Okta-Saleforce Integration

Background

This section aims at providing a detailed description on integrating Okta and Salesforce application and configure SAML for setting up SSO for the users along with configuring provisioning for Salesforce. The purpose of integrating Okta and Salesforce is to allow the users to have Single Sign On setup(SSO) so that the users can access the Salesforce application from Okta in one single login.

The solution around Okta-Saleforce integration is designed to fetch the user information from AD (Active Directory). That is, Okta pulls the user information from AD and sends it to the Salesforce application using the OOTB (Out Of The Box) API to create, delete and update the users and groups.

Prerequisites

1. Have the Okta and AD integration done prior to integrating Okta and Salesforce application.
2. Have an administrator account in Okta to add the Salesforce application.
3. Create an administrator account in Salesforce. You will use this account's username and password to configure the Salesforce app in Okta. When you create an administrator account, Salesforce will provide you with a **token**.

   Note: Every time you reset this account's password, Salesforce will provide you with a new token, and you need to edit the Salesforce app's **Provisioning** settings in Okta using the new password/token as explained in the steps below.

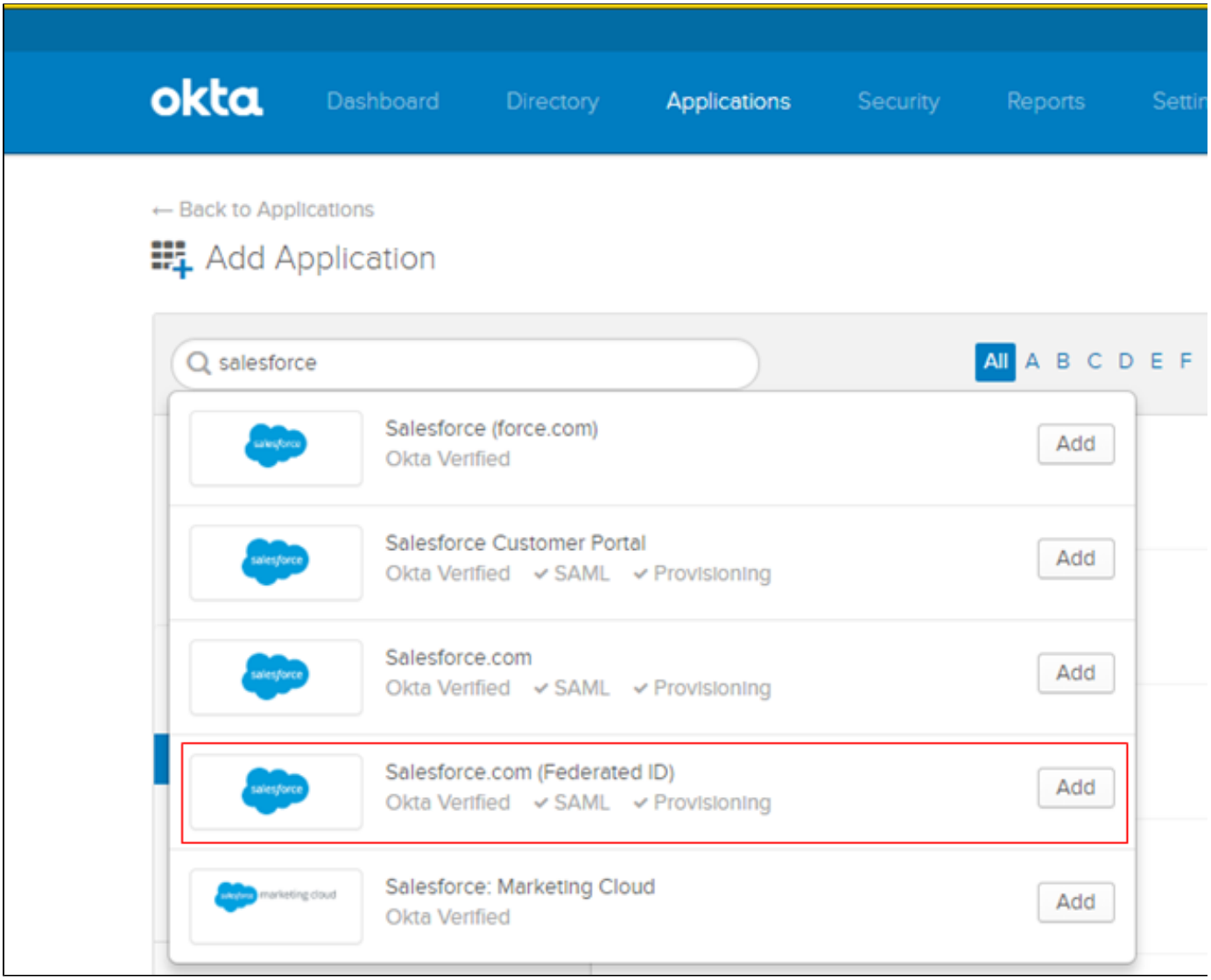
After creating the administrator account is Okta and Salesforce follow the steps below to integrate Okta and Saleforce application.

Configuration Steps

Step 1: Log in into your Okta account to add the Salesforce application. To do this, go to **Applications Add Applications Search for Specific Salesforce App** and click **Add** as shown in the image below.

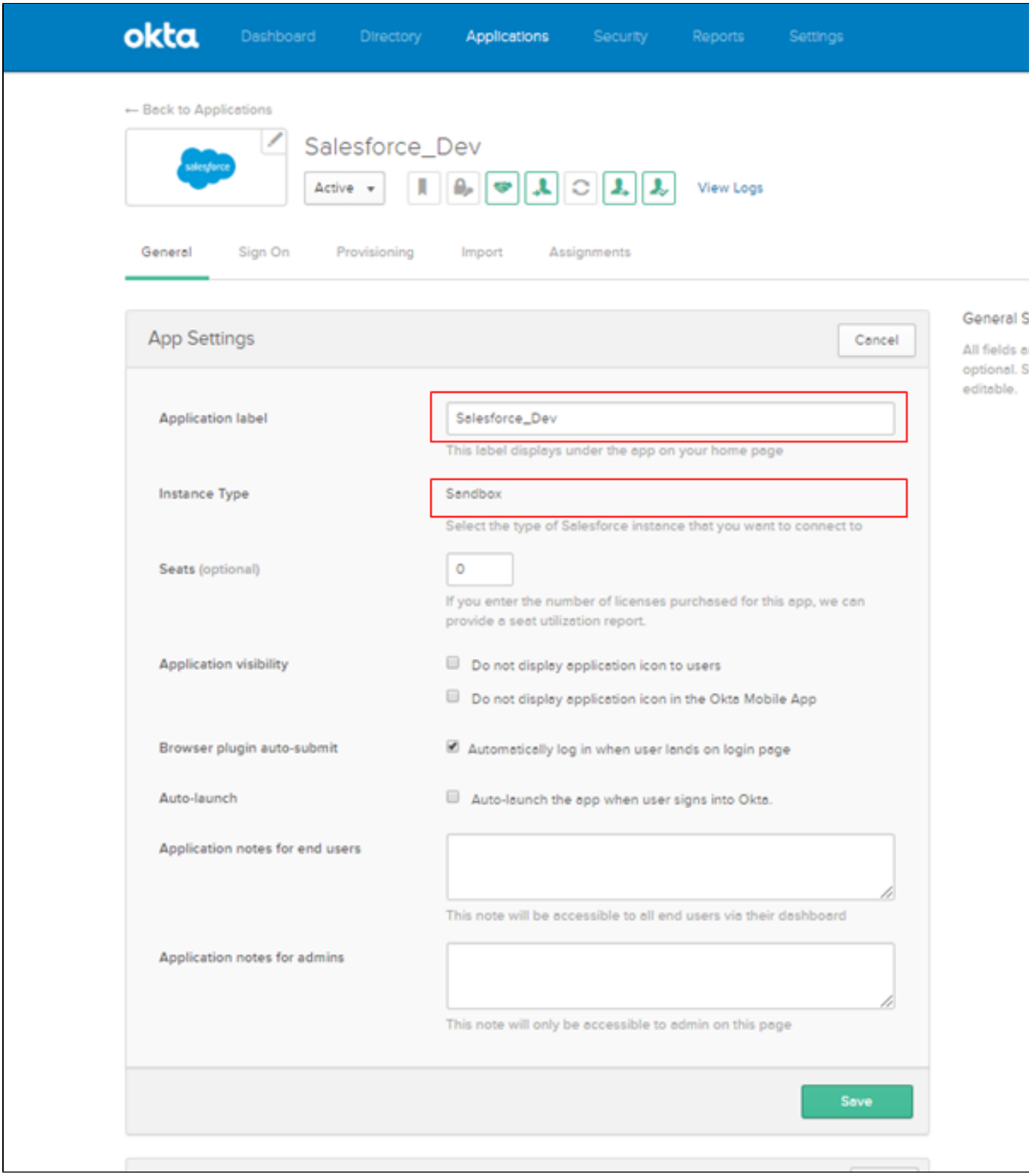
Note : - Depending on the Internal Identity scope, we have selected the Salesforce application with Federated ID as shown below.

- **Federation ID** is a unique username for each user that can be shared across multiple apps. For example, sometimes the **ID** is the user's employee **ID**.



- After adding the application you will be taken to the next page where you will have to set the General app settings such as the "Application Label", "Instance Type" etc. Click edit and Save the changes as shown below.

Note : Select "Sandbox" for the instance type as shown below. Sandbox is selected because it is a copy of production (non-production environment which can be used as an testing environment), it copies all **application** and configuration information to the **sandbox**.



- In the Sign-on options tab select "**SAML 2.0"** as this is what will be configured between Okta and Saleforce for SSO. Leave the "**Login URL"** and "**Custom Salesforce Domain"** blank for now as this will be filled up once the SAML in saleforce is enabled and configured.

Note : - Select "yes" for "Use Fed ID for SAML" option as this is the option we are using to configure in Salesforce.

- **SAML**(Security Assertion Markup Language) is a protocol used for single sign-on into Salesforce application from an identity provider (Okta). It is used to transfer information between Salesforce and Okta. SAML provides authentication and authorization between two entities (Salesforce and Okta).

Add Salesforce.com (Federated ID)

1 General Settings | 2 Sign-On Options | 3 Provisioning | 4 Assign to People

Sign-On Options · Required

SIGN ON METHODS

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

- Secure Web Authentication
- Bookmark-only
- SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

ADVANCED SIGN-ON SETTINGS

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

Use Fed ID for SAML: Yes

Login URL

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

Custom Salesforce domain

Used only for multiple SAML config. In case your custom domain is `acme.my.salesforce.com`, input acme

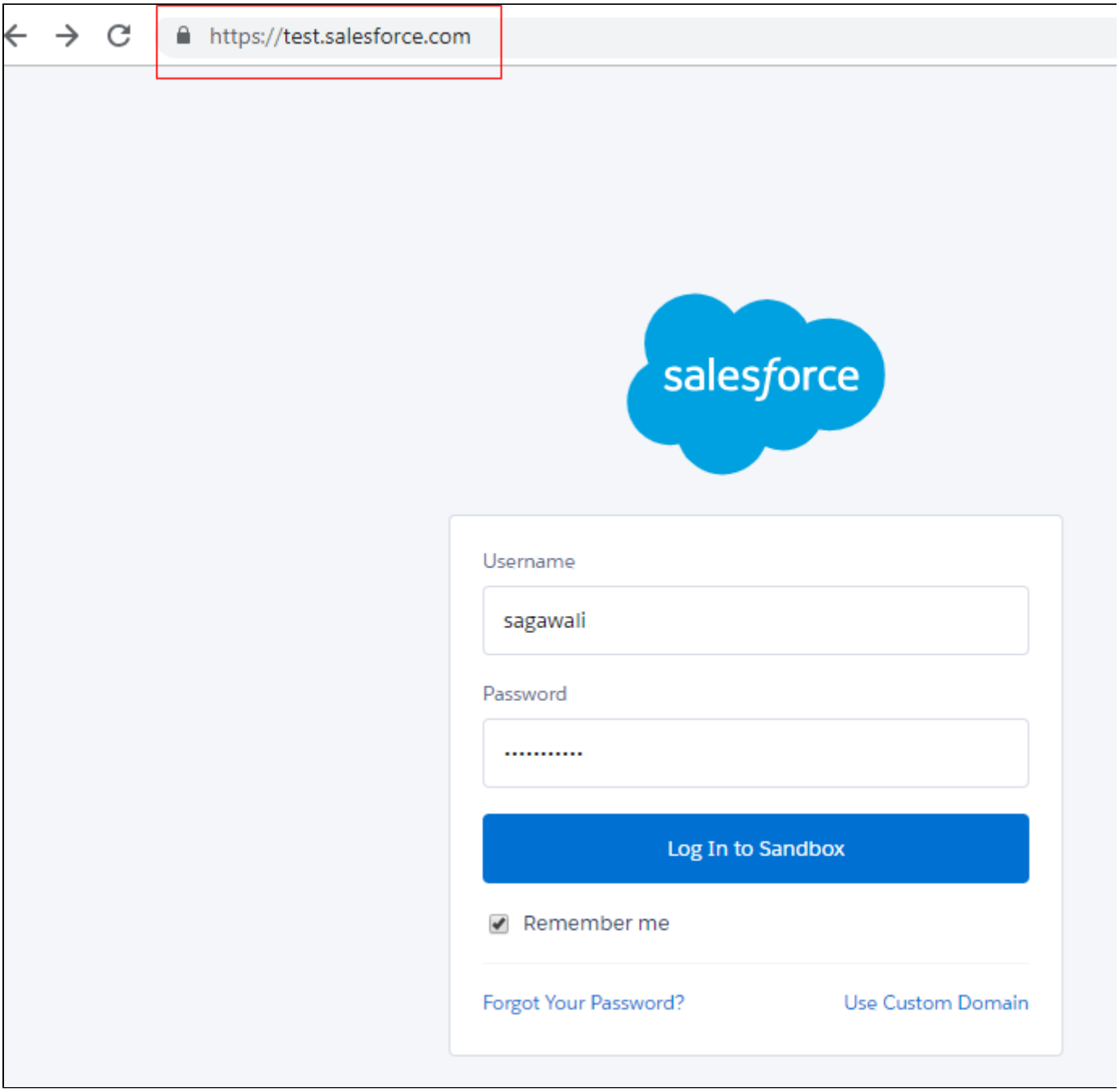
CREDENTIALS DETAILS

Application username format: Okta username

Step 2: Leave the Salesforce app settings in Okta Sign-On Options page and come back to Okta later after creating an Salesforce admin account and configuring SAML in salesforce instance. To do so, follow the steps below.

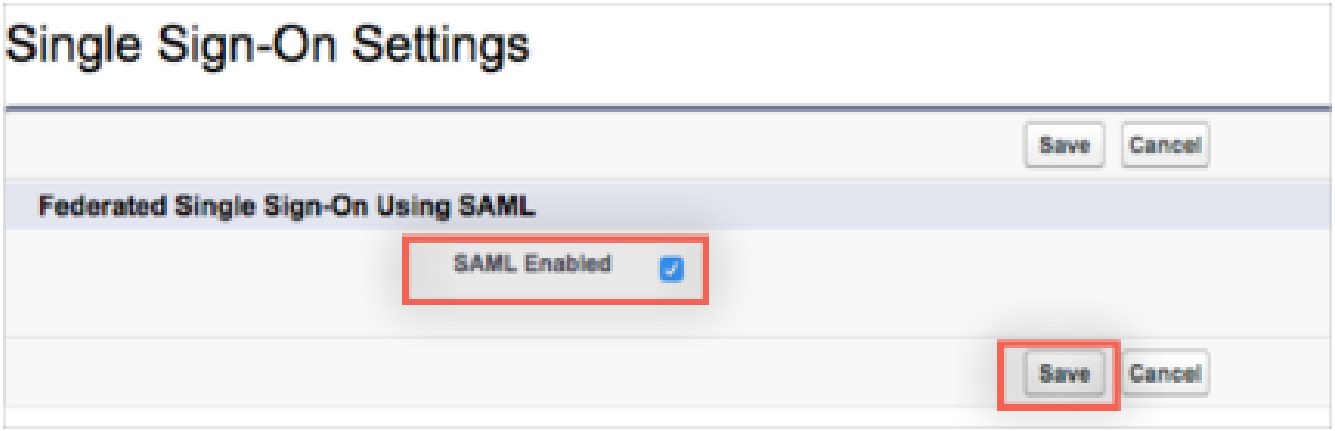
- Create a Salesforce admin account by opening a new browser tab and the Salesforce sandbox URL: https://test.salesforce.com.
- On the Salesforce login page, enter the provided Salesforce credentials and click Log In to Sandbox. You will use this account's username and password to configure the Salesforce app in Okta. When you create an administrator account, Salesforce will provide you with a *token*.

Note: Every time you reset this account's password, Salesforce will provide you with a new token, and you need to edit the Salesforce app's **Provisioning** settings in Okta using the new password/token as described below.

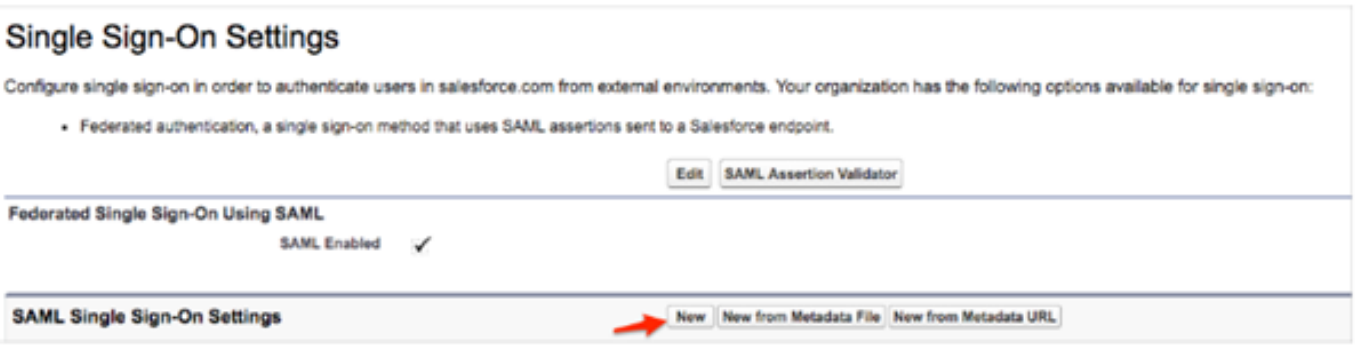


- After creating the account, navigate to **Setup** **Security Controls** **Single Sign-On Settings** as shown below.

- Next, in the Single Sign-On Settings follow the steps shown below to enable SAML in salesforce.
- Click **Edit** to enable the SAML and click **Save.**



- Further, click on "New" tab to add the SAML Single Sign-On settings as shown below.



- Enter the following to add the details in SAML Single Sign-On settings

  Unless otherwise noted, leave the default values as-is.
  - **Name**: Enter a name of your choice. Here we have entered **OktaSSO.**
  - **SAML Version**: Make sure this is set to **2.0**. This should be enabled by default.
  - **Issuer**: Copy and paste the following: **exki9meuyaJCD3SwL0h7**

    *Sign into the Okta Admin dashboard and go to **Sign on options** **Select SAML 2.0** **View set up instructions** to generate the above value to be filled in **Issuer** field.*
  - **Identity Provider Certificate**: Download your Okta Identity Provider Certificate, and then upload it in the **Identity Provider Certificate** field. Download the certificate from : https://cbus-admin.oktapreview.com/admin/org/security/0oai9meuybtn1n2v40h7/cert

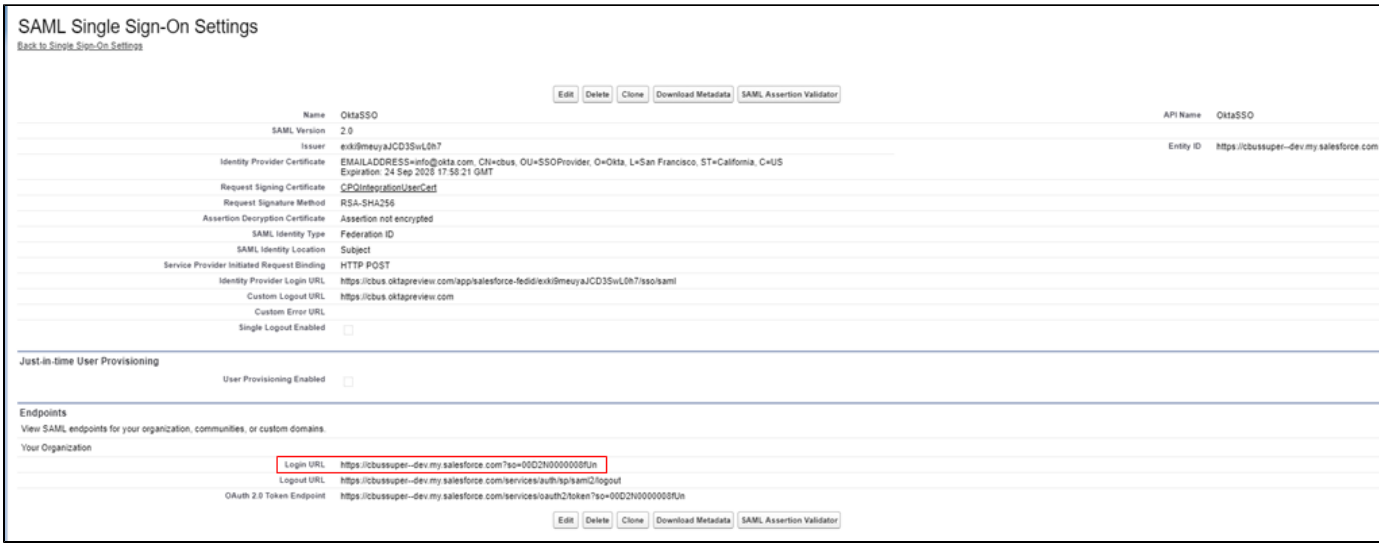
*Sign into the Okta Admin dashboard and go to **Sign on options Select SAML 2.0 View set up instructions** to generate the above value to be filled in **Identity Provider Certificate** field.*

- **Identity Provider Login URL**: Copy and paste the following: https://cbus.oktapreview.com/app/salesforce-fedid/exki9meuyaJCD3SwL0h7/sso/saml

  *Sign into the Okta Admin dashboard and go to **Sign on options Select SAML 2.0 View set up instructions** to generate the above value to be filled in **Identity Provider Login URL** field.*

  Note : This URL will authenticate your users when they attempt to log in directly in 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://cbus.oktapreview.com

  *Sign into the Okta Admin dashboard and go to **Sign on options Select SAML 2.0 View set up instructions** to generate the above value to be filled in **Custom Logout URL** field.*
- **API Name**: Enter an API name of your choice. Here we have entered **OktaSSO**
- **Entity ID**:
  - If you have a custom domain setup, use **https://<customDomain>.my.salesforce.com**.
  - If you do not have a custom domain setup, use https://saml.salesforce.com/
- For **SAML Identity Type**, select **Assertion contains the Federation ID from the User object**.
- For **SAML Identity Location,** select **Identity is in the NameIdentifier element of the Subject Statement (Subject).**
- For **Service Provider Initiated Request Binding,** select **HTTP Post**.
- Click **Save**.
- Copy the**Salesforce Login URL** (Highlighted in the image below) which will appear after clicking **Save.**
- The image below shows the sanpshot of SAML Single Sign-On Settings in Saleforce with all the relevant fields filled.



- SAML is successfully enabled in Salesforce.

- Next, paste the **Login URL :** https://cbussuper--dev.my.salesforce.com?so-00D2N0000008fUn as shown in the image below into the Login URL field of Okta which was left blank in step 1 above..

Settings

Cancel

SIGN ON METHODS

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

- Secure Web Authentication
- Bookmark-only
- SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

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

View Setup Instructions

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

ADVANCED SIGN-ON SETTINGS

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

Use Fed ID for SAML: Yes

Login URL: https://cbussuper--dev.my.salesforce.com?so=00D2N0000008fUn

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

Custom Salesforce domain: cbussuper--dev

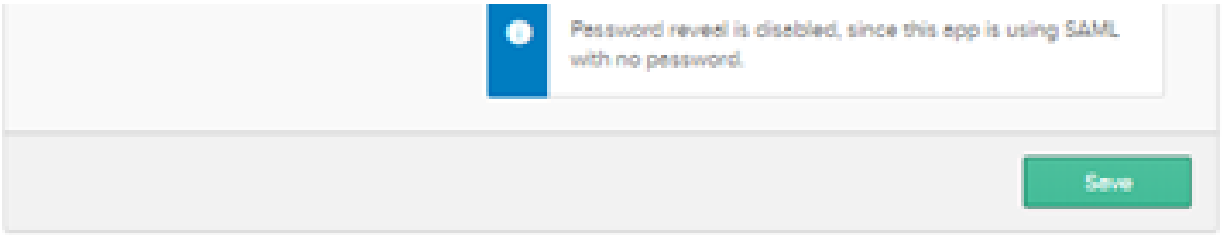
Enter your custom domain. If your domain is acme.my.salesforce.com, enter acme. This field is only required if you are using your custom domain for your Entity Id in Salesforce or if you are using Salesforce Government Cloud.

CREDENTIALS DETAILS

Application username format: Okta username

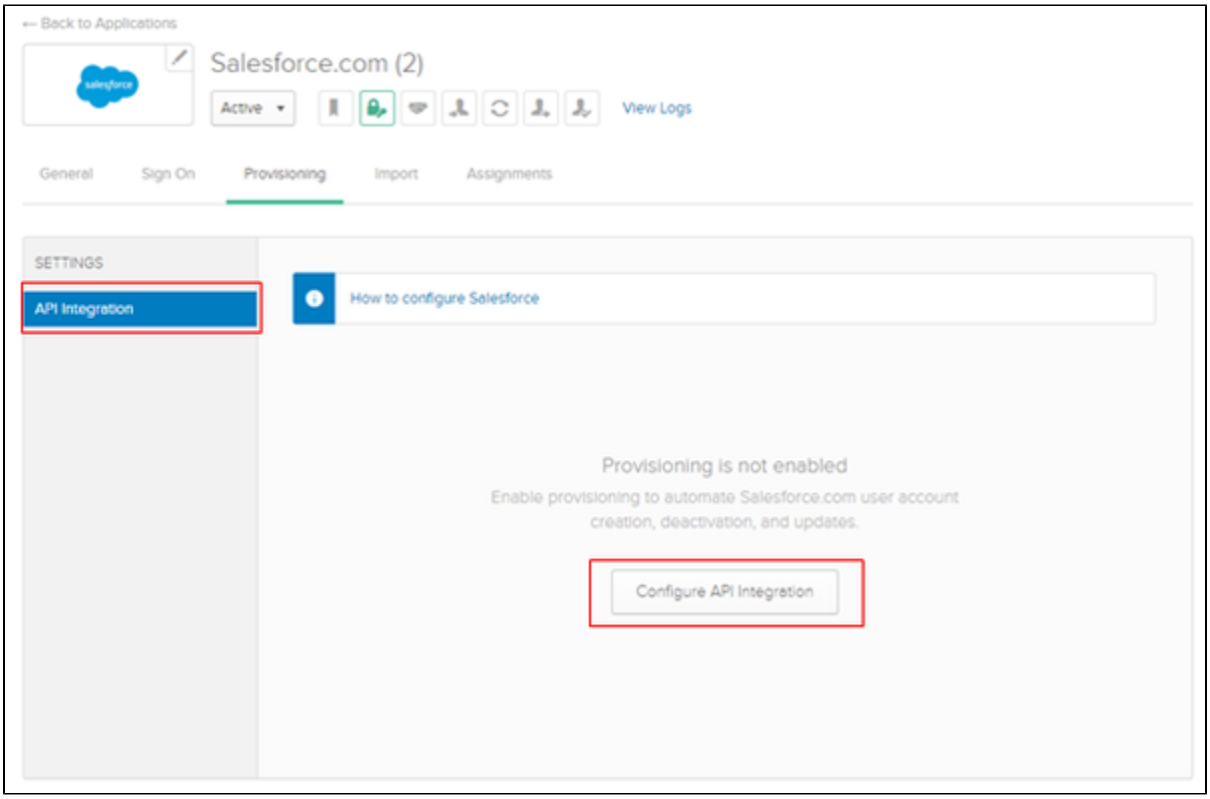
Update application username on: Create and update

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

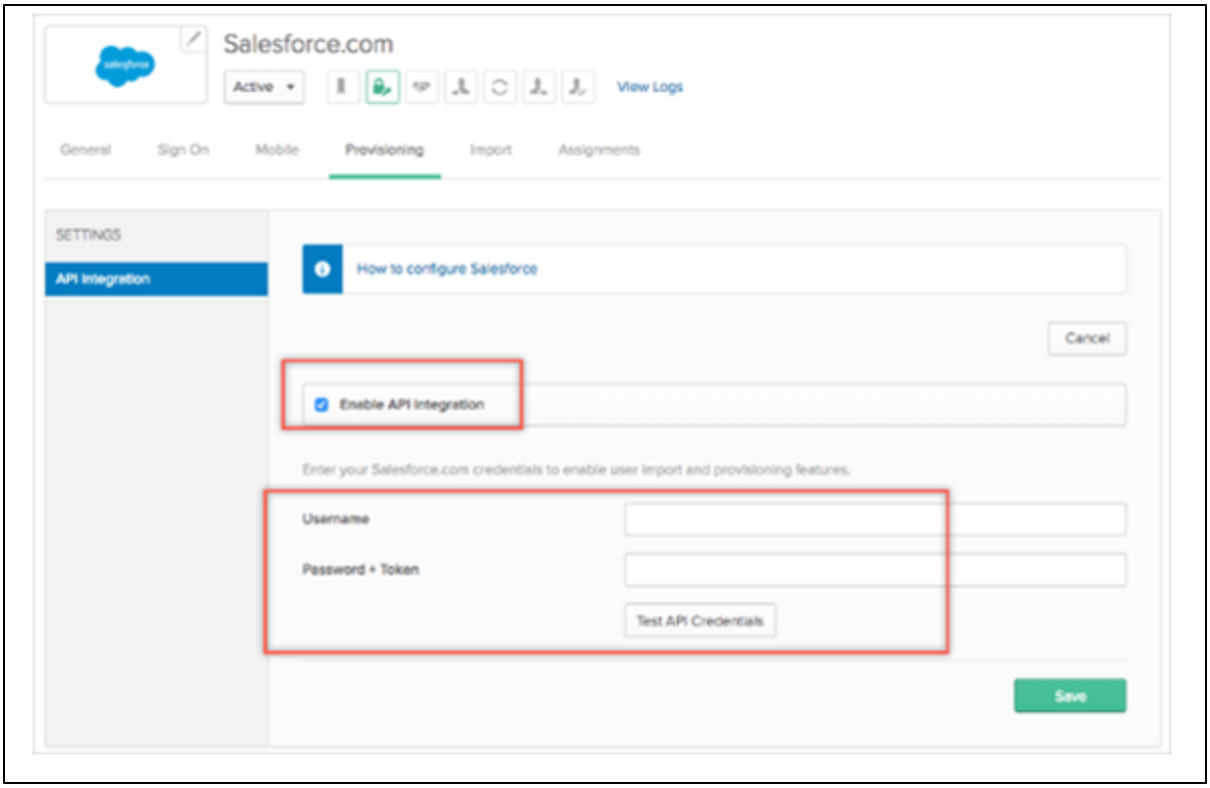


- In Okta, for **Custom Salesforce domain:** If you have a Custom Salesforce domain, such as **site-name.my.salesforce.com**, enter site-name (Here we have entered **Cbussuper--dev**), otherwise leave blank. (Hint: If your Salesforce login URL starts with https://login.salesforce.com , then leave this field blank.)
- Click Save.

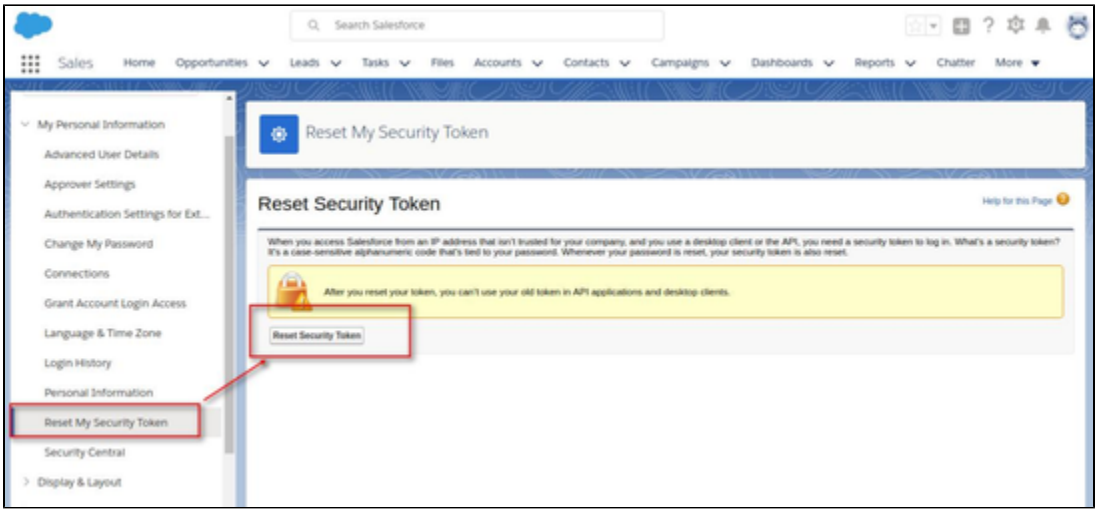
Step 3: Next go to **Provisioning API Integration Configure API Integration** as shown below.



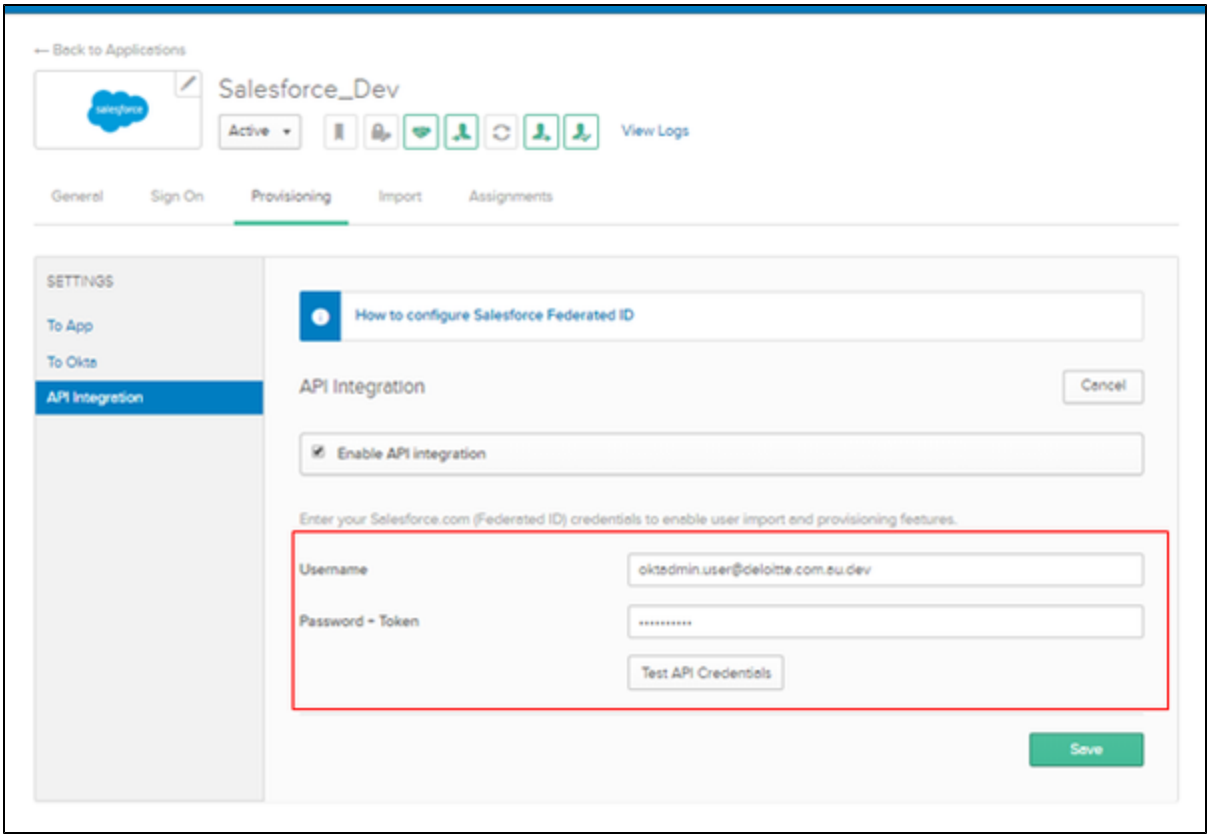
- Check the **Enable API integration** box.



- Enter the **Username**, **Password + Token** associated with your Salesforce Administrator account.
- You can generate or reset a token by logging in into your Salesforce admin account as shown below. The token will be sent to your registered email Id.



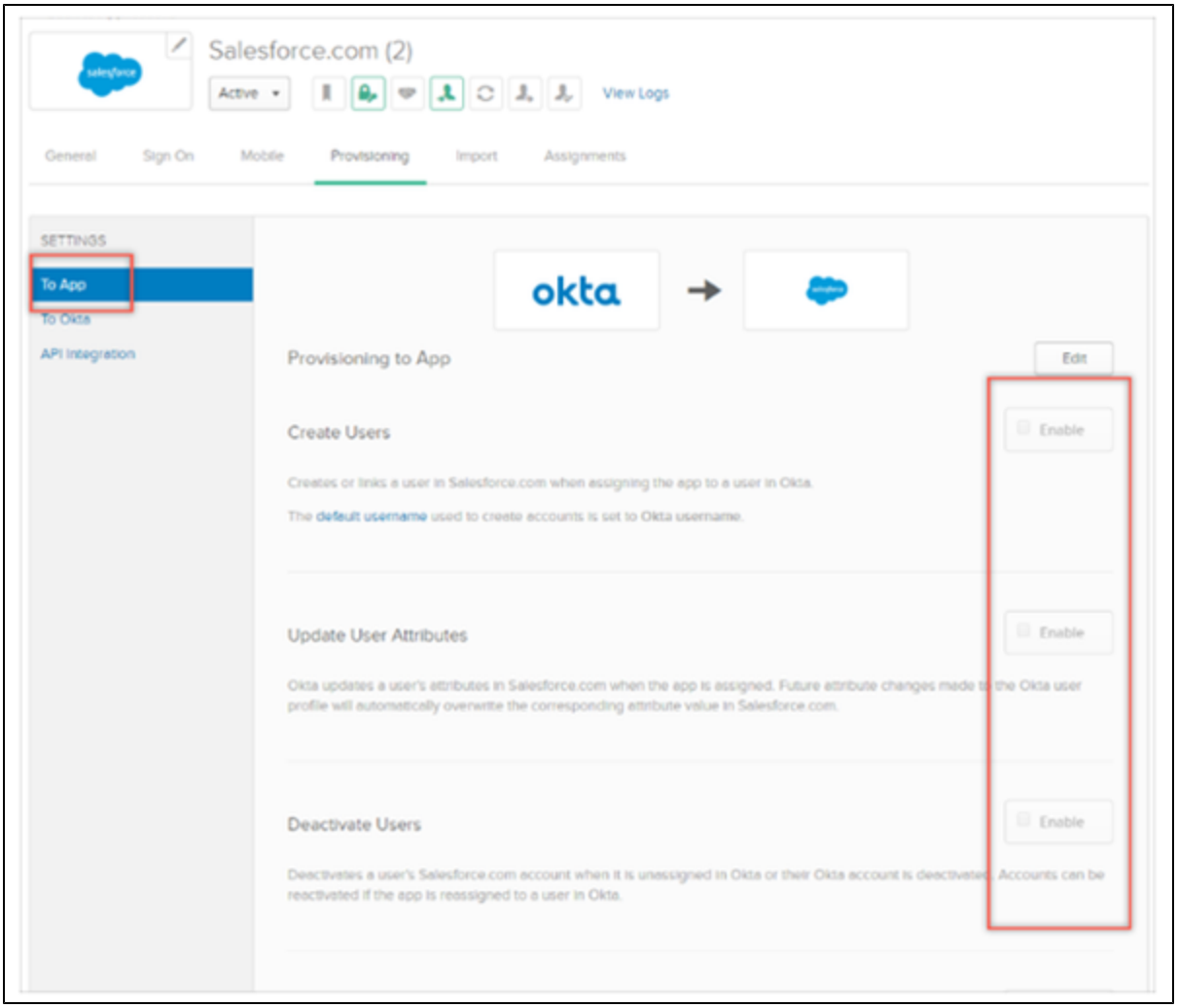
Note: Simply append the token Salesforce provided to you to your password, no spaces or other characters.



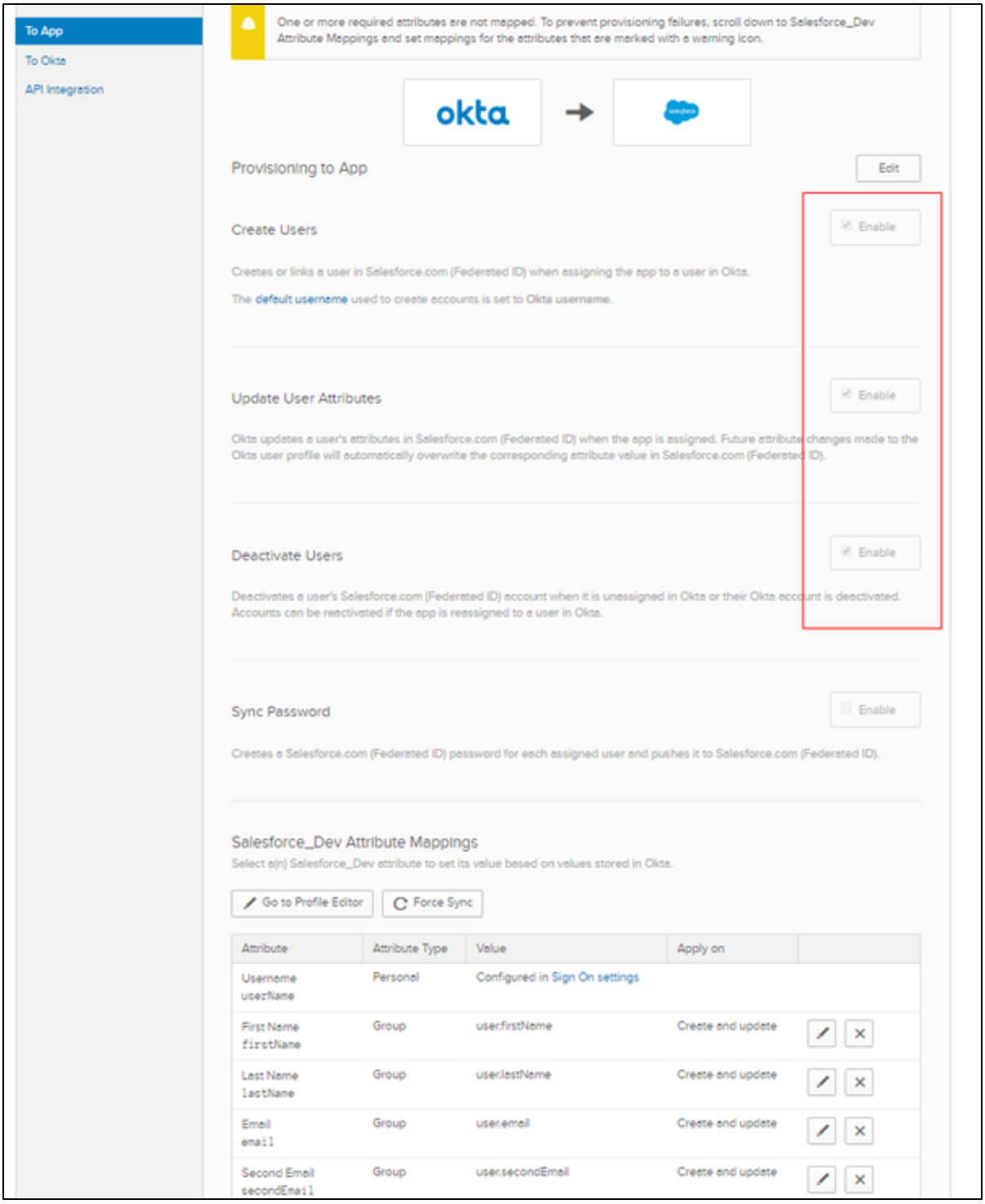
- Next, after entering the username and password click **Test API Credentials**; if successful, a verification message appears at the top of the screen.
- Click save after the API credentials are tested.

- Select **To App** in the left panel, then select the Provisioning features you want to enable:

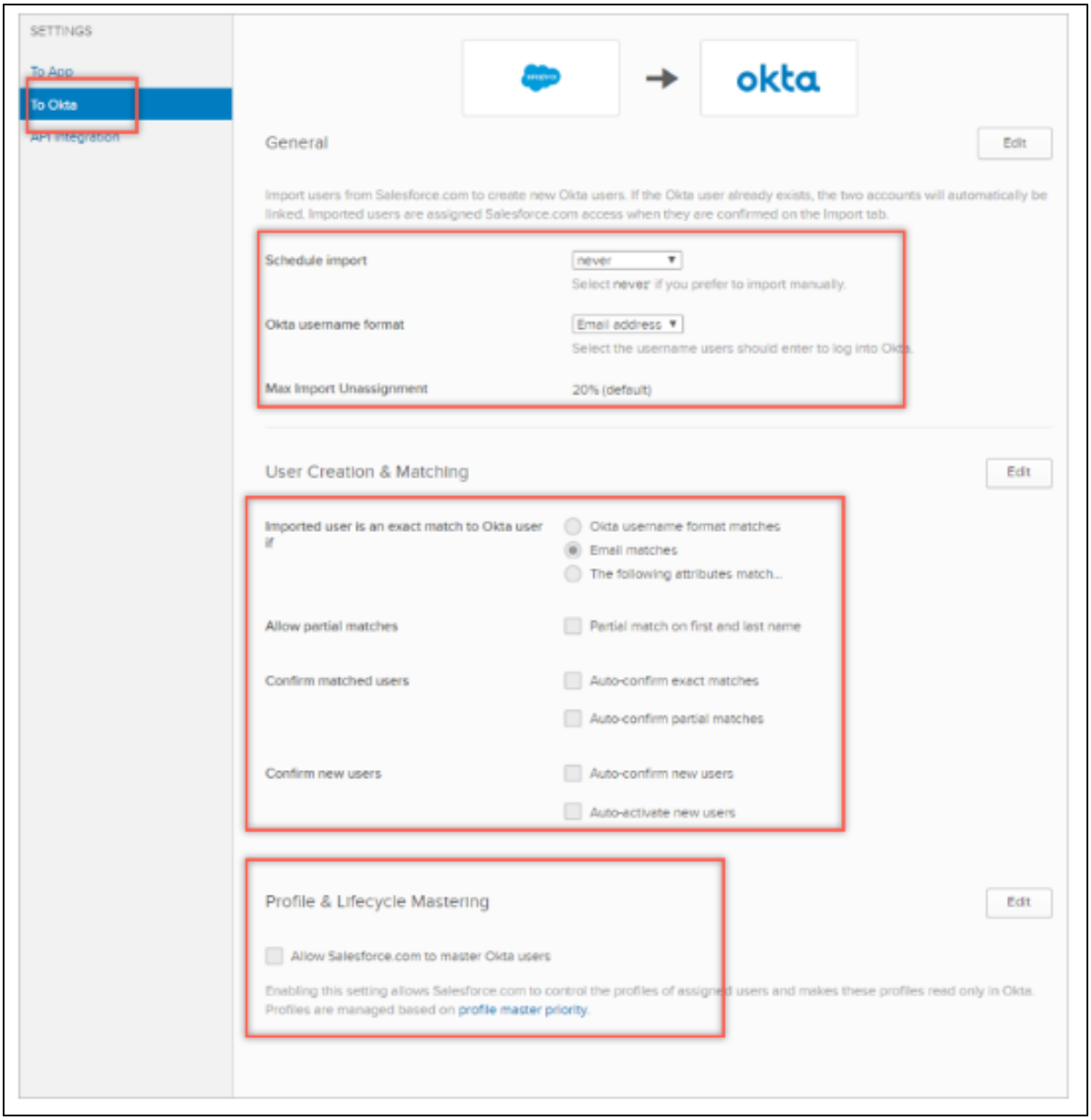
  Note: As part of provisioning each new portal user, Okta creates a new contact in Salesforce associated with the account you specify in the **AccountID** field. This new contact contains the user's name and email address. This contact is necessary because Portal users in Salesforce must be associated with a contact.



- Click edit and enable the features to Create , Update and Deactivate the users as shown below.



- Select **To Okta** in the left panel if you want to configure Salesforce as Profile & Lifecycle Mastering or change Import rule settings:



- Click save
- You can now assign people to the app (if needed) and finish the application setup.
- Okta to Salesforce integration is completed successfully.

Salesforce User Groups, Profile, Roles and Permissions

Employer Services in Salesforce will have the following user groups as mentioned in the 1st column below. Each User group will resolve to 1 Profile, 1 Role and 1+ permission set(s). These groups will be create in Okta and mapped to the roles, profiles and permissions as listed in the table below.

User Group	Profile	Role	Permission Set(s)
ERM Admin	CBUS Standard User	ERM Manager	Advisor Access CBUS Employer Services - ERM Financial Services Cloud Standard FSC Analytics Integration CBUS SME User
ERM Manager	CBUS Standard User	ERM Manager	Advisor Access CBUS Employer Services - ERM Financial Services Cloud Standard FSC Analytics Integration

ERM User	CBUS Standard User	ERM User	Advisor Access CBUS Employer Services - ERM Financial Services Cloud Standard FSC Analytics Integration
BSC Manager	CBUS Standard User	BSC Manager	Advisor Access CBUS Employer Services - ERM Financial Services Cloud Standard FSC Analytics Integration
BSC User	CBUS Standard User	BSC User	Advisor Access CBUS Employer Services - ERM Financial Services Cloud Standard FSC Analytics Integration
BPM User	CBUS Standard User	BPM Manager	TBD
BSM User	CBUS Standard User	BSM User	TBD
Marketing	CBUS Standard User	TBD	TBD
Employer Support Officer	CBUS Standard User	ERM User	Advisor Access CBUS Employer Services - ERM Financial Services Cloud Standard FSC Analytics Integration

Troubleshooting

This section will provide the issues encountered during Salesforce Integration and the related troubleshooting steps.

Appendix

Environment

Environment	Service Account	URL	Email
Dev			
Prod			
SIT			
Test			