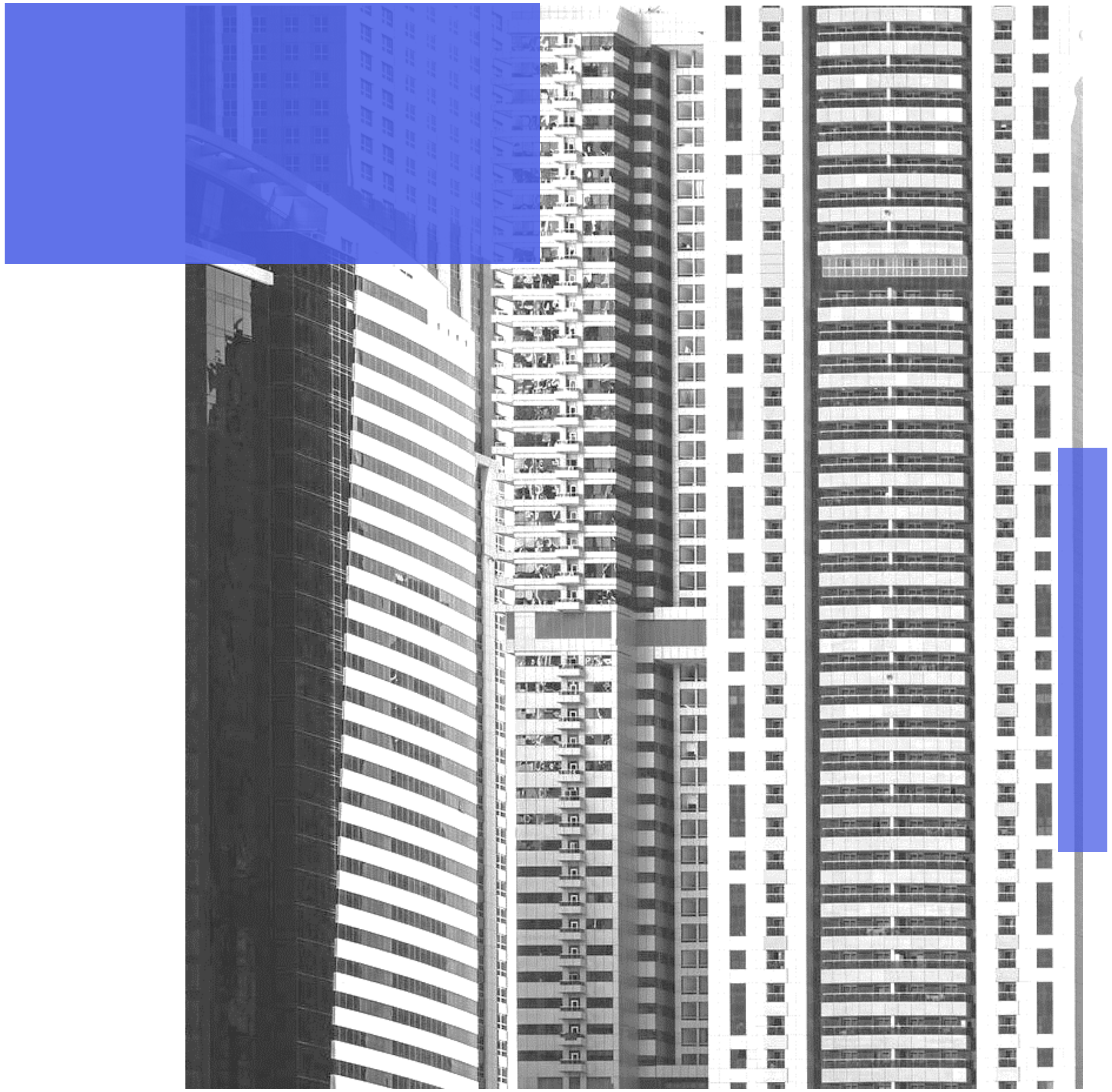
okta INTEGRATION WITH servicenow®

-By Satyanarayan Rout
servicenow.satyarout@gmail.com

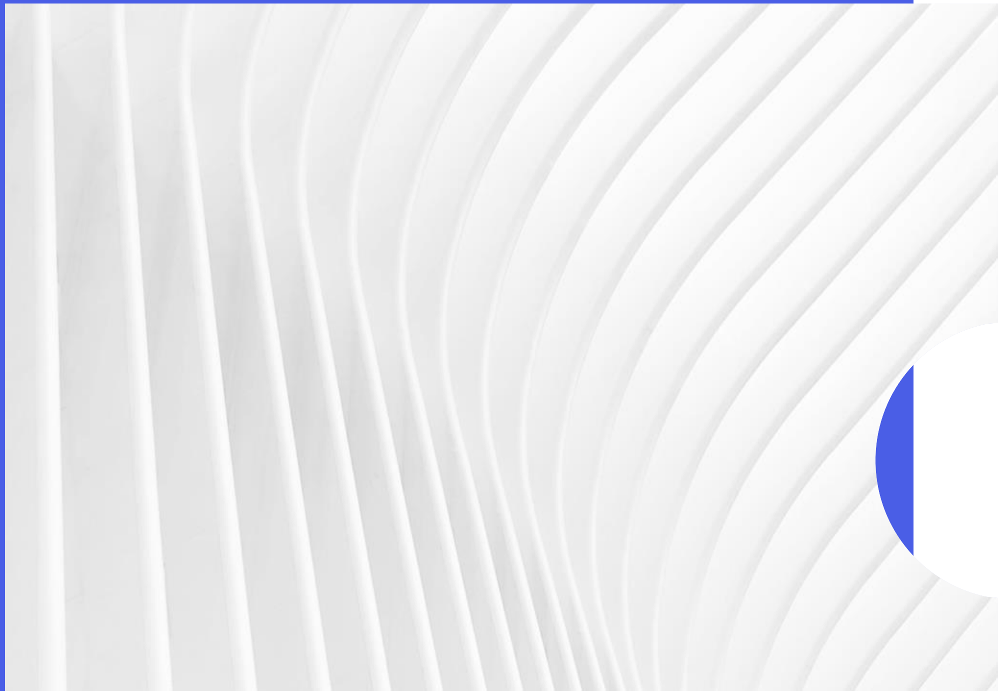


AGENDA

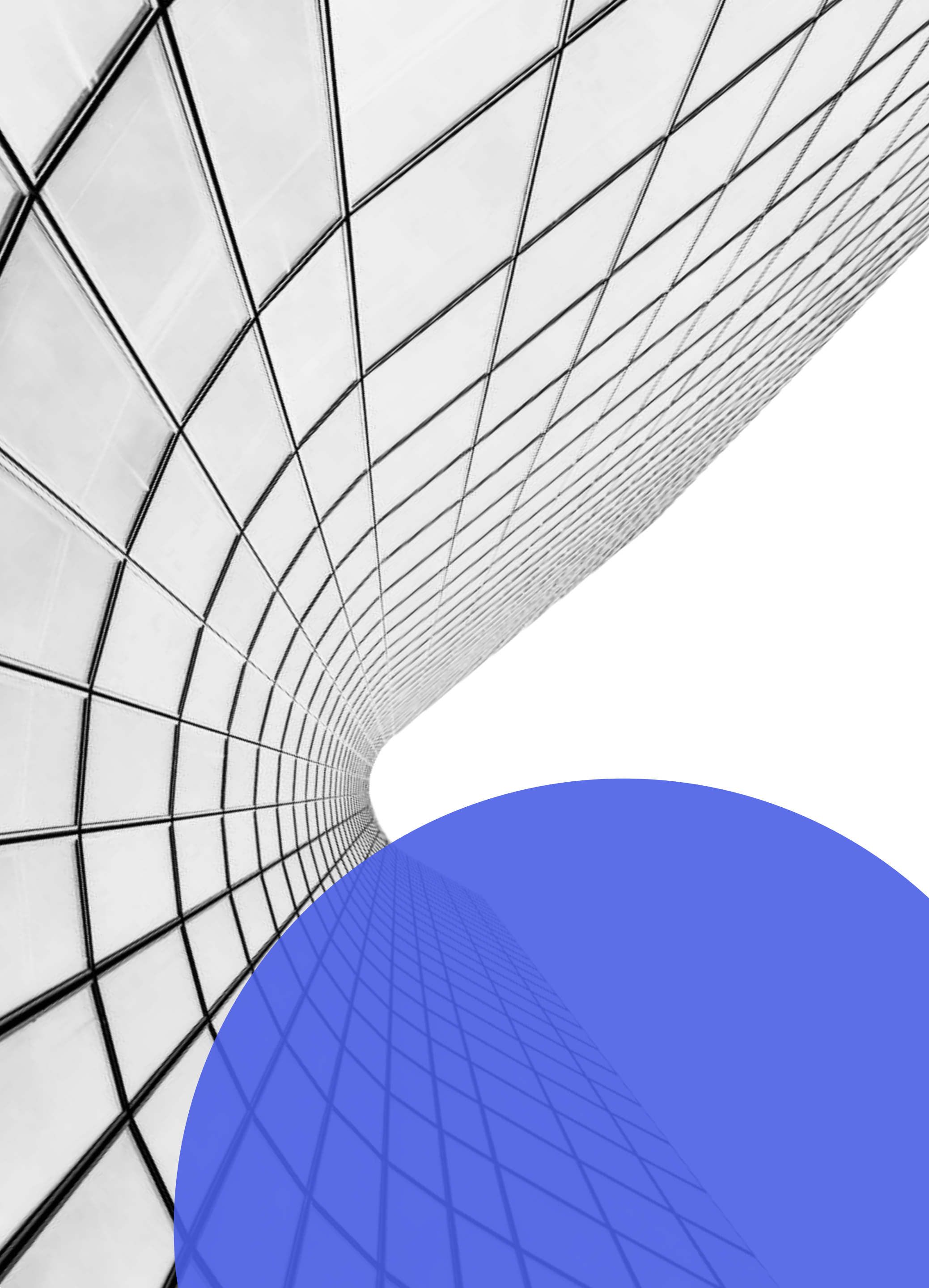
- WHAT IS OKTA
- STEPS TO CONFIGURE SSO
- STEPS TO ENABLE PROVISIONING
- SERVICENOW CONFIG FOR OKTA

Satyanarayan Rout
servicenow.satyarout@gmail.com

WHAT IS OKTA?

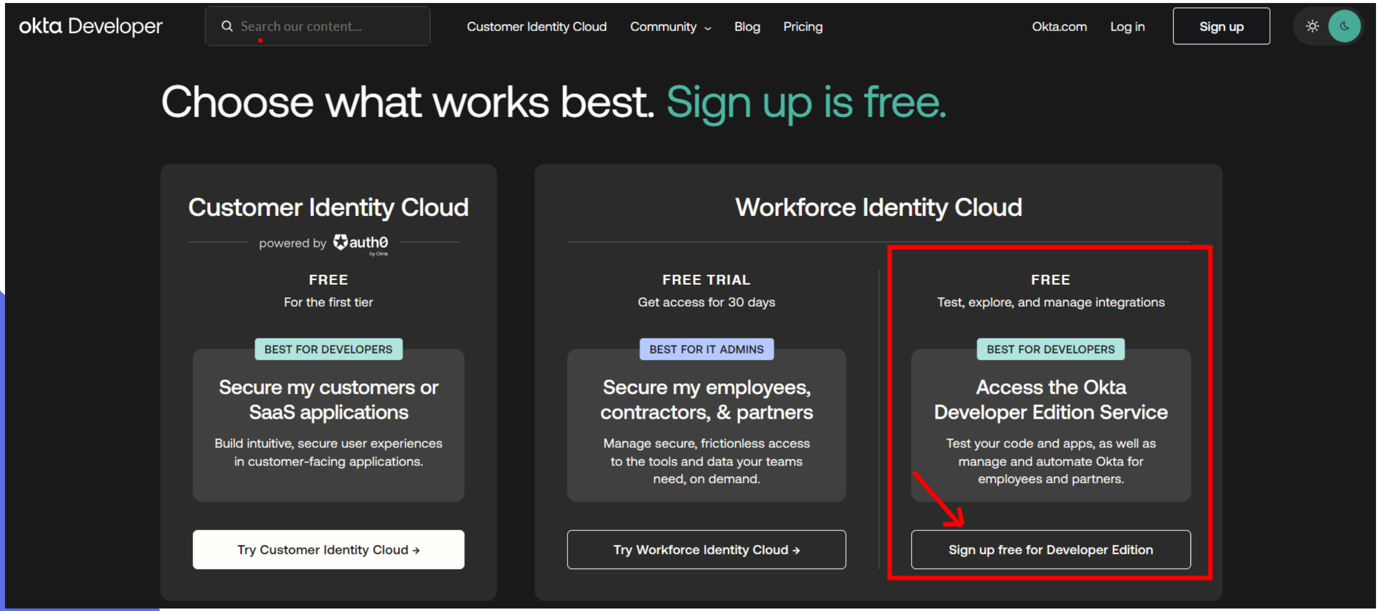


- **Okta** connects any person with any application on any device.
- It's an enterprise-grade, identity management service, built for the cloud, but compatible with many on-premises applications. With Okta, IT can manage any employee's access to any application or device. Okta runs in the cloud, on a secure, reliable, extensively audited platform, which integrates deeply with on-premises applications, directories, and identity management systems.



STEPS TO SETUP OKTA ACCOUNT

- Go to https://developer.okta.com/ & create an account by clicking on sign up button.
- Create a account by selecting Access the Okta Developer Edition Service mentioned on screenshot.



Choose what works best. Sign up is free.

Customer Identity Cloud

powered by auth0

FREE

For the first tier

BEST FOR DEVELOPERS

Secure my customers or SaaS applications

Build intuitive, secure user experiences in customer-facing applications.

Workforce Identity Cloud

FREE TRIAL

Get access for 30 days

BEST FOR IT ADMINS

Secure my employees, contractors, & partners

Manage secure, frictionless access to the tools and data your teams need, on demand.

FREE

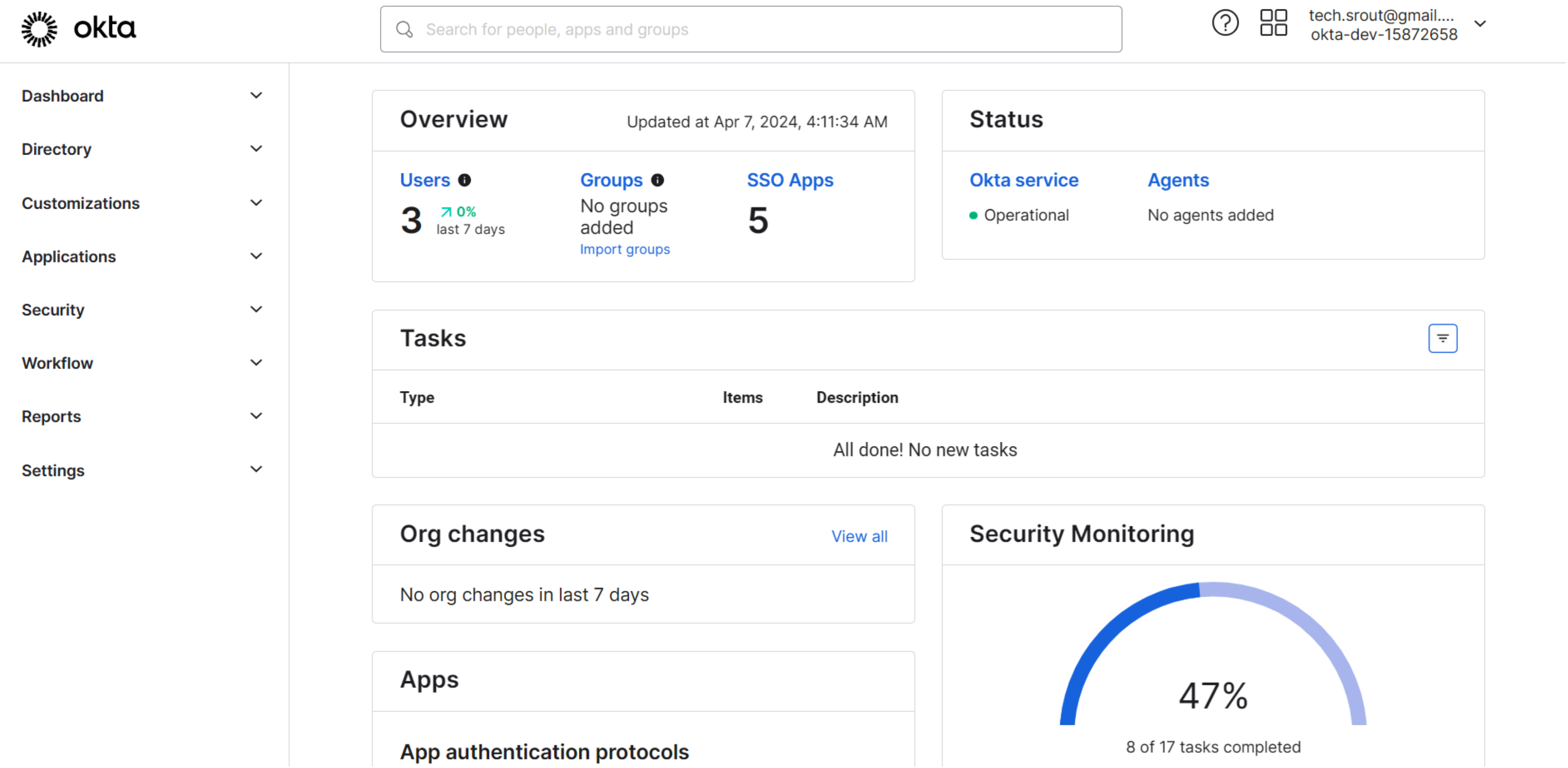
Test, explore, and manage integrations

BEST FOR DEVELOPERS

Access the Okta Developer Edition Service

Test your code and apps, as well as manage and automate Okta for employees and partners.

- After signup successfully it will redirect to **Okta Dashboard** view where we need to do all SSO related configurations like Enable SSO by connecting with ServiceNow App ,Provisioning,User/Group creation,Assigning a user to servicenow application etc.



Overview Updated at Apr 7, 2024, 4:11:34 AM

Users 3 ↗ 0% last 7 days

Groups No groups added Import groups

SSO Apps 5

Status

Okta service ● Operational

Agents No agents added

Tasks

Type	Items	Description
All done! No new tasks		

Org changes View all

No org changes in last 7 days

Apps

App authentication protocols

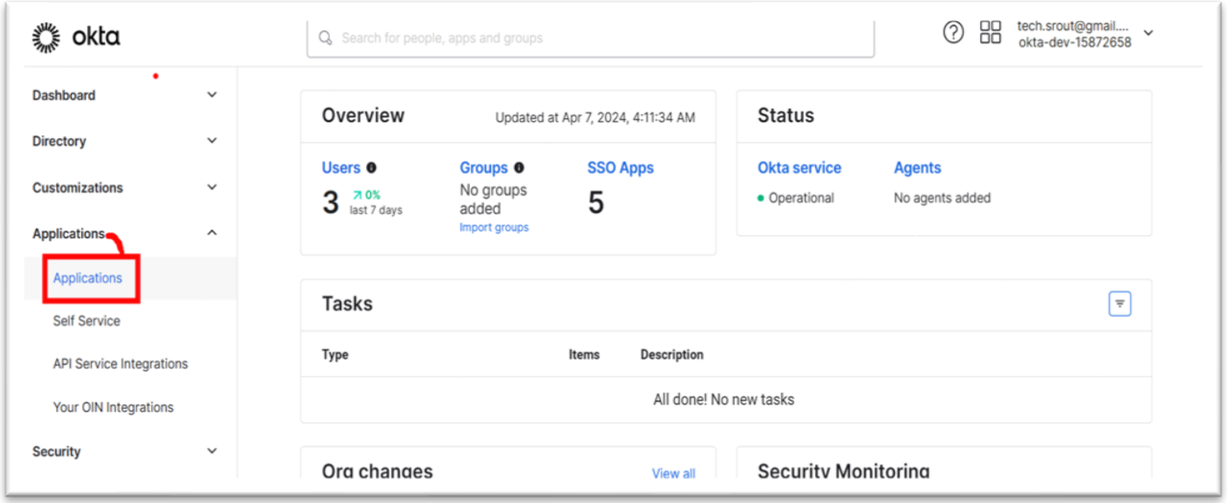
Security Monitoring

47%

8 of 17 tasks completed

STEPS TO ADD SERVICENOW APP IN OKTA

- Move to left menu > Applications>Browse app catelog button>Search for servicenow UD app>click on add integration.



okta

Search for people, apps and groups

tech.srout@gmail.... okta-dev-15872658

Dashboard
Directory
Customizations
Applications
Applications
Self Service
API Service Integrations
Your OIN Integrations
Security

Overview — Updated at Apr 7, 2024, 4:11:34 AM

Users 3 ↗ 0% last 7 days
Groups No groups added Import groups
SSO Apps 5

Status

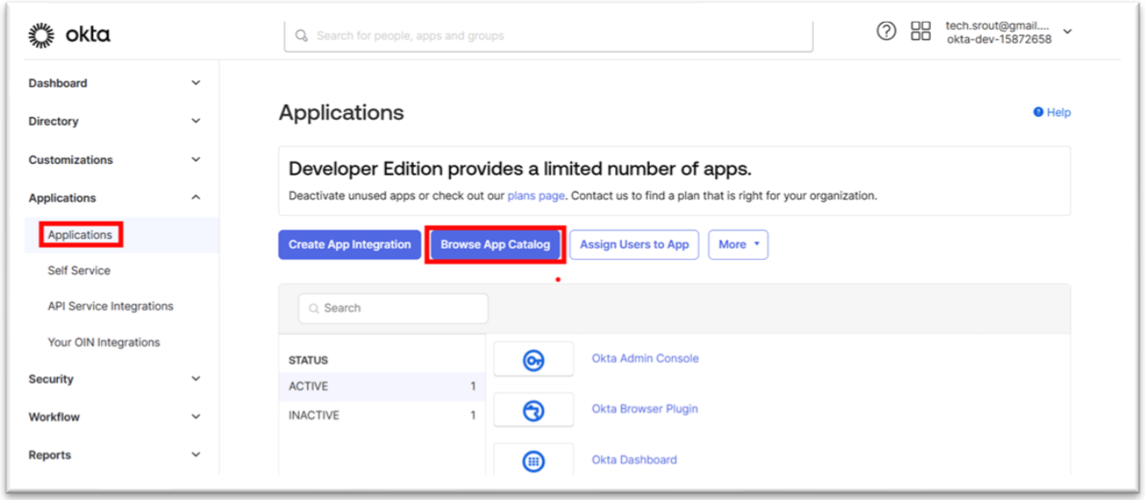
Okta service ● Operational
Agents No agents added

Tasks

Type	Items	Description
All done! No new tasks		

Org changes View all

Security Monitoring



okta

Search for people, apps and groups

tech.srout@gmail.... okta-dev-15872658

Dashboard
Directory
Customizations
Applications
Applications
Self Service
API Service Integrations
Your OIN Integrations
Security
Workflow
Reports

Applications — Help

Developer Edition provides a limited number of apps.

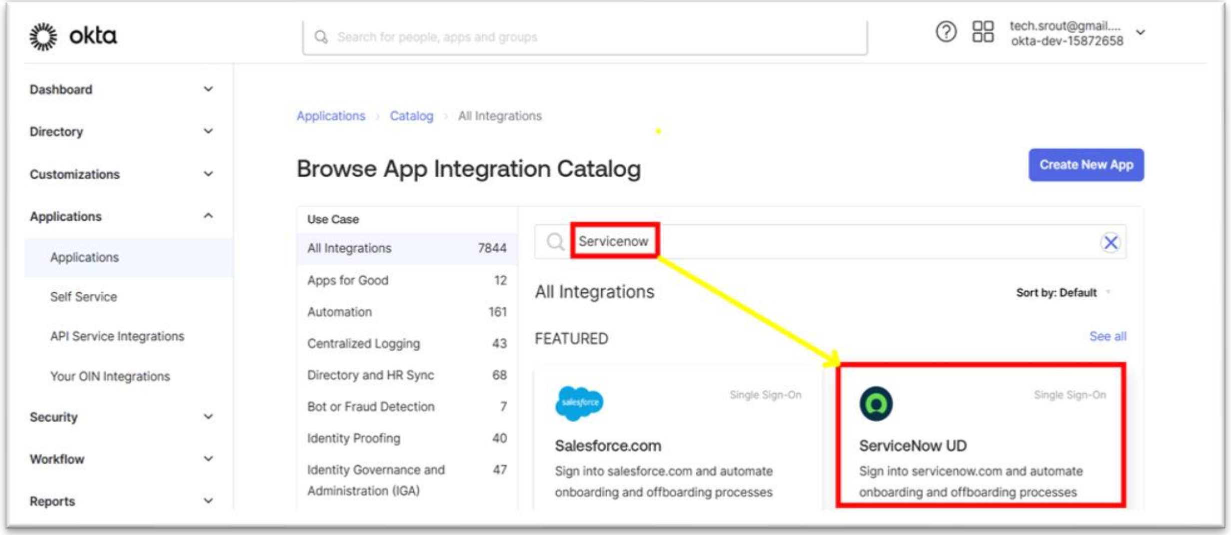
Deactivate unused apps or check out our plans page. Contact us to find a plan that is right for your organization.

Create App Integration | Browse App Catalog | Assign Users to App | More

Search

STATUS	
ACTIVE	1
INACTIVE	1

Okta Admin Console
Okta Browser Plugin
Okta Dashboard



okta

Search for people, apps and groups

tech.srout@gmail.... okta-dev-15872658

Dashboard
Directory
Customizations
Applications
Applications
Self Service
API Service Integrations
Your OIN Integrations
Security
Workflow
Reports

Applications › Catalog › All Integrations

Browse App Integration Catalog — Create New App

Use Case	
All Integrations	7844
Apps for Good	12
Automation	161
Centralized Logging	43
Directory and HR Sync	68
Bot or Fraud Detection	7
Identity Proofing	40
Identity Governance and Administration (IGA)	47

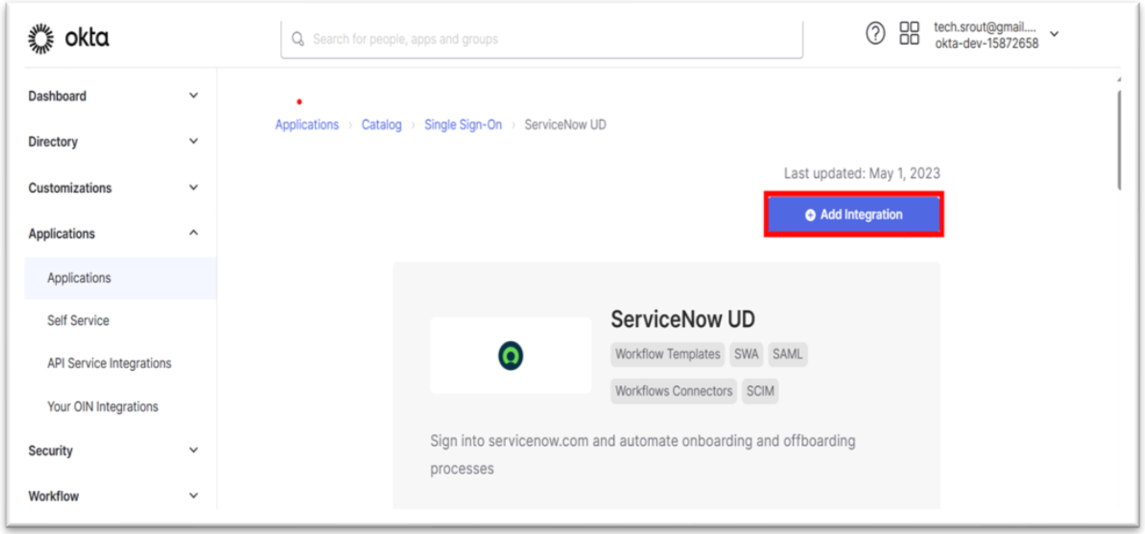
Servicenow

All Integrations — Sort by: Default

FEATURED — See all

Salesforce.com — Single Sign-On
Sign into salesforce.com and automate onboarding and offboarding processes

ServiceNow UD — Single Sign-On
Sign into servicenow.com and automate onboarding and offboarding processes



okta

Search for people, apps and groups

tech.srout@gmail.... okta-dev-15872658

Dashboard
Directory
Customizations
Applications
Applications
Self Service
API Service Integrations
Your OIN Integrations
Security
Workflow

Applications › Catalog › Single Sign-On › ServiceNow UD

Last updated: May 1, 2023

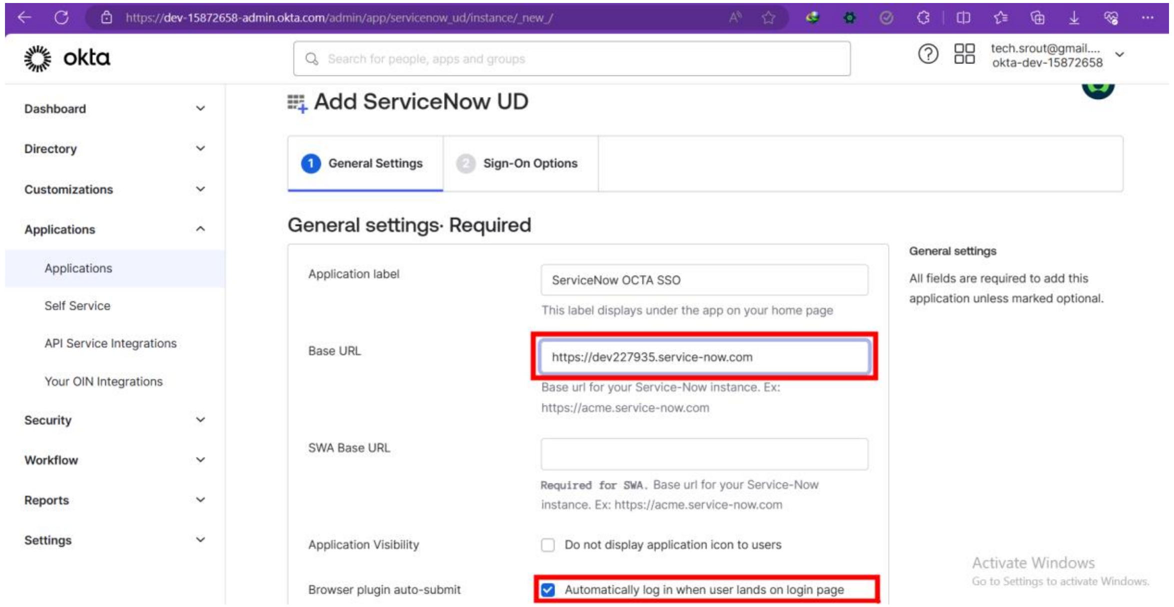
Add Integration

ServiceNow UD

Workflow Templates | SWA | SAML | Workflows Connectors | SCIM

Sign into servicenow.com and automate onboarding and offboarding processes

- After adding the servicenow ud app, it will ask for general Settings & Sign-on Options.
- In general settings we need to provide **base url** value as our **PDI URL** with whom we want to configure SSO. Then click next , in **sign-on Options>select SAML 2.0>Click on Identity provider metadata link and simply copy the url for later use.**



https://dev-15872658-admin.okta.com/admin/app/servicenow_ud/instance/_new_/

Add ServiceNow UD

1 General Settings | 2 Sign-On Options

General settings· Required

Application label: ServiceNow OCTA SSO
This label displays under the app on your home page

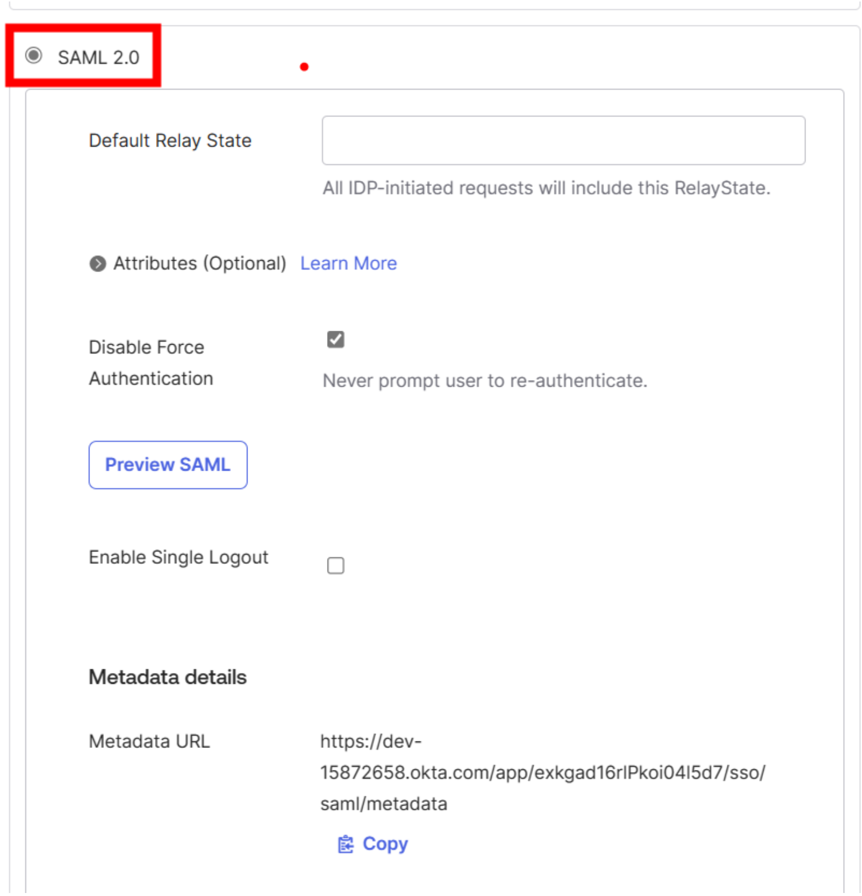
Base URL: https://dev227935.service-now.com
Base url for your Service-Now instance. Ex: https://acme.service-now.com

SWA Base URL:
Required for SWA. Base url for your Service-Now instance. Ex: https://acme.service-now.com

Application Visibility: ☐ Do not display application icon to users

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

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



● SAML 2.0

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

Attributes (Optional) Learn More

Disable Force Authentication: ☑ Never prompt user to re-authenticate.

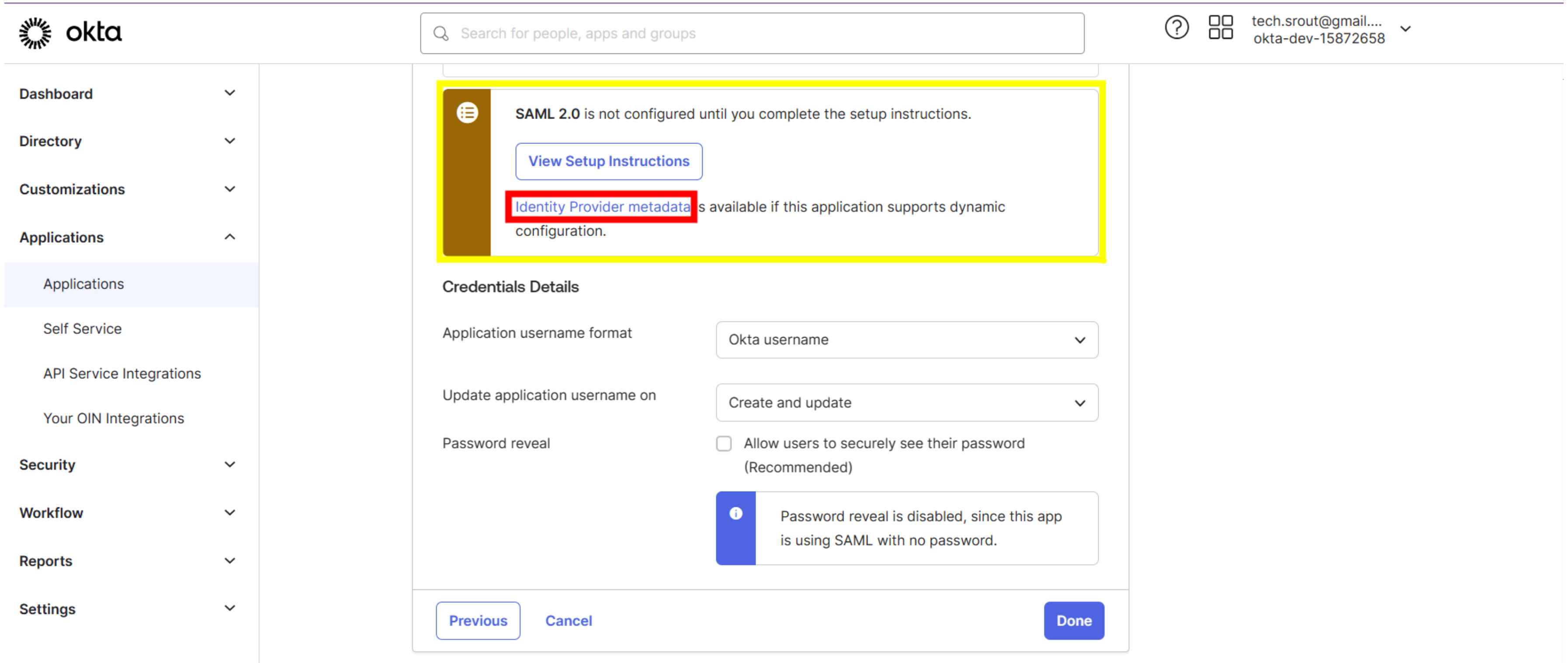
Preview SAML

Enable Single Logout: ☐

Metadata details

Metadata URL: https://dev-15872658.okta.com/app/exkgad16rlPkoi04l5d7/sso/saml/metadata

Copy



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

View Setup Instructions

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

Credentials Details

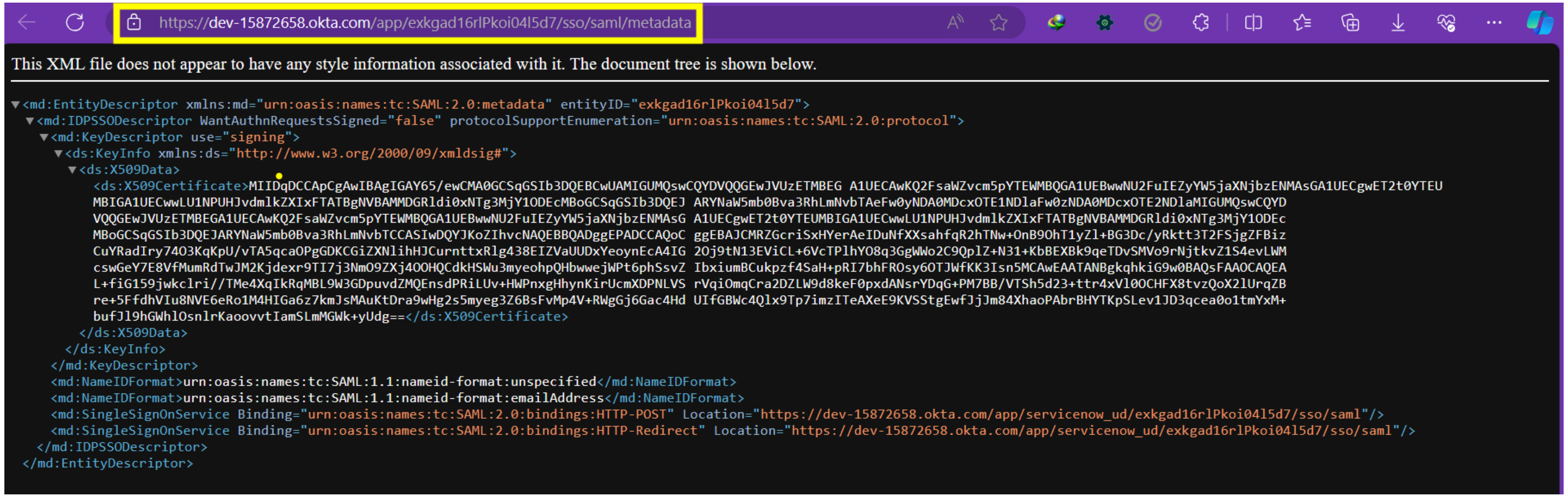
Application username format: Okta username

Update application username on: Create and update

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

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

Previous Cancel Done



https://dev-15872658.okta.com/app/exkgad16rlPkoi04l5d7/sso/saml/metadata

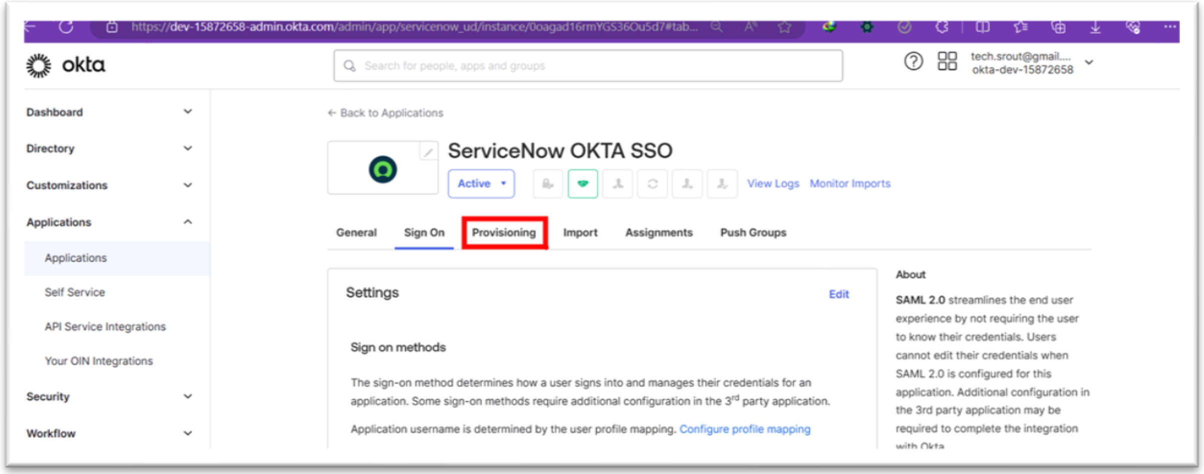
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="exkgad16rlPkoi04l5d7">
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
           <ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAY65/ewCMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
           MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi0xNTg3MjY1ODEcMBoGCSqGSIb3DQEJ ARYNaW5mb0Bva3RhLmNvbTAeFw0yNDA0MDcxOTE1NDlaFw0zNDA0MDcxOTE2NDlaMIGUMQswCQYD
           VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi0xNTg3MjY1ODEc
           MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC ggEBAJCMRZGcriSxHYerAeIDuNfXXsahfqR2hTNw+OnB9OhT1yZl+BG3Dc/yRktt3T2FSjgZFBiz
           CuYRadIry74O3KqKpU/vTA5qcaOPgGDKCGiZXNlihHJCurnttxRlg438EIZVaUUDxYeoynEcA4IG 2Oj9tN13EViCL+6VcTPlhYO8q3GgWWo2C9QplZ+N31+KbBEXBk9qeTDvSMVo9rNjtkvZ1S4evLWM
           cswGeY7E8VfMumRdTwJM2Kjdexr9TI7j3NmO9ZXj4OOHQCdkHSWu3myeohpQHbwwejWPt6phSsvZ IbxiumBCukpzf4SaH+pRI7bhFROsy6OTJWfKK3Isn5MCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
           L+fiG159jwkclri//TMe4XqIkRqMBL9W3GDpuvdZMQEnsdPRiLUv+HWPnxgHhynKirUcmXDPNLVS rVqiOmqCra2DZLW9d8keF0pxdANsrYDqG+PM7BB/VTSh5d23+ttr4xVl0OCHFX8tvzQoX2lUrqZB
           re+5FfdhVIu8NVE6eRo1M4HIGa6z7kmJsMAuKtDra9wHg2s5myeg3Z6BsFvMp4V+RWgGj6Gac4Hd UIfGBWc4Qlx9Tp7imzITeAXeE9KVSStgEwfJjJm84XhaoPAbrBHYTKpSLev1JD3qcea0o1tmYxM+
           bufJl9hGWhlOsnlrKaoovvtIamSLmMGWk+yUdg==</ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
     </md:KeyDescriptor>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
     <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev-15872658.okta.com/app/servicenow_ud/exkgad16rlPkoi04l5d7/sso/saml"/>
     <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://dev-15872658.okta.com/app/servicenow_ud/exkgad16rlPkoi04l5d7/sso/saml"/>
   </md:IDPSSODescriptor>
 </md:EntityDescriptor>
```

- After copying the URL mentioned on above screenshot save it for later use and click on done to complete Sign On process .

Next we need to enable provisioning for our Servicenow Application:

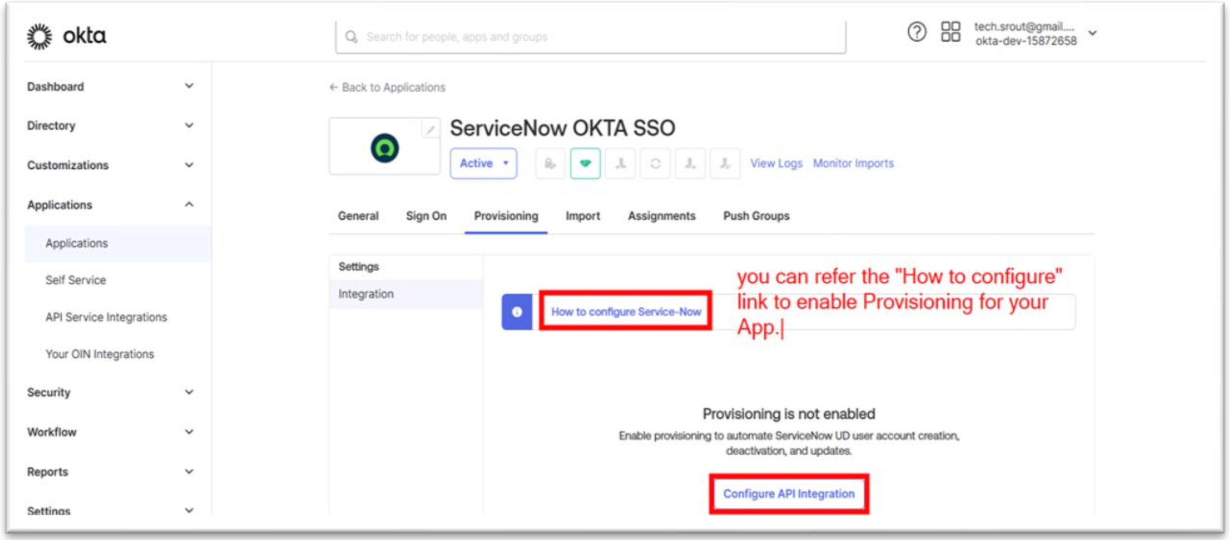
- **Click on provision>Configure API Integration**(you can also refer “How to configure Service-Now” link)>It ask for admin credentials of your ServiceNow account to enable provisioning>After successfully validating credentials it will show provisioning to App window where we need to edit provisioning settings like Create user,Update user attribute,Deactivate user & sync password.



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

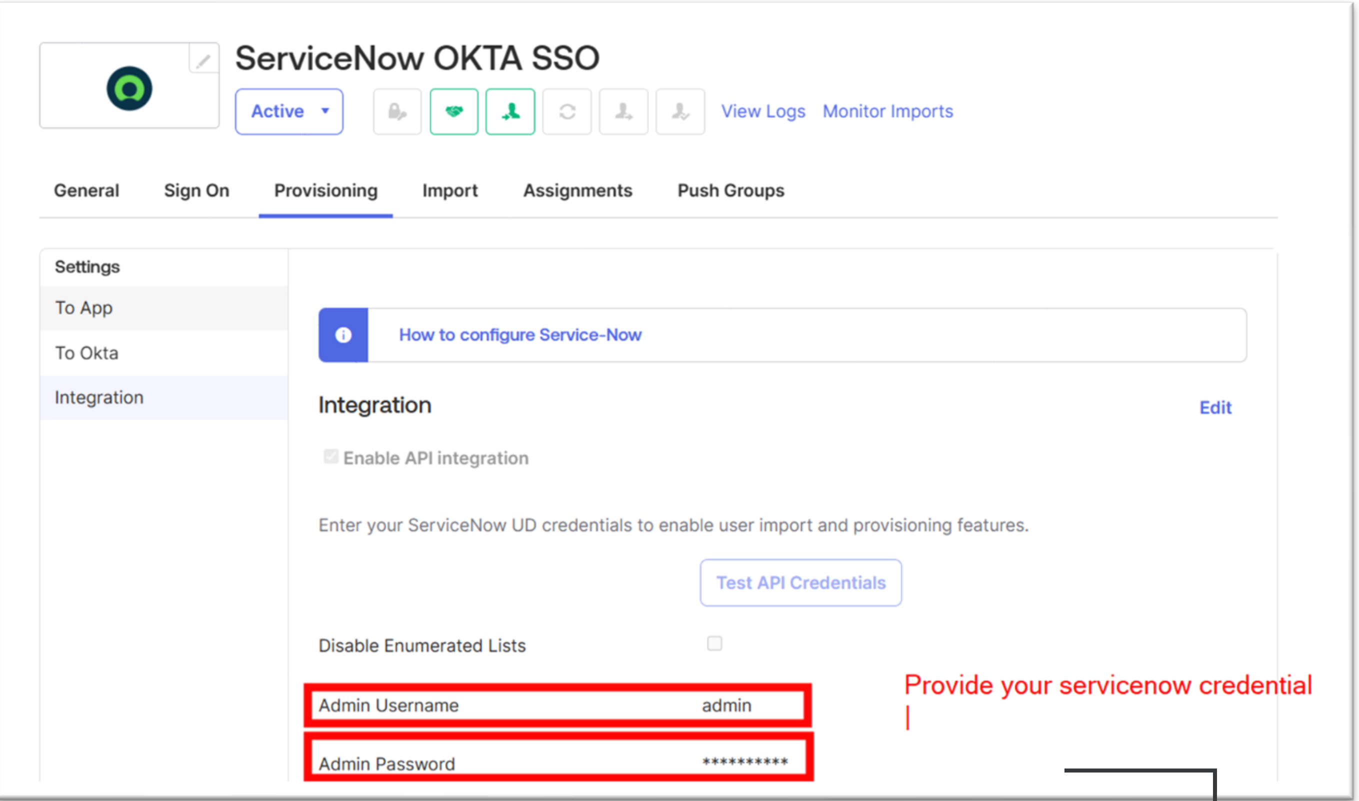
Application username is determined by the user profile mapping. Configure profile mapping

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



you can refer the "How to configure" link to enable Provisioning for your App.|

Enable provisioning to automate ServiceNow UD user account creation, deactivation, and updates.



ServiceNow OKTA SSO

How to configure Service-Now

Integration

Edit

☑ Enable API integration

Enter your ServiceNow UD credentials to enable user import and provisioning features.

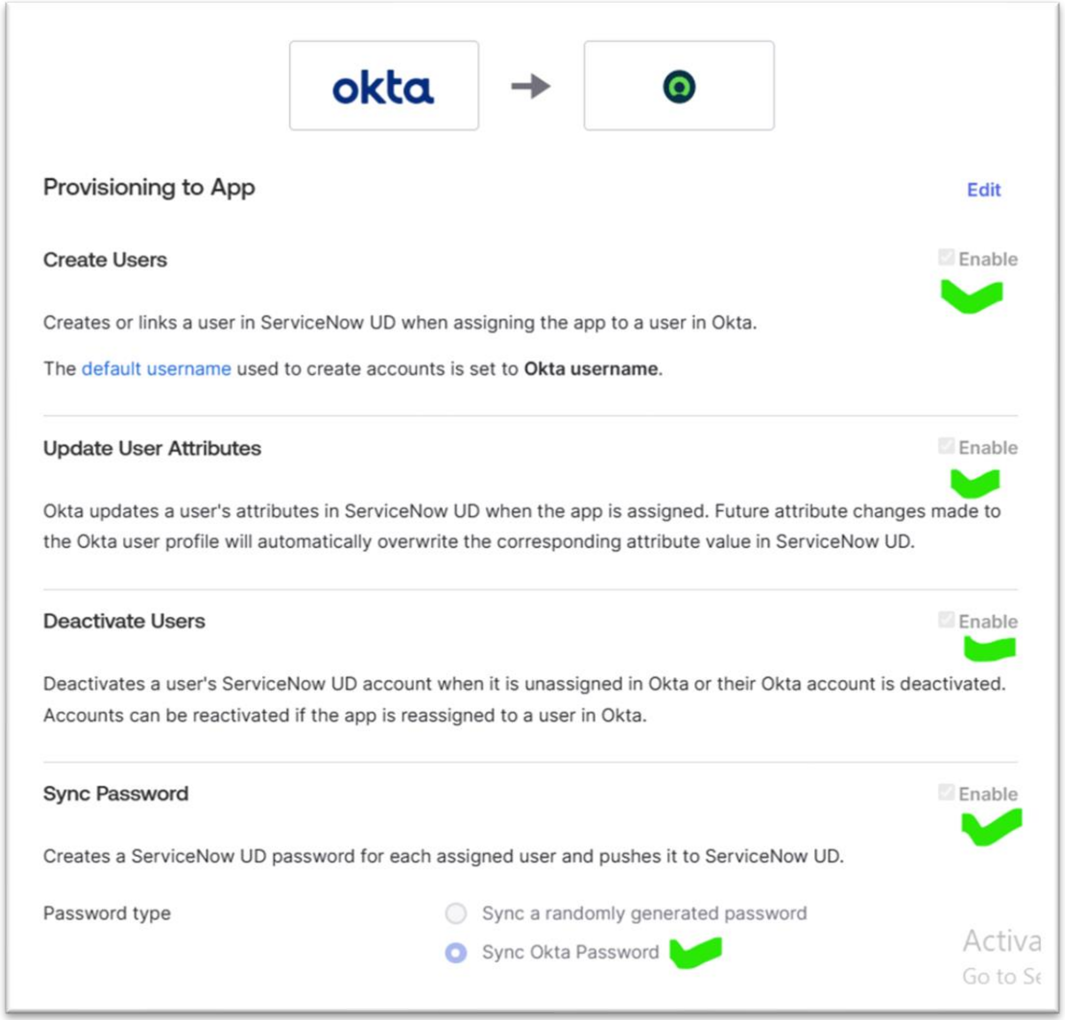
Test API Credentials

Disable Enumerated Lists □

Admin Username admin

Admin Password **********

Provide your servicenow credential



Provisioning to App

Edit

Create Users ☑ Enable ✓

Creates or links a user in ServiceNow UD when assigning the app to a user in Okta.

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

Update User Attributes ☑ Enable ✓

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

Deactivate Users ☑ Enable ✓

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

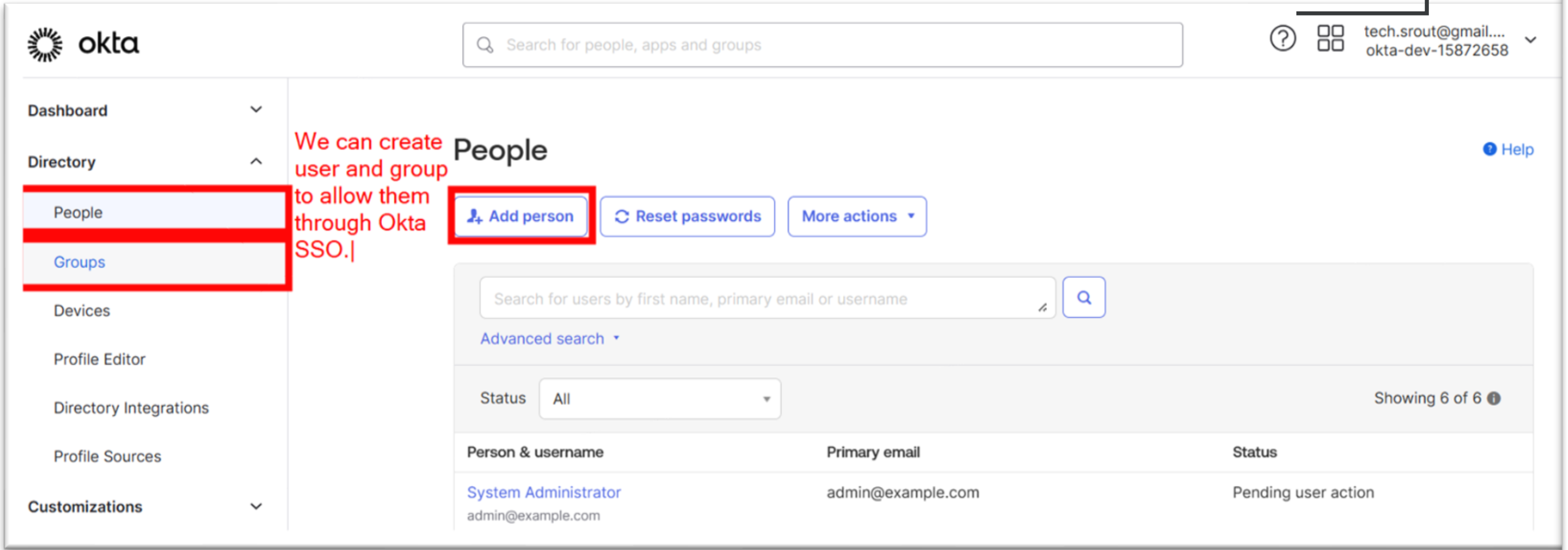
Sync Password ☑ Enable ✓

Creates a ServiceNow UD password for each assigned user and pushes it to ServiceNow UD.

Password type ○ Sync a randomly generated password

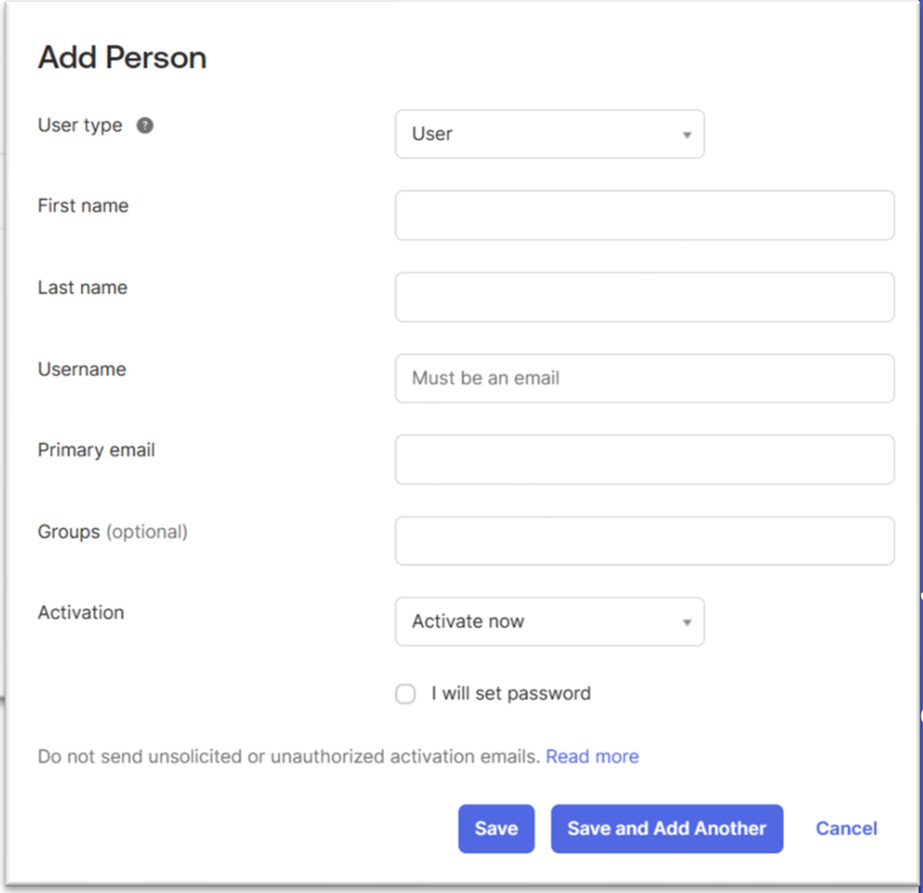
● Sync Okta Password ✓

- After enabling provisioning settings like Create user,Update user attribute,Deactivate user & sync password ,the provisioning process complete for our application.
- Next we need to create User and assign them to our application so that that particular user can able to login through SSO to servicenow instance.
- **Steps:**
- **Click on Directory menu>people>>add person>provide user details like first name ,last name, email & password>click on save.**



We can create user and group to allow them through Okta SSO.|

Person & username	Primary email	Status
System Administrator admin@example.com	admin@example.com	Pending user action



Add Person

User type: User

First name

Last name

Username: Must be an email

Primary email

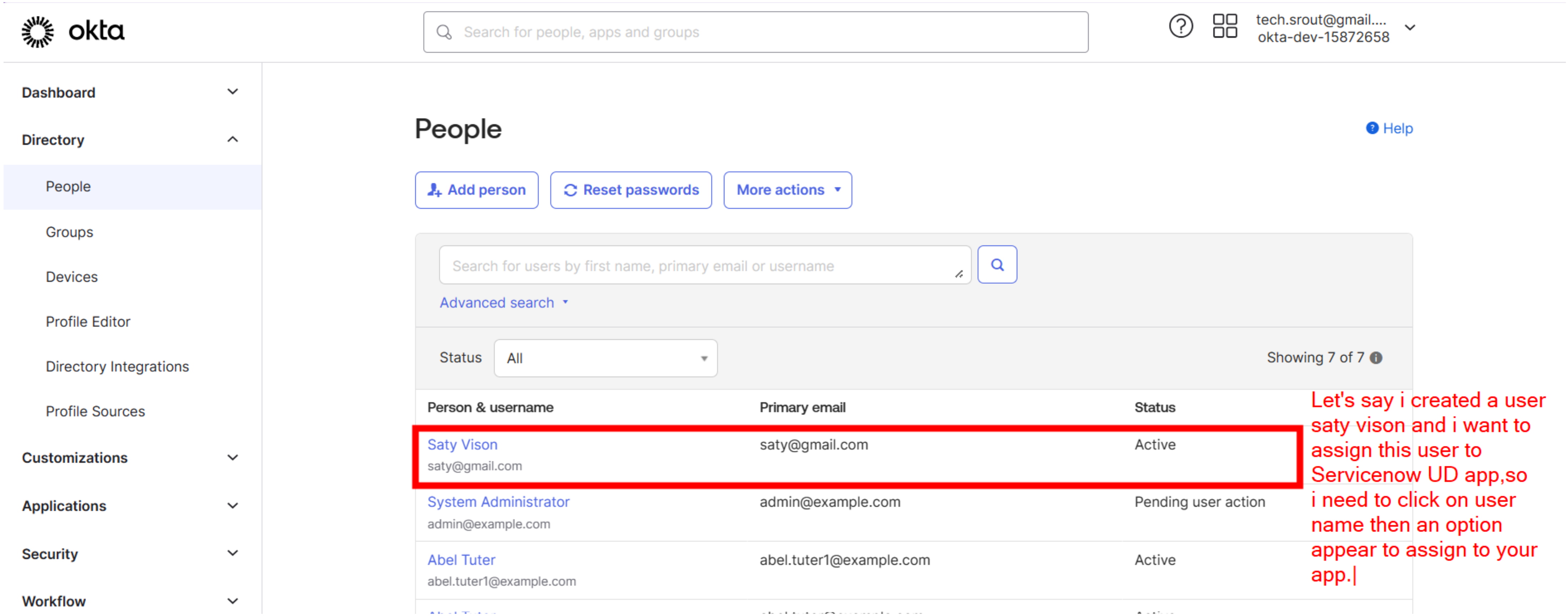
Groups (optional)

Activation: Activate now

□ I will set password

Do not send unsolicited or unauthorized activation emails. Read more

- After successfully creating the user it’s going to visible under People with status as active.



People

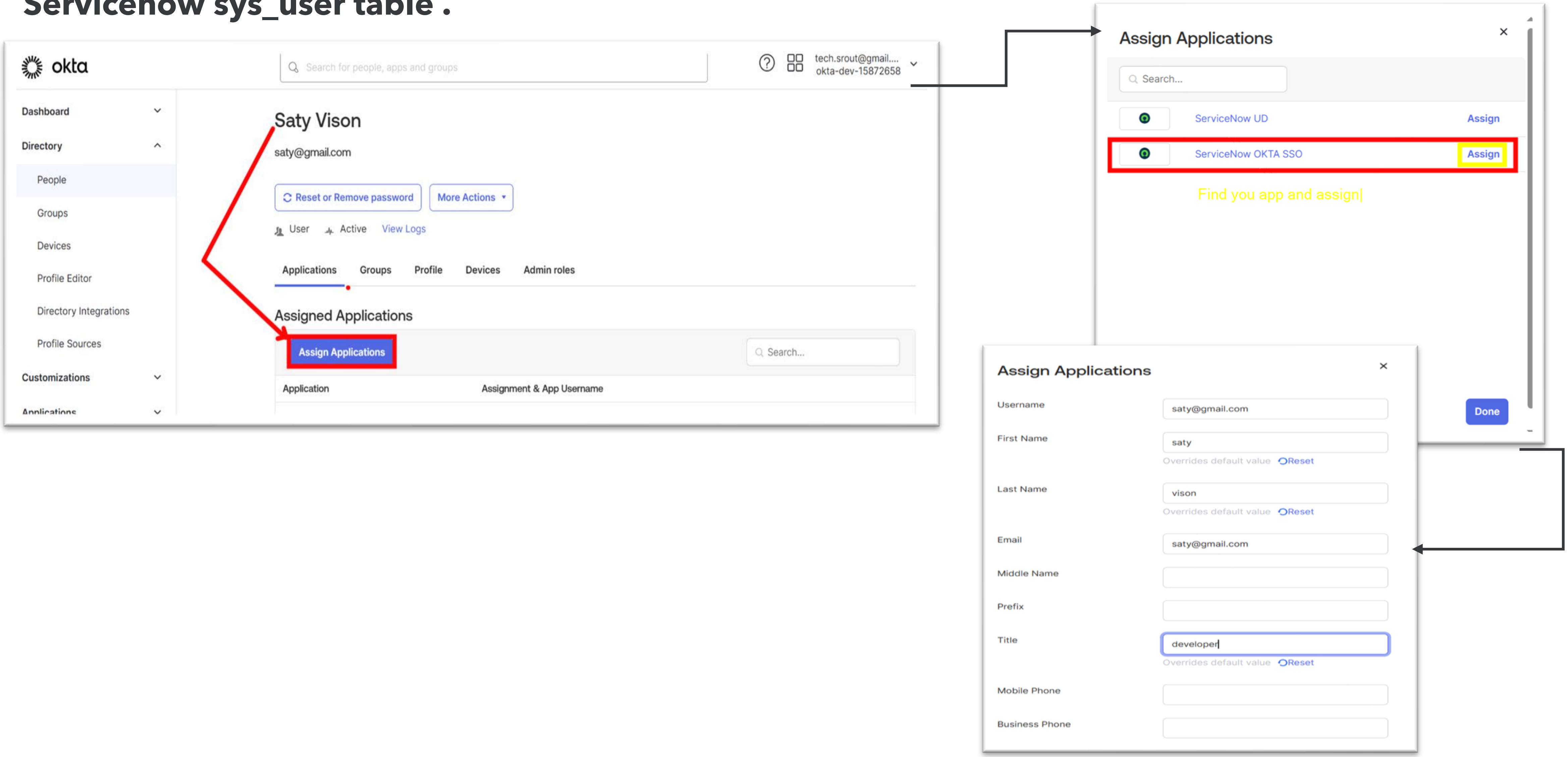
Status: All

Showing 7 of 7

Person & username	Primary email	Status
Saty Vison saty@gmail.com	saty@gmail.com	Active
System Administrator admin@example.com	admin@example.com	Pending user action
Abel Tuter abel.tuter1@example.com	abel.tuter1@example.com	Active

Let's say i created a user saty vison and i want to assign this user to Servicenow UD app,so i need to click on user name then an option appear to assign to your app.|

- To assign the user you created just now to your Servicenow application follow these steps: **Click on user name under Directory>People>then click on assign application>Select your application>click on assign>provide some user details >then it will assign the user to your Servicenow App and as the user provisioning is enabled the same account will be created on Servicenow sys_user table .**



Saty Vison

saty@gmail.com

User Active

Assigned Applications

Assign Applications

ServiceNow UD Assign

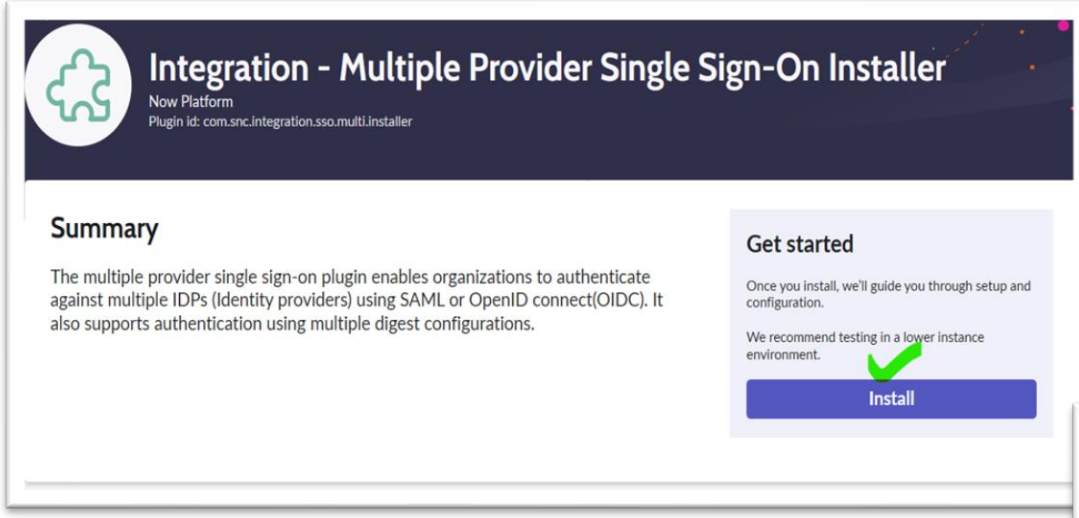
ServiceNow OKTA SSO Assign

Find you app and assign|

Assign Applications

Username	saty@gmail.com
First Name	saty Overrides default value Reset
Last Name	vison Overrides default value Reset
Email	saty@gmail.com
Middle Name	
Prefix	
Title	developer Overrides default value Reset
Mobile Phone	
Business Phone	

- Everything configured from Okta end now we need to setup ServiceNow SSO Configuration as follows:
  - Enable **Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer) .**
  - **Enable multiple provider SSO property as per given screenshot.**



Integration - Multiple Provider Single Sign-On Installer

Now Platform

Plugin id: com.snc.integration.sso.multi.installer

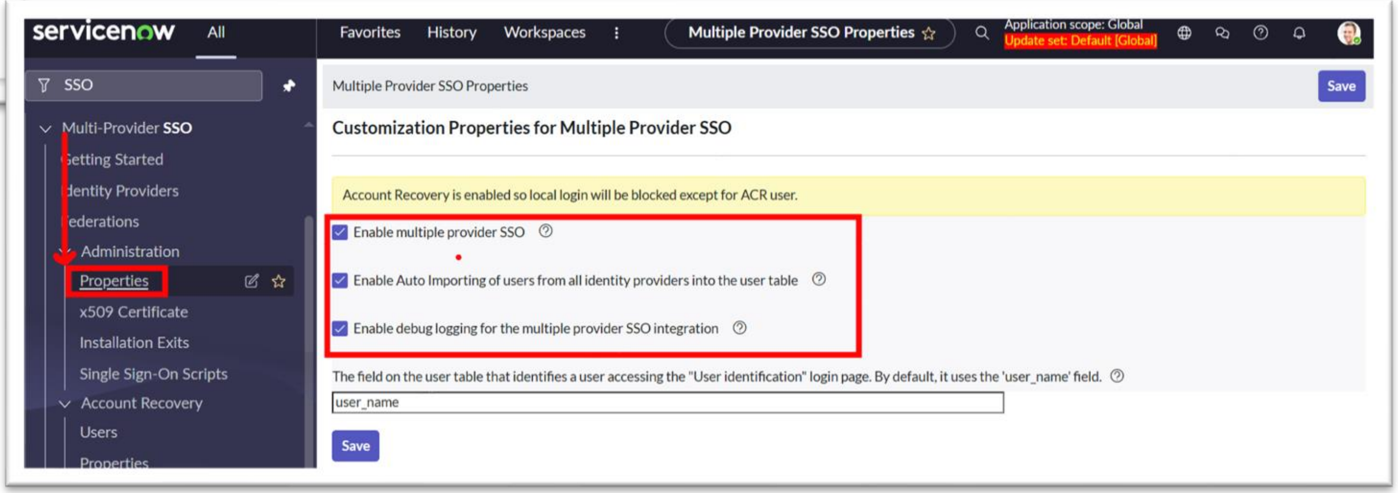
Summary

The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML or OpenID connect(OIDC). It also supports authentication using multiple digest configurations.

Get started

Once you install, we'll guide you through setup and configuration.

We recommend testing in a lower instance environment.



Multiple Provider SSO Properties

Customization Properties for Multiple Provider SSO

Account Recovery is enabled so local login will be blocked except for ACR user.

☑ Enable multiple provider SSO

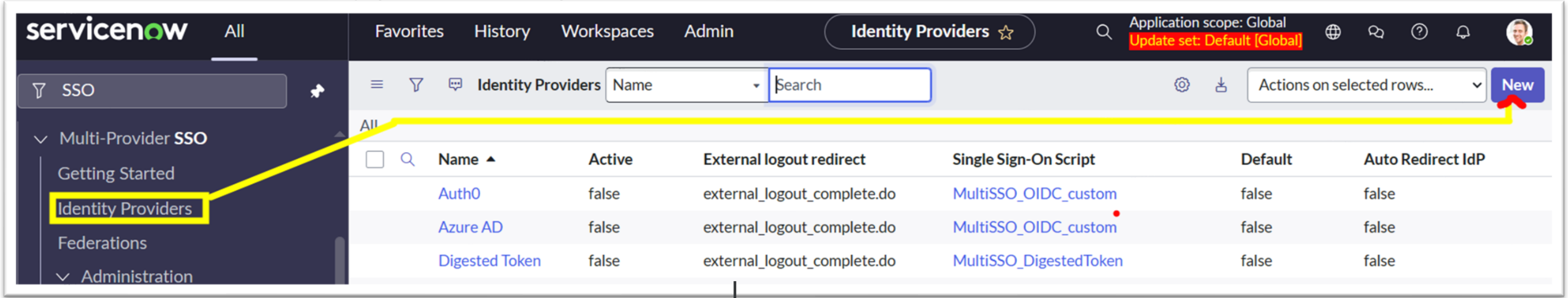
☑ Enable Auto Importing of users from all identity providers into the user table

☑ Enable debug logging for the multiple provider SSO integration

The field on the user table that identifies a user accessing the "User identification" login page. By default, it uses the 'user_name' field.

user_name

- To create a identity provider simple do this:



servicenow All | Favorites | History | Workspaces | Admin | Identity Providers ☆ | Application scope: Global | Update set: Default [Global]

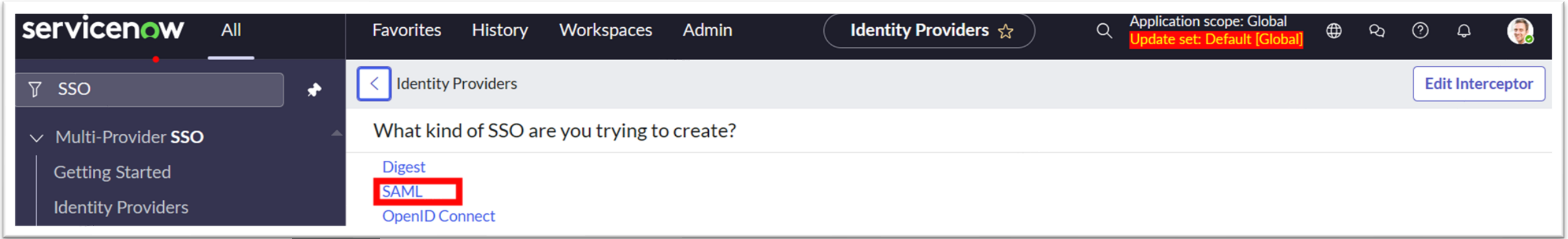
SSO

Multi-Provider SSO
- Getting Started
- Identity Providers
- Federations
- Administration

Identity Providers | Name | Search | Actions on selected rows... | New

All

Name ▲	Active	External logout redirect	Single Sign-On Script	Default	Auto Redirect IdP
Auth0	false	external_logout_complete.do	MultiSSO_OIDC_custom	false	false
Azure AD	false	external_logout_complete.do	MultiSSO_OIDC_custom	false	false
Digested Token	false	external_logout_complete.do	MultiSSO_DigestedToken	false	false



servicenow All | Favorites | History | Workspaces | Admin | Identity Providers ☆ | Application scope: Global | Update set: Default [Global]

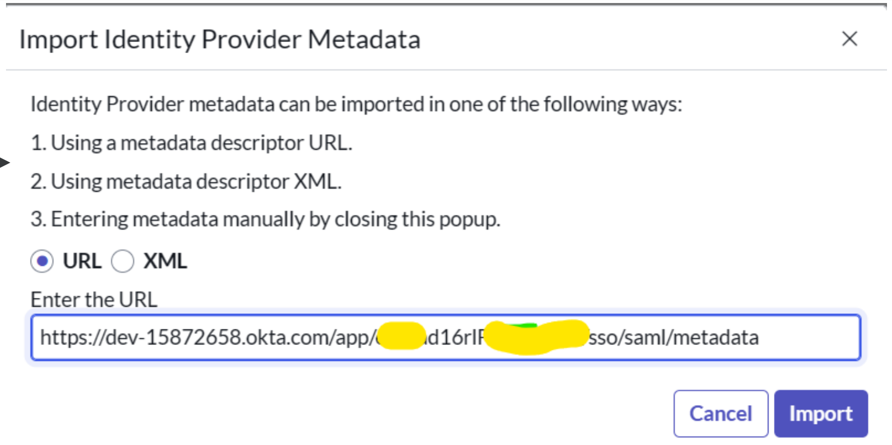
SSO

Multi-Provider SSO
- Getting Started
- Identity Providers

Identity Providers | Edit Interceptor

What kind of SSO are you trying to create?

- Digest
- SAML
- OpenID Connect



Import Identity Provider Metadata ×

Identity Provider metadata can be imported in one of the following ways:

1. Using a metadata descriptor URL.
2. Using metadata descriptor XML.
3. Entering metadata manually by closing this popup.

● URL ○ XML

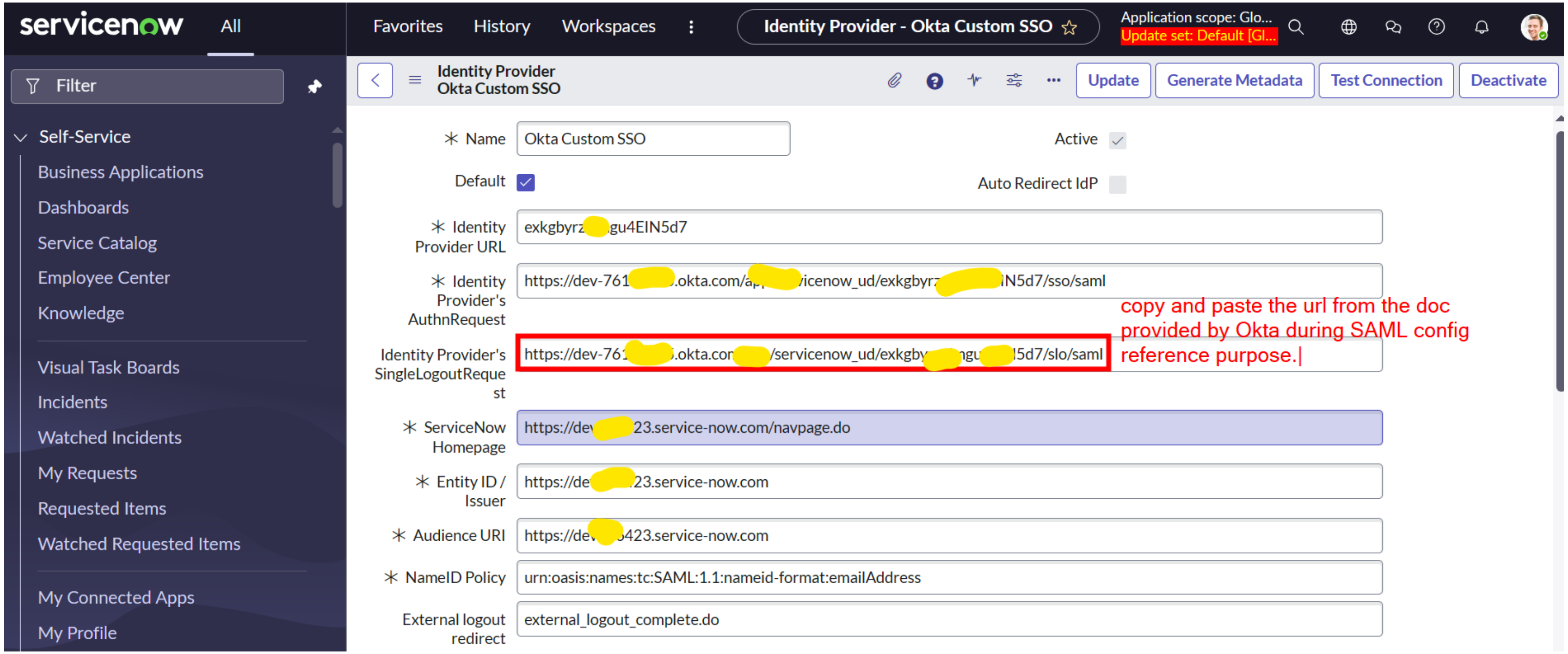
Enter the URL

https://dev-15872658.okta.com/app/[redacted]d16rIF[redacted]sso/saml/metadata

Cancel | Import

- Here provide the url that you have copied during SAML SignOn configuration & import.

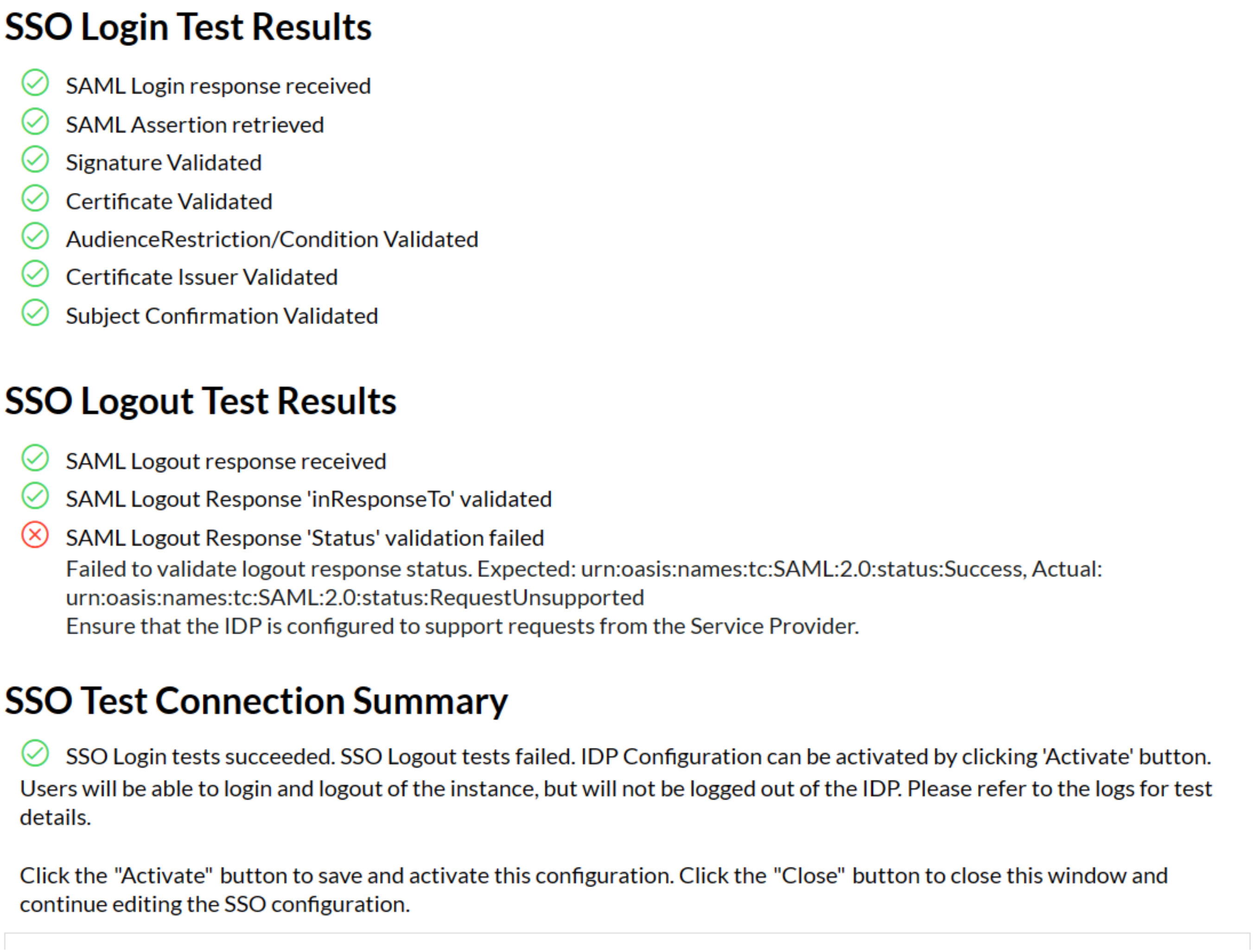
- Then an IDP will be created as per the import link data where we need to do few things like in Identity Provider's SingleLogoutRequest field paste the url mentioned in the OKTA DOC & in Advance section change User Field value as “user_name”, then click on test connection .



* Name	Okta Custom SSO
Active	✓
Default	☑
Auto Redirect IdP	□
* Identity Provider URL	exkgbyrz[redacted]gu4EIN5d7
* Identity Provider's AuthnRequest	https://dev-761[redacted].okta.com/a[redacted]icenow_ud/exkgbyrz[redacted]N5d7/sso/saml
Identity Provider's SingleLogoutRequest	https://dev-76[redacted].okta.co[redacted]/servicenow_ud/exkgby[redacted]ngu[redacted]5d7/slo/saml
* ServiceNow Homepage	https://de[redacted]23.service-now.com/navpage.do
* Entity ID / Issuer	https://de[redacted]23.service-now.com
* Audience URI	https://de[redacted]423.service-now.com
* NameID Policy	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
External logout redirect	external_logout_complete.do

copy and paste the url from the doc provided by Okta during SAML config reference purpose.

- If SSO test Connection Summary display success message then click on activate .



SSO Login Test Results

- ✓ SAML Login response received
- ✓ SAML Assertion retrieved
- ✓ Signature Validated
- ✓ Certificate Validated
- ✓ AudienceRestriction/Condition Validated
- ✓ Certificate Issuer Validated
- ✓ Subject Confirmation Validated

SSO Logout Test Results

- ✓ SAML Logout response received
- ✓ SAML Logout Response 'inResponseTo' validated
- ⊗ SAML Logout Response 'Status' validation failed
  Failed to validate logout response status. Expected: urn:oasis:names:tc:SAML:2.0:status:Success, Actual: urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported
  Ensure that the IDP is configured to support requests from the Service Provider.

SSO Test Connection Summary

✓ SSO Login tests succeeded. SSO Logout tests failed. IDP Configuration can be activated by clicking 'Activate' button. Users will be able to login and logout of the instance, but will not be logged out of the IDP. Please refer to the logs for test details.

Click the "Activate" button to save and activate this configuration. Click the "Close" button to close this window and continue editing the SSO configuration.

THANK YOU!!!

Satyanarayan Rout

servicenow.satyarout@gmail.com