User'. Below these are search and filter fields. A red arrow points to the 'Provision User' button, which is highlighted in blue. The main table lists a user named 'John Onboard' with the email 'john.onboard@atko.email'. The status for this user is 'Individual' with a pencil icon for edit and a delete icon. A red callout box below the table contains the message: 'User was assigned this application before Provisioning was enabled and not provisioned in the downstream application. Click Provision User.'

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.



The screenshot shows the Salesforce All Users page. The sidebar includes sections for Lightning Experience Transition Assistant, Salesforce Mobile Quick Start, Home, Administer (with a red box around the 'Users' link), Release Updates, and Manage Users. The main area displays a table of users with columns for Action, Full Name, Alias, Username, and Role. The table lists various users such as 'customer', 'kyle.a', 'a.b', 'mike_bar', 'aid', 'george.b', 'Chatter Expert', 'Doe_John', 'bob.jone', 'fred.jon', 'j_ruchir', 'Lin_Jian', 'Ly_Bruce', 'ly_com', 'ly_community', and 'Ly_Hai'. Buttons at the top right include 'New User', 'Reset Password(s)', and 'Add Multiple Users'. A note at the bottom right says 'Customer Support, North America'.

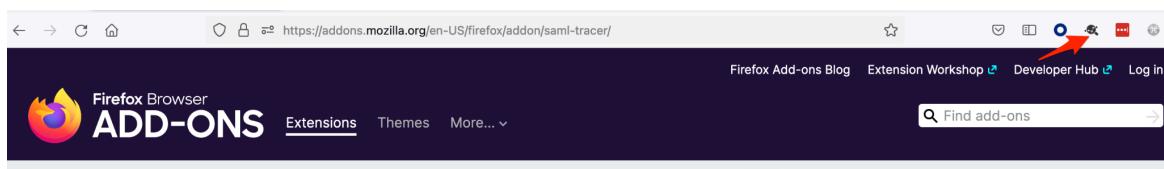
14. Repeat Step 6 to assign one more user.
 15. Log in to Okta with both users who were assigned to Salesforce to verify the SAML authentication flow and the profile assignment.

Lab 1-8: Set Up SAML Tracer for Troubleshooting

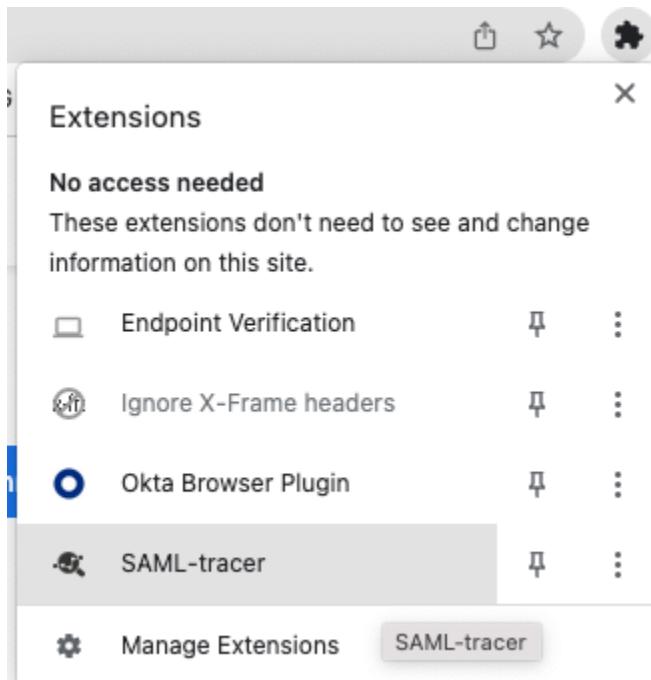
Objective	To configure troubleshooting options with SAML.
Procedures	<ul style="list-style-type: none"> Configure SAML Tracer for Firefox & Chrome
Duration	10-20 minutes

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**.

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



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

Method	URL
GET	https://cs-bloom.okta.com/home/salesforce/0oa148iq1c1HA0Nsn697/46?fromHome=true
GET	https://cs-bloom.okta.com/app/salesforce/0oa148iq1c1HA0Nsn697/mc?fromHome=true
GET	https://cs-bloom.okta.com/app/salesforce/exk148iq1b8W58N5K697/sso/saml
POST	https://bryster-dev-ed.my.salesforce.com/?so=0 [highlighted]
GET	https://bryster-dev-ed.my.salesforce.com/secur/frontdoor.jsp?sid=00Df4000000m6uY%21AQoAQC
GET	https://na153.salesforce.com/secur/myDomainDoor?oid=00Df4000000m6uY&retURL=https%3A%2F%2F
GET	https://bryster-dev-ed-c.na153.content.force.com/secur/contentDoor?startURL=https%3A%2F%2F
GET	https://bryster-dev-ed-c.na153.content.force.com/jlibrary/1635874030236/sfdc/SfdcSessionBase2
GET	https://login.salesforce.com/login/sessionserver212.html
GET	https://bryster-dev-ed.my.salesforce.com/setup/forcecomHomepage.apexp?setupid=ForceCom
GET	https://bryster-dev-ed.my.salesforce.com/sCSS/54.0/sprites/1641822910000/Theme3/default/base/

HTTP Parameters SAML Summary

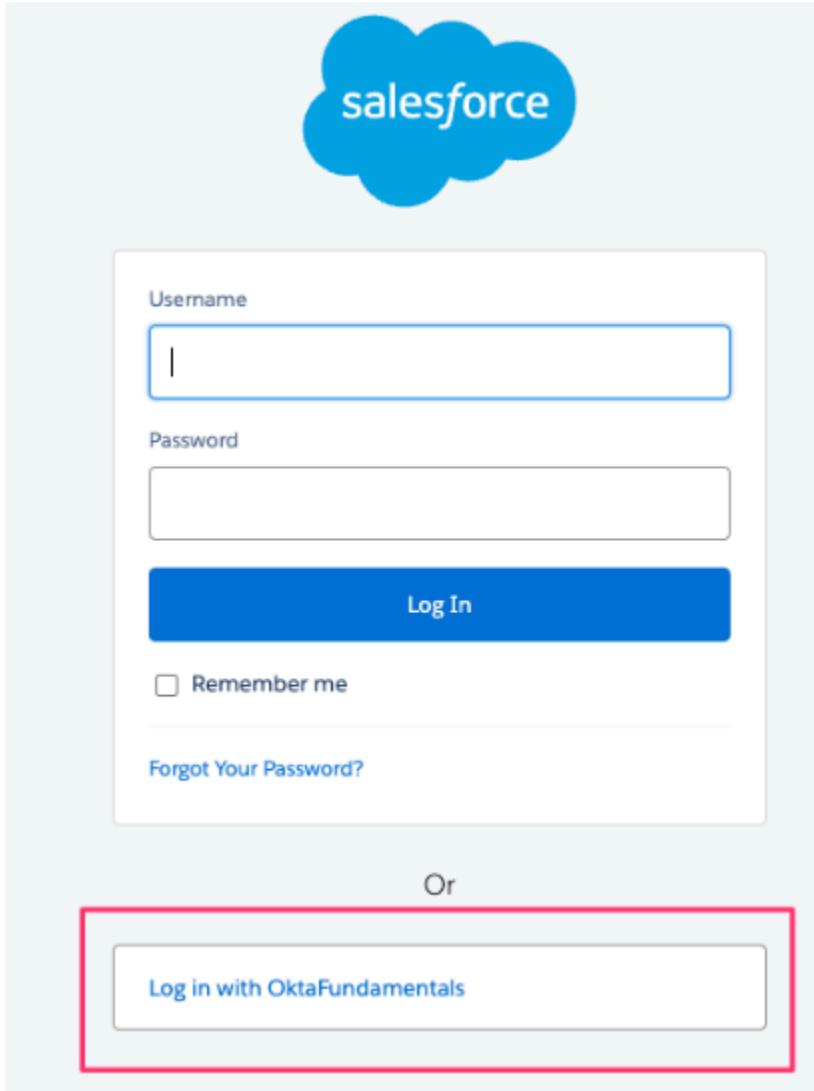
```

POST https://bryster-dev-ed.my.salesforce.com/ [highlighted] HTTP/1.1
Host: bryster-dev-ed.my.salesforce.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100.0)
Gecko/20100101 Firefox/100.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 6669
Origin: https://cs-bloom.okta.com
Connection: keep-alive
Referer: https://cs-bloom.okta.com/
Cookie: CookieConsentPolicy=0:1; LSKey-c$CookieConsentPolicy=0:1;

```

- You can now validate the Destination URL, Audience, NameID and other attributes.
- Log out** of Salesforce.
- 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

The screenshot shows the SAML Tracer tool interface. At the top, there are several buttons: 'Clear', 'Pause', 'Autoscroll', 'Filter resources', 'Colorize' (which is selected), 'Export', and 'Import'. Below the buttons, a list of network requests is displayed. Two specific requests are highlighted with orange boxes and labeled 'SAML': a POST request to 'https://bryster-dev-ed.my.salesforce.com/app/salesforce/exk148iq1b8W58N5K697/sso/saml' and a POST request to 'https://bryster-dev-ed.my.salesforce.com/?so=00Df400000m6uY'. The requests are color-coded by protocol: blue for POST and green for GET. The 'SAML' tab is currently active. At the bottom of the tool, it says '131 requests received (98 hidden)'.

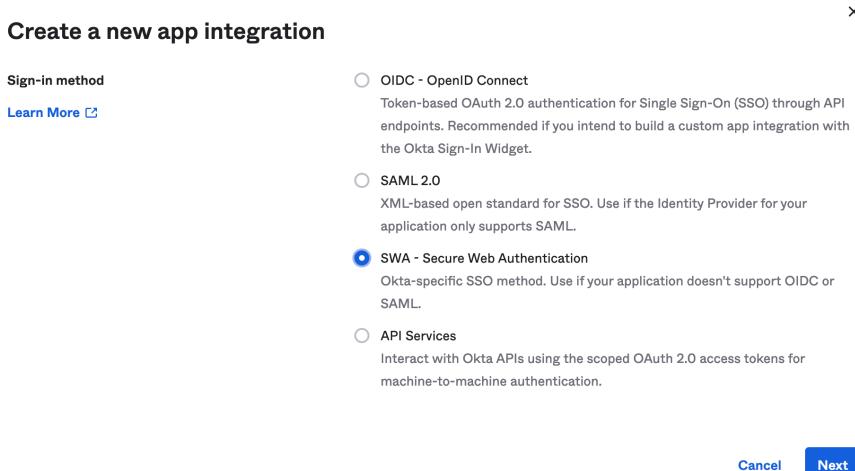
16. You can now see two SAML labels (*one for the **SAML Request** and the other for the **SAML Response***). Review both.
17. Use the **Export** option to save the web traffic flow.
18. Capture and review another SAML assertion from an application of your choice.

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

Objective	To configure Applications using the Application Integration Wizard (AIW)
Procedures	<ul style="list-style-type: none"> Configure a SWA application using the AIW – LinkedIn Configure a SAML application using the AIW – Salesforce (metadata file)
Duration	20-30 minutes

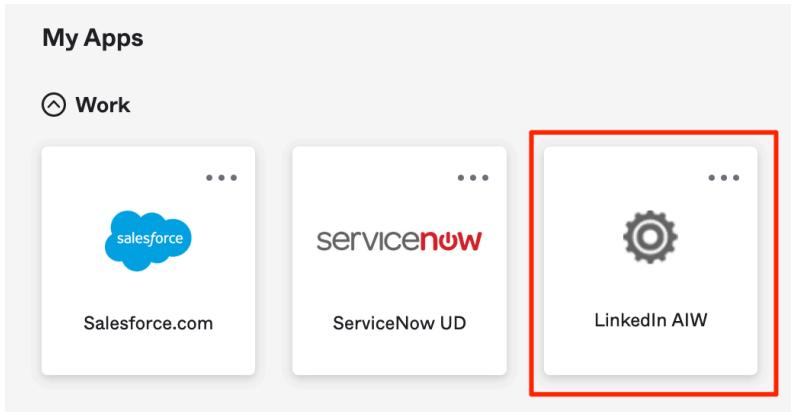
1.1 - Configure LinkedIn using the Application Integration Wizard

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**.

The screenshot shows a 'Sign In To App' page for LinkedIn AIW. At the top is a placeholder icon with a gear. Below it is a text instruction: 'Enter your username and password for LinkedIn AIW. If you don't have one, please create an account on LinkedIn AIW or contact your administrator.' The 'Username' field is filled with 'bryan@bryly.net' and has a blue outline, indicating it is selected. The 'Password' field contains several dots and has a smaller blue outline. A blue 'Sign in' button is at the bottom right.

Sign In To App

Enter your username and password for LinkedIn AIW. If you don't have one, please create an account on LinkedIn AIW or contact your administrator.

Username

bryan@bryly.net

Password

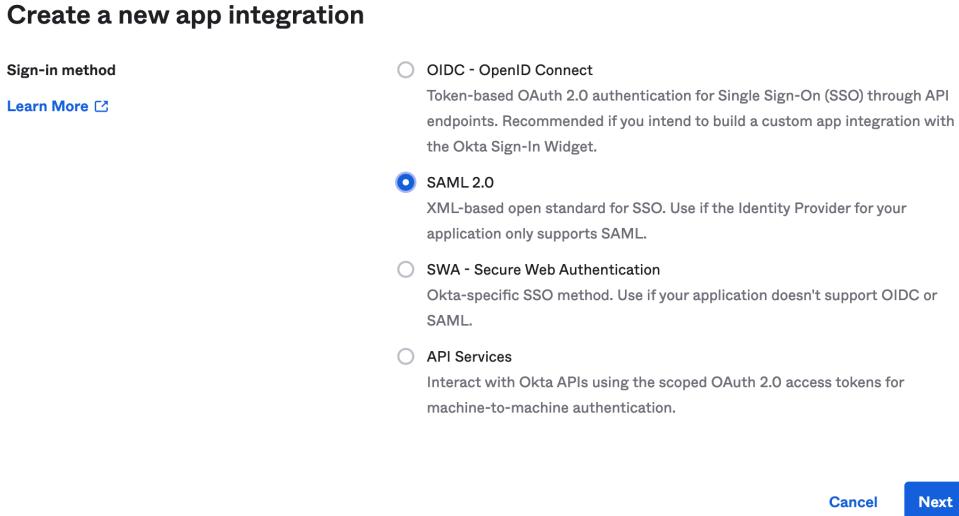
.....

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**.

The screenshot shows the 'Create SAML Integration' wizard. It has two tabs: 'General Settings' (selected) and 'Configure SAML'. In the 'General Settings' tab, the 'App name' field contains 'Salesforce SAML 2.0 AIW'. Below it is an 'App logo (optional)' section with a placeholder box and upload/download icons. Under 'App visibility', there are two checkboxes: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile app'. At the bottom are 'Cancel' and 'Next' buttons.

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

A SAML Settings

General

Single sign on URL ? More

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

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**.

Create SAML Integration

1 General Settings 2 Configure SAML

3 Help Okta Support understand how you configured this application

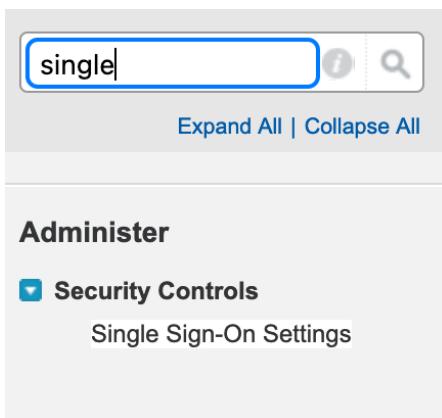
Are you a customer or partner? I'm an Okta customer adding an internal app I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type This is an internal app that we have created

[Previous](#) [Finish](#)

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**.

SAML Single Sign-On Settings		
	New	New from Metadata File
Action	Name	SAML Version
		Issuer

13. Choose the metadata file you saved earlier and click **Create**.

14. Add **SAML_AIW** as the Name and API Name and click **Save**.

SAML Single Sign-On Settings

[Help for this Page](#)

		Save	Save & New	Cancel
Name	<input type="text" value="www"/>			
SAML Version	2.0			
Issuer	<input type="text" value="http://www.okta.com/exk1654"/>			
Identity Provider Certificate	<input type="button" value="Browse..."/> No file selected.			
Request Signing Certificate	<input type="text" value="SelfSignedCert_19May2022_182903"/>			
Request Signature Method	<input type="text" value="RSA-SHA256"/>			
Assertion Decryption Certificate	<input type="text" value="Assertion not encrypted"/>			
SAML Identity Type	<input checked="" type="radio"/> Assertion contains the User's Salesforce username <input type="radio"/> Assertion contains the Federation ID from the User object <input type="radio"/> Assertion contains the User ID from the User object			
SAML Identity Location	<input checked="" type="radio"/> Identity is in the NameIdentifier element of the Subject statement <input type="radio"/> Identity is in an Attribute element			
Service Provider Initiated Request Binding	<input type="radio"/> HTTP POST <input checked="" type="radio"/> HTTP Redirect			
Warning: The metadata file specifies multiple bindings for the login URL. <input type="text" value="https://cs-bloom.okta.com/app/cs-bloom_salesforcesaml20aiw_1/exk1654vxaR"/>				
Identity Provider Login URL	<input type="text"/>			
Custom Logout URL	<input type="text"/>			
Custom Error URL	<input type="text"/>			
Single Logout Enabled	<input type="checkbox"/>			

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.

A SAML Settings

General

Single sign on URL

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

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.

Assign Salesforce SAML 2.0 AIW to People

User Name

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

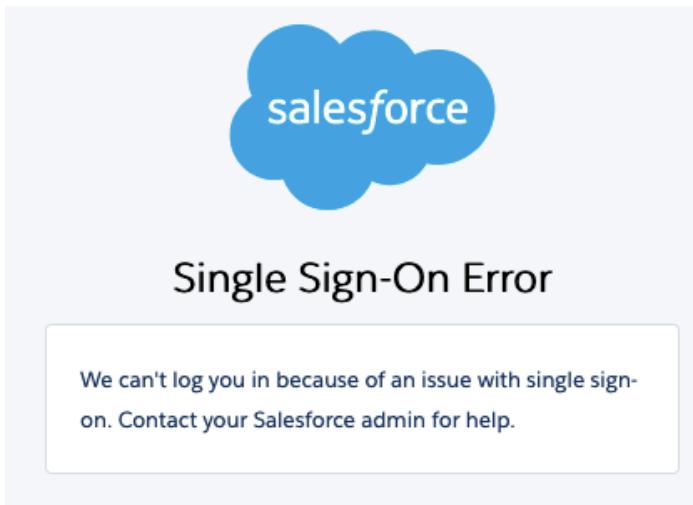
27. Click **Done**.

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	<ul style="list-style-type: none">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*.

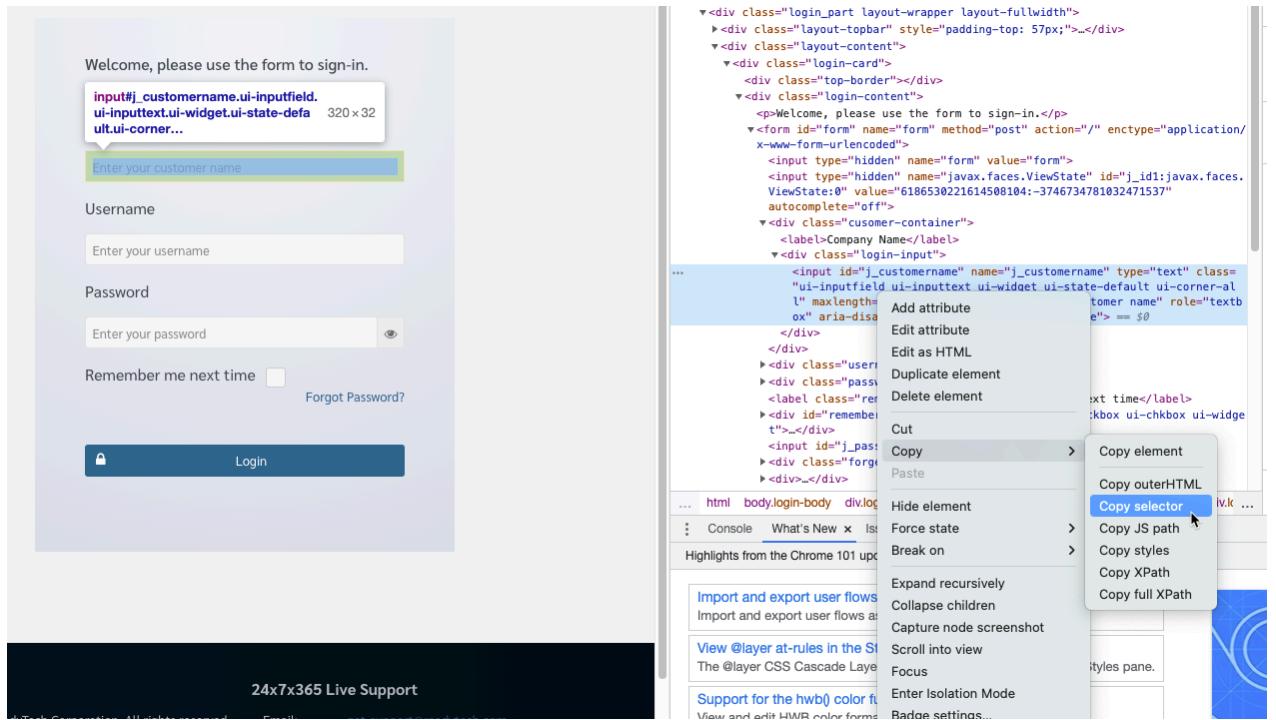
A screenshot of the Okta search interface. The search bar at the top contains the text "template". Below the search bar, there is a "POPULAR SEARCHES" section with links to "Bookmark App", "SCIM 2.0 Test App", "Okta Org2Org", and "Template App". The main search results list shows four items: "Template App" (selected), "Template Frame Plugin App", "Template Plugin App", and "Template WS-Fed". Each item has a gear icon and the text "SWA" below it. A "See All Results →" link is located at the bottom right of the list.

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

A screenshot of a login form. At the top, it says "Welcome, please use the form to sign-in.". The form includes fields for "Company Name" (with placeholder "Enter your customer name"), "Username" (with placeholder "Enter your username"), and "Password" (with placeholder "Enter your password" and an eye icon). Below the password field is a "Remember me next time" checkbox and a "Forgot Password?" link. At the bottom is a blue "Login" button with a lock icon.

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:

General settings· Required

Application label	Enter Ready Tech Template Plugin App 3 Fields
	This label displays under the app on your home page
URL	https://admin.readytech.com/
	The URL of the login page for this app
Username parameter	#j_username
	Name of the username parameter in the login form
Password parameter	#password
	Name of the password parameter in the login form
Optional parameter name	#j_customername
	Name of the optional parameter in the login form
Optional parameter value	Okta
	Name of the optional value in the login form
Optional parameter name	Login
	Name of the optional parameter in the login form
Optional parameter value	#login > span.ui-button-text.ui-c

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.

Welcome, please use the form to sign-in.

! The company name, username or password you have entered is invalid.
Please try again.

Company Name

Username

Password

 • eye

Remember me next time

[Forgot Password?](#)

🔒 Login

Lab 1-11: Configure the Application Approval Workflow.

Objective	To configure the Application Approval Workflow.
Procedures	<ul style="list-style-type: none"> Configure Self-Service for Salesforce. Submit and Approve Requests. Review Application Access Reports
Duration	15-20 minutes

1.1 - Configure Self-Service for Salesforce

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

Add group

Name	<input type="text" value="Approval Group"/>
Description (optional)	<input type="text" value="All approvers"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

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

User App Requests	<input type="button" value="Cancel"/>
App Catalog Settings	<input checked="" type="checkbox"/> Allow users to add org-managed apps <input checked="" type="checkbox"/> Allow users to add personal apps <input checked="" type="checkbox"/> Allow users to email "Technical Contact" to request an app
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

- Click **Save**.
- Navigate to **Applications**.

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

The screenshot shows the Okta Assignments page. At the top, there is a search bar labeled "Search..." and a dropdown menu set to "People". Below this, there is a table with three rows, each labeled "Individual". To the right of each row are edit ("pencil") and delete ("X") icons. To the right of the table, there are two sections: "REPORTS" containing "Current Assignments" and "Recent Unassignments", and "SELF SERVICE" containing "Requests" (set to "Disabled") and "Approval" (set to "-"). A red box highlights the "Edit" button located within the "SELF SERVICE" section.

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).

Salesforce.com - Self Service

Requests

Allow users to request app

No

Yes

Note for
requester (optional)

Please provide your reason.

473 characters remaining

Approval

Approval

Not Required

Required

Send app requests to

Step		Approver	Entitlements ?	Groups ▾
1		<input checked="" type="radio"/> Approval Group	Write	

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

If request is approved	<div style="border: 1px solid #ccc; padding: 10px; background-color: #fff;"> <div style="background-color: #2e7131; color: white; padding: 5px 10px; border-radius: 5px; display: inline-block;"> ✓ </div> <p>Assign the app and provision an account according to your provisioning options.</p> <hr/> <p><input checked="" type="checkbox"/> Send email to requester <input type="checkbox"/> Send email to approvers <input type="checkbox"/> Send email to others...</p> </div>
<hr/>	
If request is denied	<p><input checked="" type="checkbox"/> Send email to requester <input type="checkbox"/> Send email to approvers <input type="checkbox"/> Send email to others...</p>
<hr/>	
Approver must respond within	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">1 Week</div>
<hr/>	
If request expires	<p><input checked="" type="checkbox"/> Send email to requester <input type="checkbox"/> Send email to approvers <input type="checkbox"/> Send email to others...</p>
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block; margin-right: 10px;">Save</div> <div style="display: inline-block;">Cancel</div>	

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

Available Apps

The apps shown below are currently configured for users to request. To add an app to the list, go to the app's "Assignments" tab and configure "Self Service".

App	Approval
 Salesforce.com	On

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.

The screenshot shows the Okta App Catalog interface. On the left, there's a sidebar with options like 'My Apps', 'Work', 'Add section', 'Notifications' (with 1 notification), and 'Add apps'. The 'Add apps' option is highlighted with a grey background. The main area is titled 'App Catalog' with the sub-instruction 'Add apps to your dashboard'. It features a search bar labeled 'Search the app catalog', a filter dropdown set to 'Apps managed by Accelerated Onboarding', and a card for 'Salesforce.com' with its logo and name. A blue 'Request' button is located on the right side of the card.

20. Click Request.

21. Provide the necessary details. Click Request App.

The screenshot shows a 'Request Salesforce.com' dialog box. At the top, it says 'Request Salesforce.com'. Below that, it states 'Salesforce.com requires approval from your admin before it can be added to your apps.' A note from the admin says 'Note from your Admin: Please provide your reason.' A large text area for comments is present, with the placeholder 'Enter anything you want to mention to the approver(s)...'. It also shows 'Comments (Maximum 1000 characters)' and 'Optional'. A character counter indicates '1000 characters remaining'. At the bottom are 'Cancel' and 'Request app' buttons.

22. The application request has been sent.

The screenshot shows the App Catalog again, with the 'Add apps' button still highlighted. The 'Salesforce.com' card is now shown with a green checkmark next to the word 'Requested'.

23. The approvers will receive an email notification. Open the message.

24. Click the **Approval Link**.



Hi Bryan,

Jae Test has requested access to Salesforce.com. Approval is required from a member of Approval Group.

"" -Jae

Click the following link to approve or deny this request:

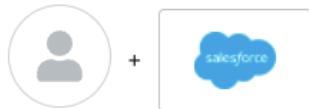
[Approval Link](#)

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

A screenshot of the Okta Tasks page. At the top left is the word "Tasks". To the right is a dropdown menu showing "Pending" with a downward arrow. Below this, there is a list of tasks. The first task is titled "Salesforce.com Access Request" and has the due date "May 24th" to its right. Below the title, it says "Jae-test@atko.email has requested access to Salesforce.com". At the bottom of this card, it says "Expires in 7 days".

Task	Due Date
Salesforce.com Access Request Jae-test@atko.email has requested access to Salesforce.com Expires in 7 days	May 24th

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



Allow Jae Test to access Salesforce.com?

Salesforce.com User Attributes & Entitlements

Username

Jae-test@bryly.net

Profile URL

Optional

Chatter Free User

Street

Optional

27. (Optional) You can add a comment in the Approval Action section.

28. Click **Approve**.

Request History

- Jae Test requested 11 minutes ago

Approval Action

Optional

Your comments (optional)...

Approve

Deny

29. You will receive a task confirmation.

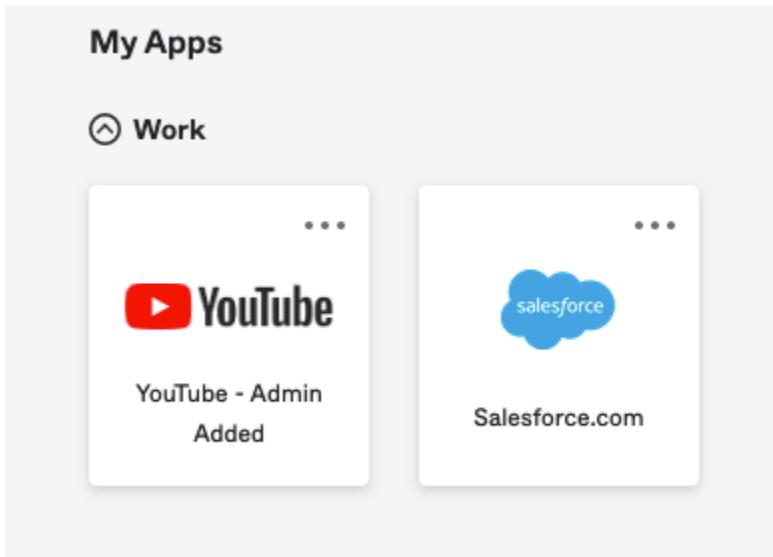


All tasks completed

No pending tasks

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

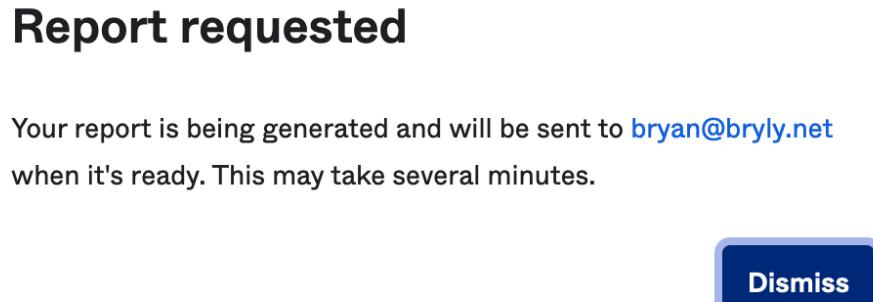
1. Log in to **Okta Admin** dashboard.
2. Navigate to **Reports > Reports**.
3. Scroll down to the **Application Access Audit** section.

A screenshot of the 'Application Access Audit' section in the Okta Admin dashboard. The title 'Application Access Audit' is at the top. Below it are two buttons: 'Current Assignments' and 'Recent Unassignments'.

Column 1	Column 2
Row 1, Col 1	Row 1, Col 2
Row 2, Col 1	Row 2, Col 2

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

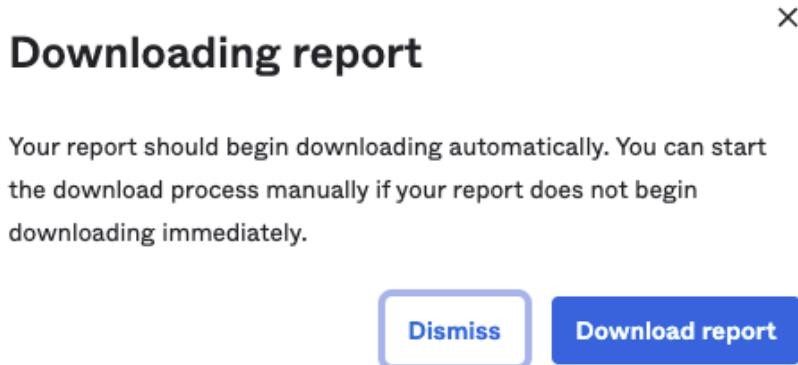
6. Click **Request Report**. You'll be presented with the below message:



7. Click **Dismiss**.
8. Check the email and you should 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	<ul style="list-style-type: none">● 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.

The screenshot shows the Okta Admin dashboard with the sidebar menu expanded. The 'Customizations' section is selected, and the 'Brands' sub-section is highlighted. The main panel displays the 'Brands' configuration page. It features a search bar labeled 'Search brands'. Below it is a table with two columns: 'Logo' and 'Brand'. A row is shown for the subdomain 'okta-dev-55357309', which is identified as an 'Okta subdomain'. The 'okta' logo is displayed next to the subdomain name.

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

Brands /

okta-dev-55357309 dev-55357309.okta.com

This is your default Okta brand. You can customize the theme, but it has limited

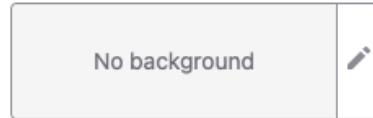
Theme Pages Emails Domains Settings

Logo



Max file size 1MB. Recommended: PNG, landscape orientation, transparent bkgd. Min: 420px x 120px.

Background



Maximum file size 2 MB. Used for Sign-in page, Error page, and emails.

Primary color



Color for primary actions, buttons, text links. 3 and 6 digit hex code values accepted.

Secondary color



Color for background to accent your UI. 3 and 6 digit hex code values accepted.

Favicon



Maximum dimensions 512 x 512. 1:1 ratio.

Save

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**.

okta-dev-55357309 dev-55357309.okta.com

This is your default Okta brand. You can customize the theme, but it has limited

Theme Pages Emails Domains Settings

Logo  A large blue "okta" logo with a small edit icon in the top right corner.	Background  A placeholder image showing a brown textured background with a small edit icon in the bottom right corner. A red arrow points to this edit icon.
Max file size 1MB. Recommended: PNG, landscape orientation, transparent bkgd. Min: 420px x 120px.	Maximum file size 2 MB. Used for Sign-in page, Error page, and emails.
Primary color  A swatch divided into two equal halves: white on the left and a solid blue on the right. The hex code "#1662dd" is displayed below it.	Secondary color  A swatch divided into two equal halves: white on the left and a light gray on the right. The hex code "#ebebed" is displayed below it.

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

Theme Pages Emails Domains Settings

Logo

Max file size 1MB. Recommended: PNG, landscape orientation, transparent bkgd. Min: 420px x 120px.

Background

Maximum file size 2 MB. Used for Sign-in page, Error page, and emails.

Primary color

#1662dd

Color for primary actions, buttons, text links. 3 and 6 digit hex code values accepted.

Secondary color

#ebebed

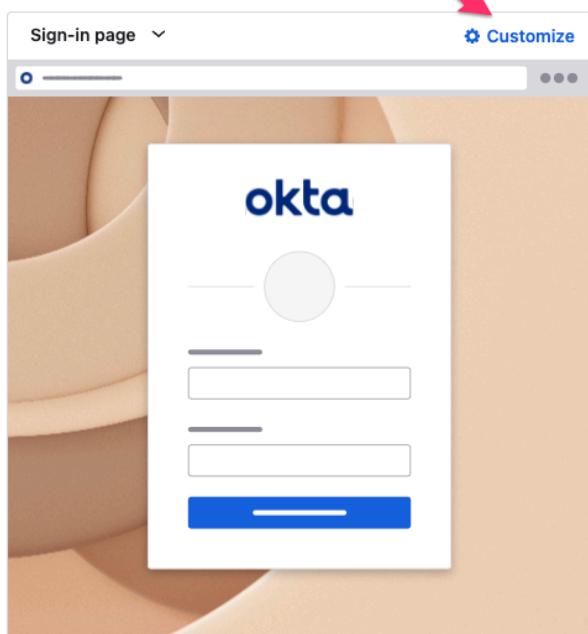
Color for background to accent your UI. 3 and 6 digit hex code values accepted.

Favicon

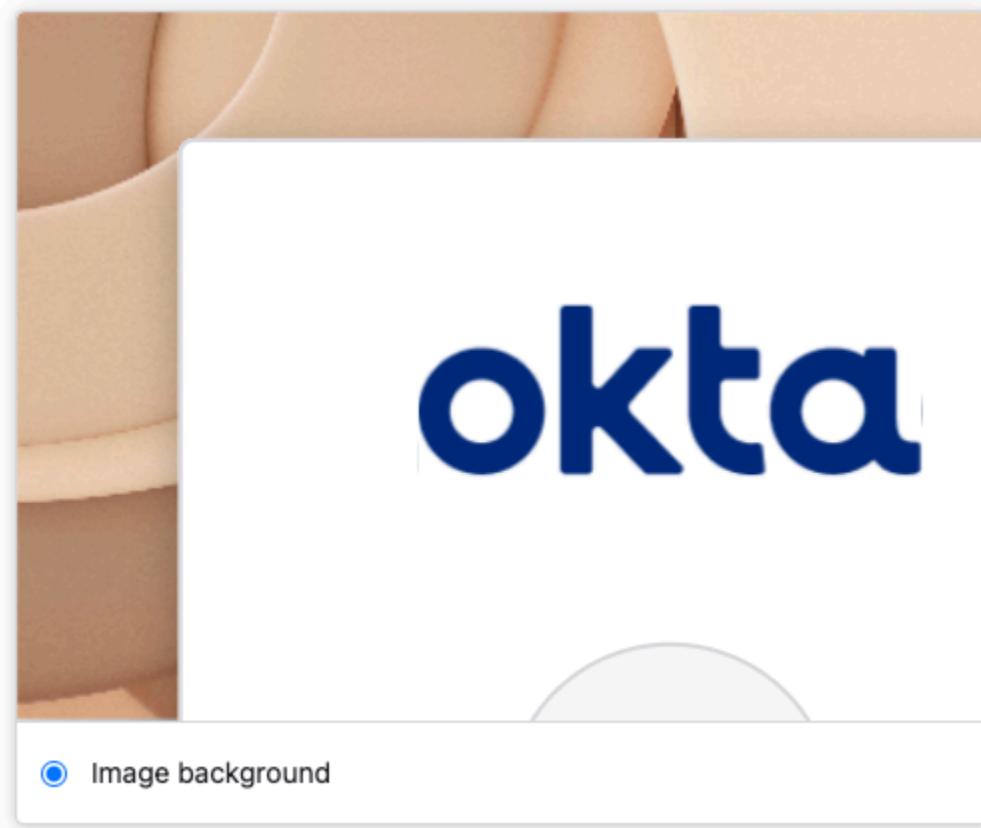
Maximum dimensions 512 x 512, 1:1

Sign-in page ▾

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

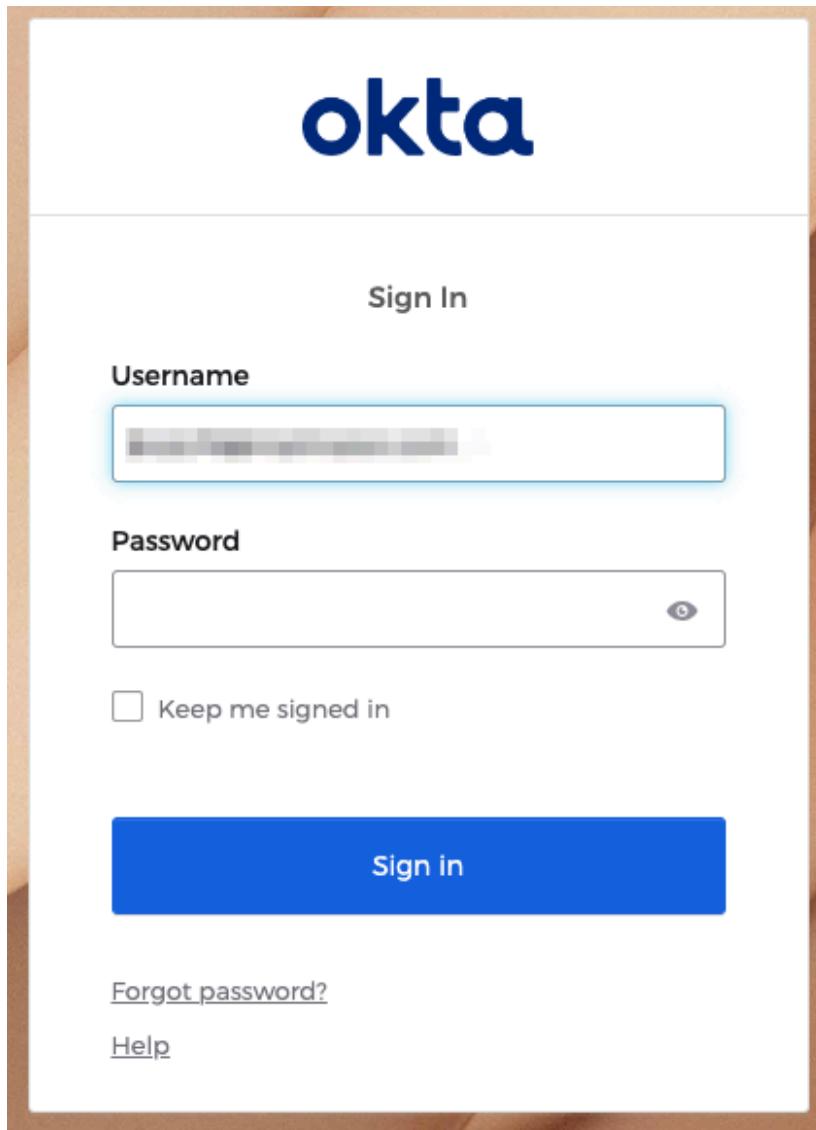
1. From your **Okta Admin** dashboard, navigate to **Customizations > Brands**.
2. Click on your subdomain.
3. In the ‘sign-in page’, click Customize. Then click on the ‘Labels’ tab.
4. Change the ‘Sign In’ heading, ‘Password info tip’ and ‘Okta Help’.

The image contains four separate screenshots of the Okta Admin interface, each showing a different configuration screen for customizing the sign-in page:

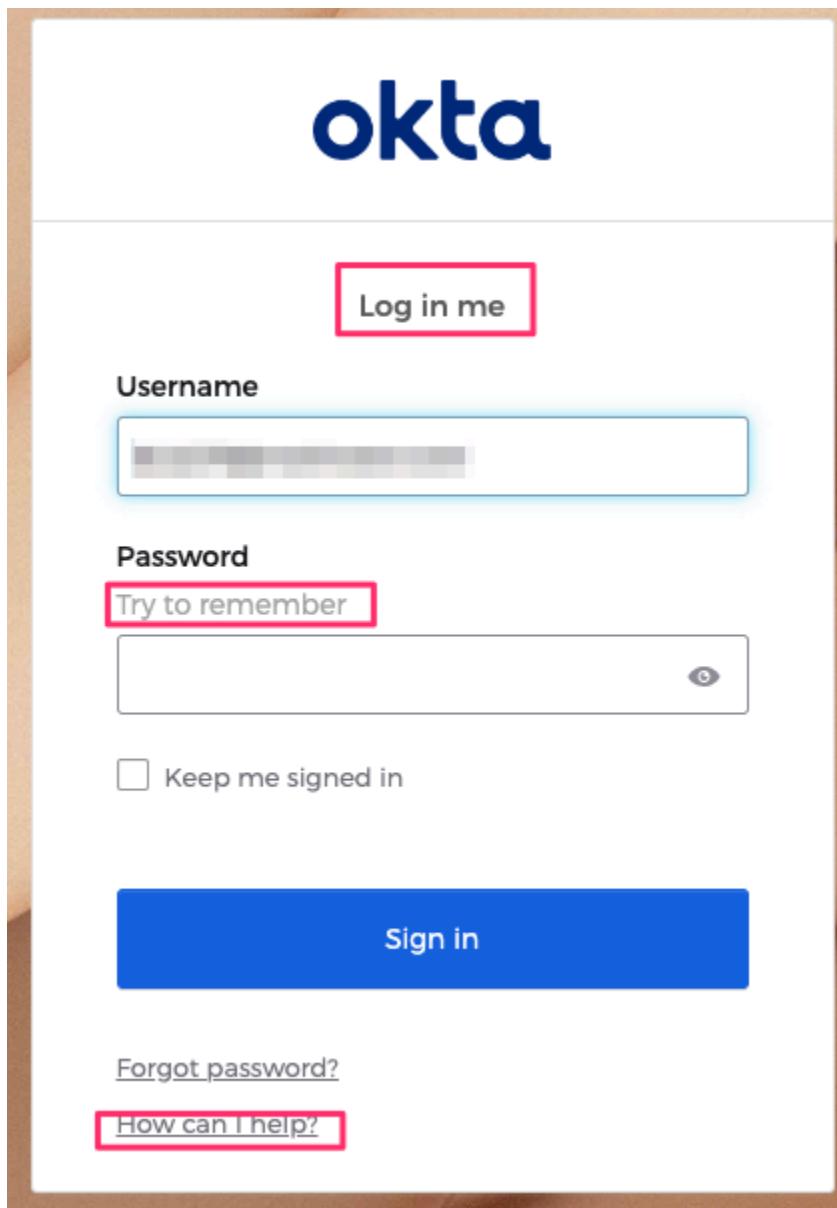
- Heading:** Shows the 'Sign in' label and a 'Log in me' button. Buttons for 'Cancel' and 'Save to draft' are at the top right.
- Username & password fields:** Includes fields for 'Username label' (labeled 'Username'), 'Username info tip' (empty), 'Password label' (labeled 'Password'), 'Password info tip' (labeled 'Try to remember'), and a 'Password visibility toggle' set to 'Enabled'. Buttons for 'Cancel' and 'Save to draft' are at the top right.
- Account recovery flow:** Shows the 'Recovery flow label' set to 'Email or Username'. A blue 'Edit' link is at the top right.
- Customized help links:** Includes fields for 'Forgotten password' (labeled 'Forgot password?'), 'Forgotten password URL' (empty), 'Unlock account' (labeled 'Unlock account?'), 'Unlock account URL' (empty), 'Okta help' (labeled 'How can I help?'), and 'Okta help URL' (empty). Buttons for 'Cancel' and 'Save to draft' are at the top right.

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

Before:



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

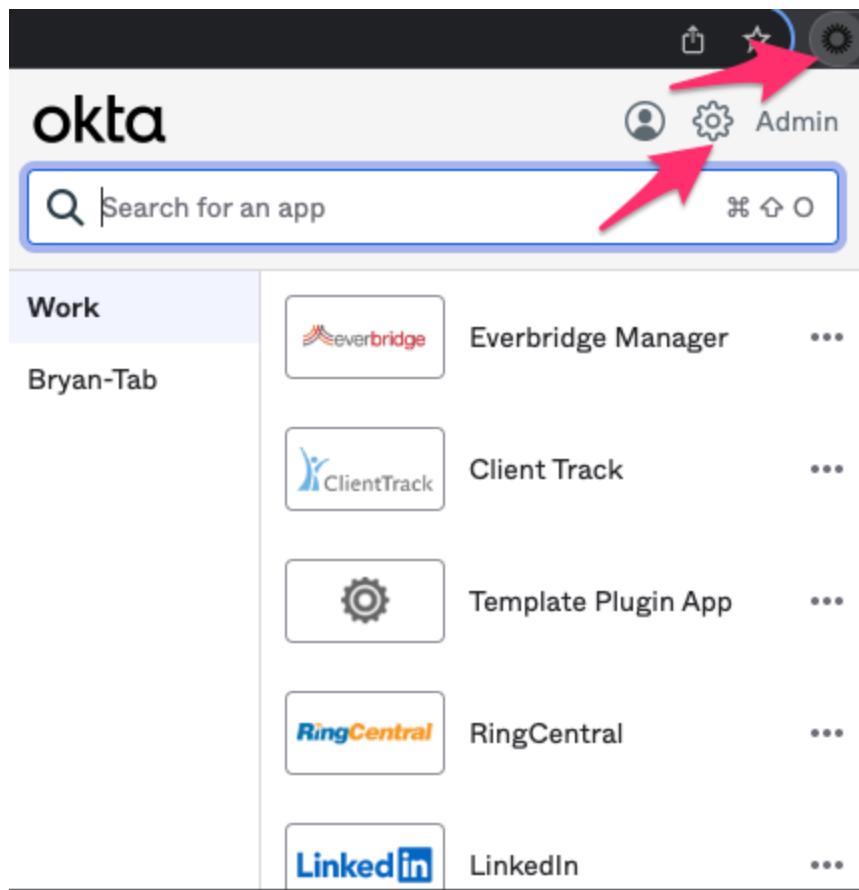
Objective	To configure the Okta Browser plugin
Procedures	<ul style="list-style-type: none">Configure the Okta Browser Plugin (End-User settings).Configure the Okta Browser Plugin (Admin settings).Switch between multiple Okta accounts using the Plugin.
Duration	15-20 minutes

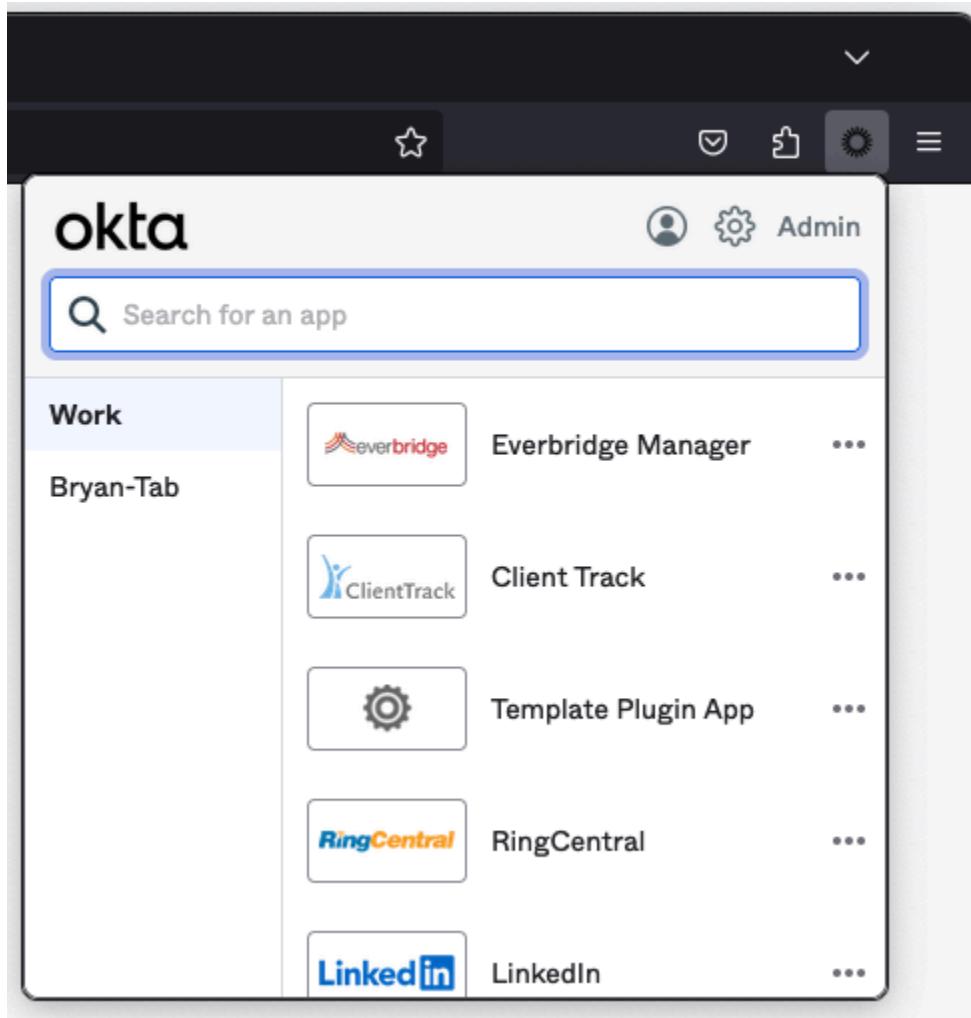
1.1 - Configure the Okta Browser Plugin (End-User settings)

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:



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.

Okta Browser Plugin Settings

Version: V6.23.0.73.108.0

Password management

Recommend strong passwords for apps 

The Okta plugin will recommend strong random passwords when you reset app passwords.

Disable browser password prompts NEW 

When you login to Okta or to an application saved in Okta, your browser is currently asking you to save your credentials.

To disable this, the plugin needs an additional permission to manage privacy settings. Click Allow to disable browser passwords prompts.

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

The screenshot shows a user interface for managing Okta browser plugin settings. At the top, a section titled "Advanced" is visible. Below it, a yellow warning box contains the text: "Warning: Changing these settings can sometimes cause unexpected behavior or compromise the security of your system." Underneath this, there is a setting labeled "Enable Okta plugin logs" with a toggle switch that is currently off (grey). A descriptive text below the switch states: "Displays Okta plugin activity on the developer console. You can also record a log of plugin activity. This setting is intended for troubleshooting." Further down, there is a "Reset Plugin" button, which is highlighted with a blue border. Below the button, a note says: "This button will clear your Okta 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**.

Okta Browser Plugin

The [Okta Browser Plugin](#) enables you to quickly launch apps from any page and automatically signs you into applications that would otherwise require you to manually enter your credentials (e.g., applications that do not support SAML). See [here](#) for more details about Okta browser plugin admin settings.

Hide plugin installation/upgrade messages from end users

Enable Okta toolbar for group

Warn when visiting new organizations [?](#)

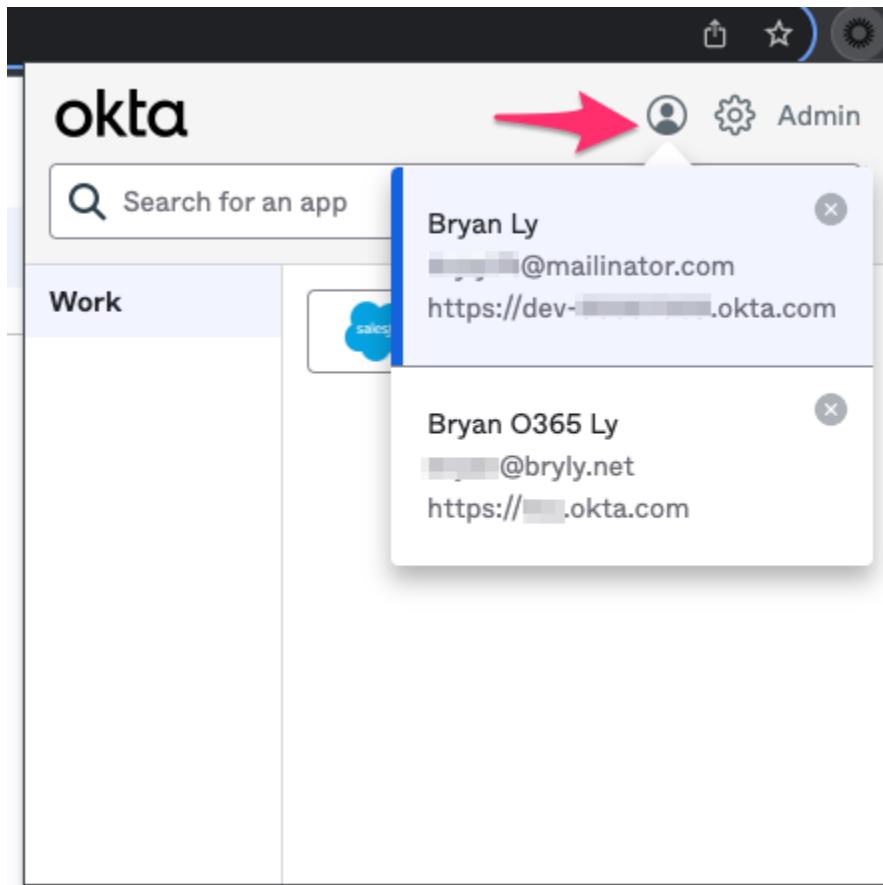
Save

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