Pulse Secure

Cloud Secure – Okta Integration

Configuration Guide

Document Revisions 3.0
Published Date December 2018

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

https://www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Cloud Secure – Okta Integration Configuration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

List of Figures

Introduction

About This Guide

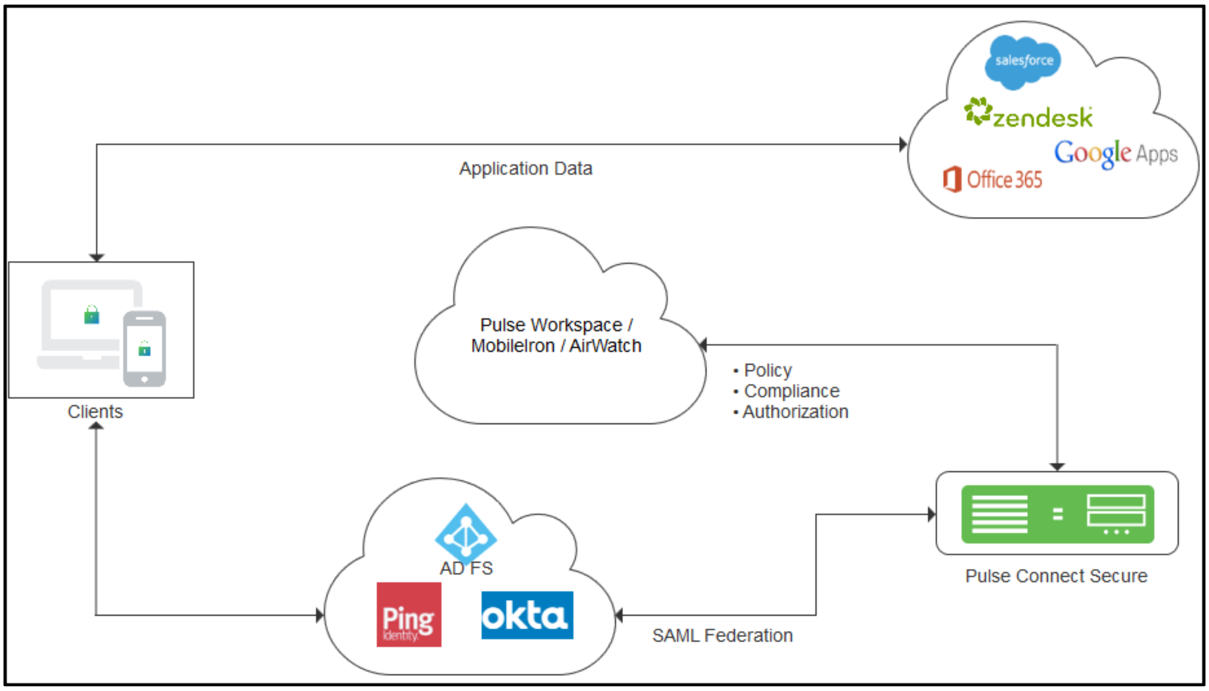
Cloud Secure Solution provides Secure Single Sign-On for Cloud services using Okta as Identity Management Provider. In this federated solution, Okta acts as both Identity Provider (for Cloud services) and Service Provider (for Pulse Connect Secure). Inbound SAML capabilities of Okta allows users to authenticate to Okta using Pulse Connect Secure as external SAML Identity Provider to enable Secure Single Sign-On to Cloud applications.

Prerequisites

Prerequisites for this solution include:

- Identity Provider: Pulse Connect Secure with minimum version of 8.2R3
- (Optional) MDM Server: Pulse Workspace Server/ MobileIron/ AirWatch
- Identity Management Provider: Okta

Figure 1 Overview



Pulse Connect Secure Configuration

The deployment discussed in the guide explores an alternative approach called IdP federation, where Cloud Secure (PCS) acts as IdP for Okta and handles all the authentication requests. This helps the customer to get the benefits of Cloud Secure such as compliance checks, secure single sign-on through VPN tunneling without making major changes to the existing setup. Pulse Connect Secure (PCS) is used as Identity Provider in Cloud Secure solution.

In this deployment scenario:

- PCS is configured as an IdP provider in Okta. See **Configuring Pulse Connect Secure - Basic Configurations (Mandatory).**
- Okta is configured as a third-party IdP in PCS. See Configure Okta as third-party IdP in PCS.
- Okta is configured as Service Provider in PCS. See Okta Configuration.

MobileIron and AirWatch Third-party MDM servers can also be used in this solution to manage devices and to evaluate compliance posture of the mobile devices.

Configure Okta as third-party IdP in PCS

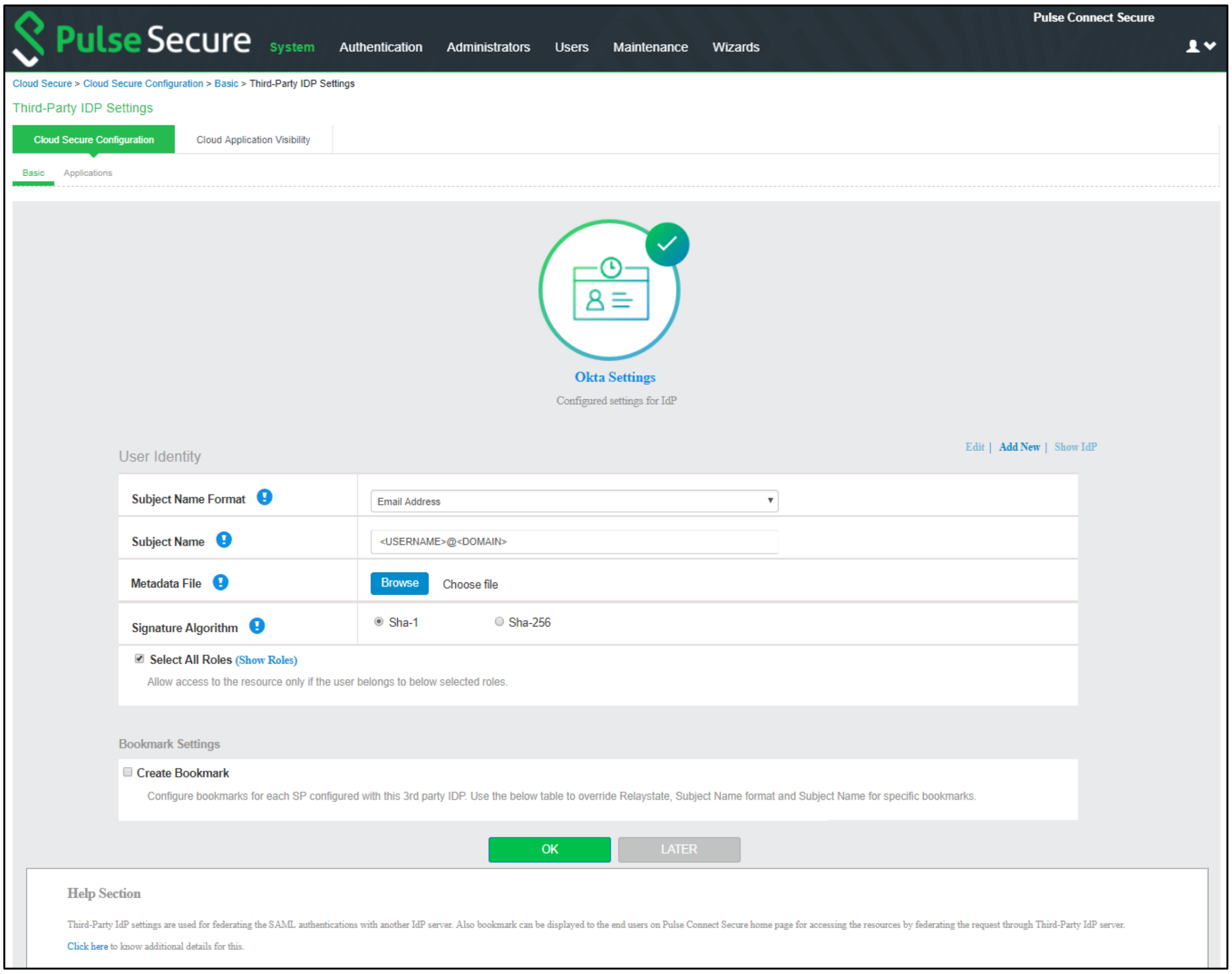
Cloud Secure can be configured with the new UX, which allows you to quickly and easily configure the Cloud Secure functionality without navigating into multiple pages. The new UX enhances the administrator experience through pre-populating some of the relevant settings and reusing the existing configurations.

Follow the below steps to configure Okta as third-party IDP on PCS:

1. Navigate to System > Cloud Secure > Cloud Secure Configuration.

   If you have completed the basic configurations and activated Cloud Secure. Click Open to go back to the Basic Configuration page.
2. Click Third-party IdP Settings:
   a. Click Add New and select the Third-party IdP as Okta.
   b. Select the Subject Name Format = Email Address.
   c. Enter the Subject Name.
   d. Click Browse and upload the metadata file (Step 7 of Okta Configuration).
   e. Set the signature algorithm to Sha-1 or Sha-256.
   f. Select the desired roles.
   g. Click OK.

Figure 2 Third-Party IdP Settings



Cloud Secure > Cloud Secure Configuration > Basic > Third-Party IDP Settings

Third-Party IDP Settings

Okta Settings

Configured settings for IdP

User Identity

Subject Name Format	Email Address ▾
Subject Name	<USERNAME>@<DOMAIN>
Metadata File	Browse Choose file
Signature Algorithm	● Sha-1 ○ Sha-256

☑ Select All Roles (Show Roles)

Allow access to the resource only if the user belongs to below selected roles.

Bookmark Settings

□ Create Bookmark

Configure bookmarks for each SP configured with this 3rd party IDP. Use the below table to override Relaystate, Subject Name format and Subject Name for specific bookmarks.

Help Section

Third-Party IdP settings are used for federating the SAML authentications with another IdP server. Also bookmark can be displayed to the end users on Pulse Connect Secure home page for accessing the resources by federating the request through Third-Party IdP server.

Click here to know additional details for this.

Okta Configuration

In this solution, Okta serves as Identity Management Provider. Okta acts as Identity Provider for Cloud services and as Service Provider for Pulse Connect Secure.

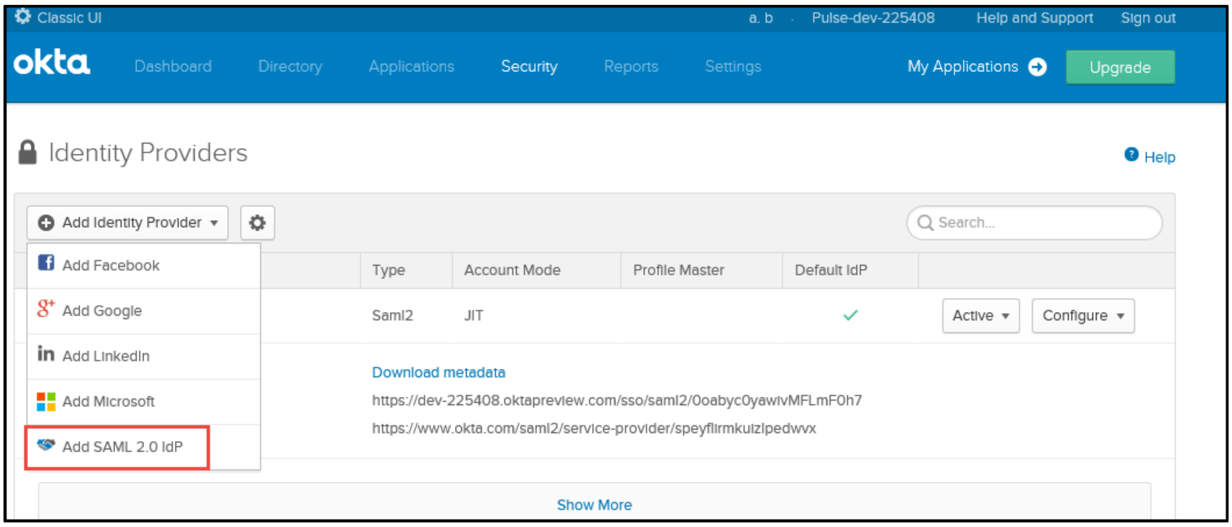
For Cloud Secure solution in Okta, configure the following:

- Add PCS as SAML IdP
- Configure Cloud Applications

Steps to Configure

To configure Okta as Service Provider, do the following:

1. Sign up for Okta developer account at https://www.okta.com/developer/signup.
2. If you see a < > **Developer** prompt in the top left, click it and select **Classic UI** to switch to the Classic UI.
3. Navigate to **Security > Identity Providers.** Click **Add Identity Provider.**
4. Select **Add SAML2.0 IdP** from the list.



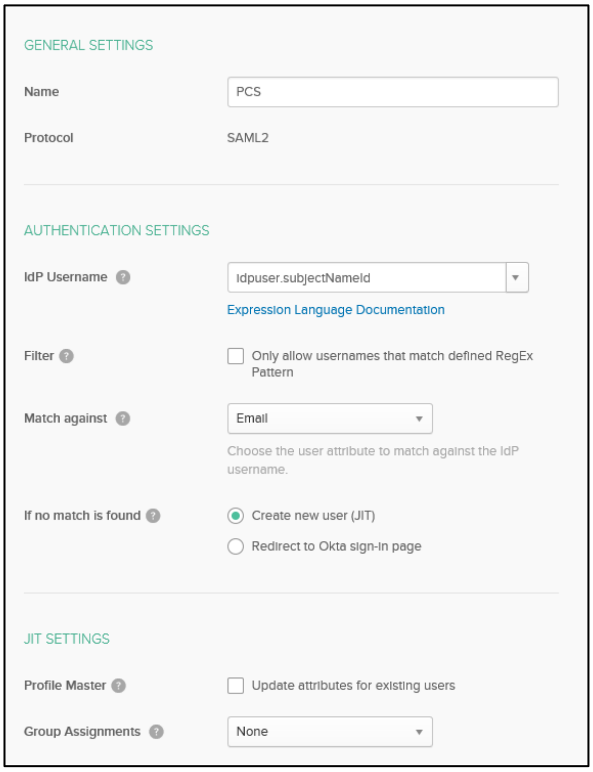
Type	Account Mode	Profile Master	Default IdP
Saml2	JIT		✓

https://dev-225408.oktapreview.com/sso/saml2/0oabyc0yawIvMFLmF0h7

https://www.okta.com/saml2/service-provider/speyflirmkulzlpedwvx

5. Provide the following details to configure Pulse Connect Secure as Identity Provider:
   a. Name = **<name reference to PCS>**
   b. Select the IdP username = Idpuser.subjectNameid.
   c. Match against = Email
   d. Under SAML Protocol Settings, enter the following:
      - IDP Issuer = https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi
      - IDP Login URL = https://<Alternate Host FQDN for SAML /dana-na/auth/saml-sso.cgi
      - Choose the IdP Signing Certificate configured under Authentication > Signin-in > Sign-in SAML > Identity Provider page of PCS and upload it (or)
      - Download PCS Metadata file from Authentication >Signing-in >Sign-in SAML > Metadata Provider. Copy Certificate content out of PCS Metadata to a file, save it, generate X509 Certificate out of it and upload it.
      - Click Show Advanced Settings, enable Sign SAML Authentication requests, set Request Binding = HTTP Redirect, Request/Response Signature Algorithm = SHA-1.
   e. Click **Add Identity Provider**.

Figure 3 Add Identity Provider



GENERAL SETTINGS

Name: PCS

Protocol: SAML2

AUTHENTICATION SETTINGS

IdP Username: idpuser.subjectNameId

Expression Language Documentation

Filter: □ Only allow usernames that match defined RegEx Pattern

Match against: Email

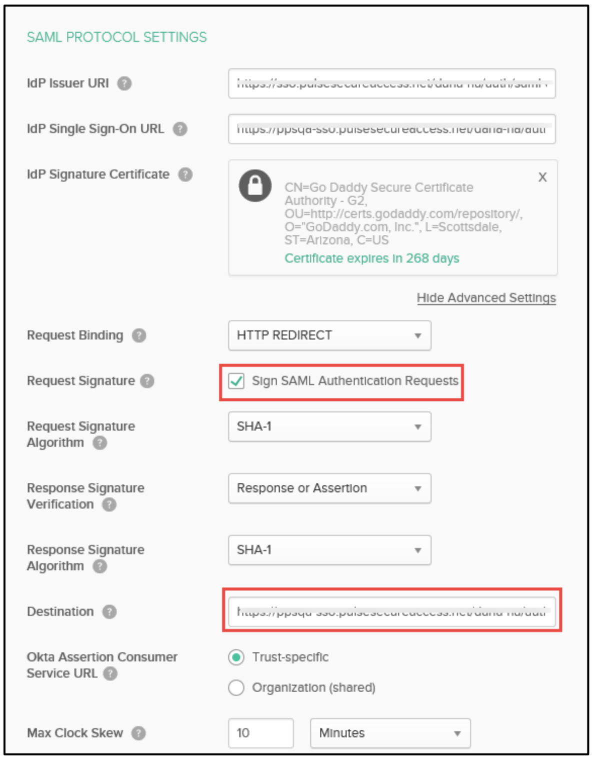
Choose the user attribute to match against the IdP username.

If no match is found: ● Create new user (JIT)
○ Redirect to Okta sign-in page

JIT SETTINGS

Profile Master: □ Update attributes for existing users

Group Assignments: None



SAML PROTOCOL SETTINGS

IdP Issuer URI: https://sso.pulsesecureaccess.net/dana-na/auth/saml

IdP Single Sign-On URL: https://ppsqa-sso.pulsesecureaccess.net/dana-na/auth

IdP Signature Certificate: CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US
Certificate expires in 268 days

Request Binding: HTTP REDIRECT

Request Signature: ☑ Sign SAML Authentication Requests

Request Signature Algorithm: SHA-1

Response Signature Verification: Response or Assertion

Response Signature Algorithm: SHA-1

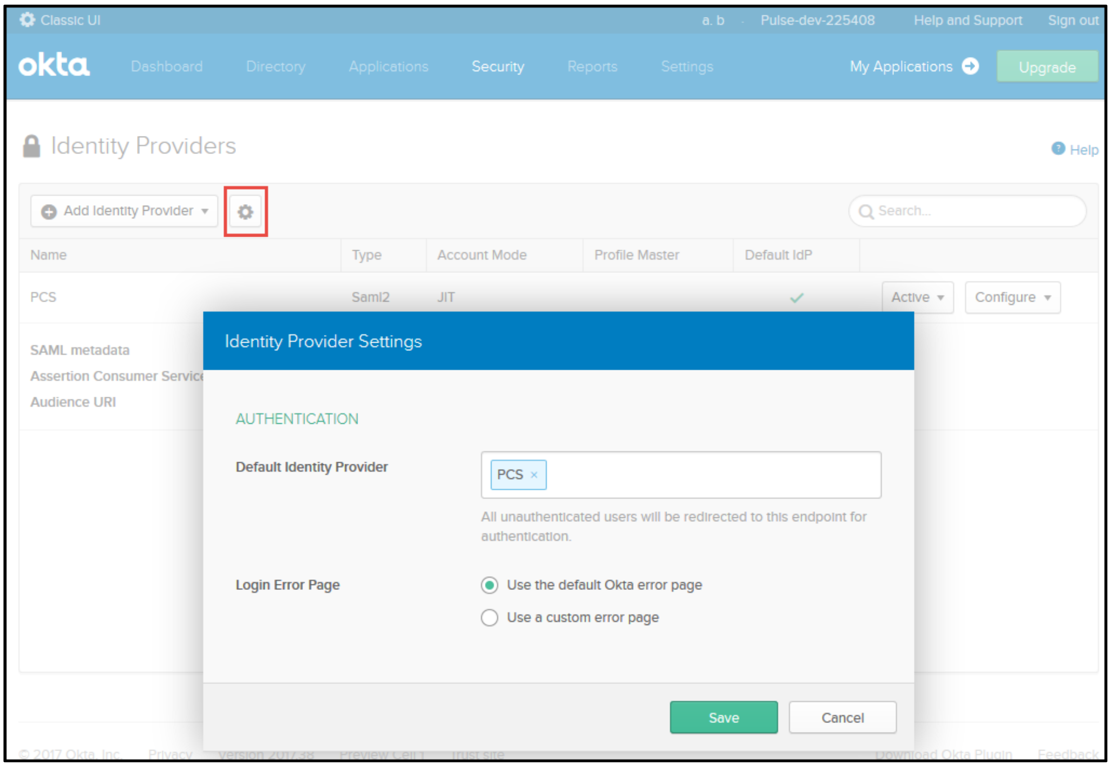
Destination: https://ppsqa-sso.pulsesecureaccess.net/dana-na/auth

Okta Assertion Consumer Service URL: ● Trust-specific
○ Organization (shared)

Max Clock Skew: 10 Minutes

6. Click the Settings icon next to Add Identity Provider and add the Identity Provider created as a default Identity Provider.

Figure 4 Default Identity Provider



Name	Type	Account Mode	Profile Master	Default IdP
PCS	Saml2	JIT		✓

SAML metadata
Assertion Consumer Servic
Audience URI

Identity Provider Settings

AUTHENTICATION

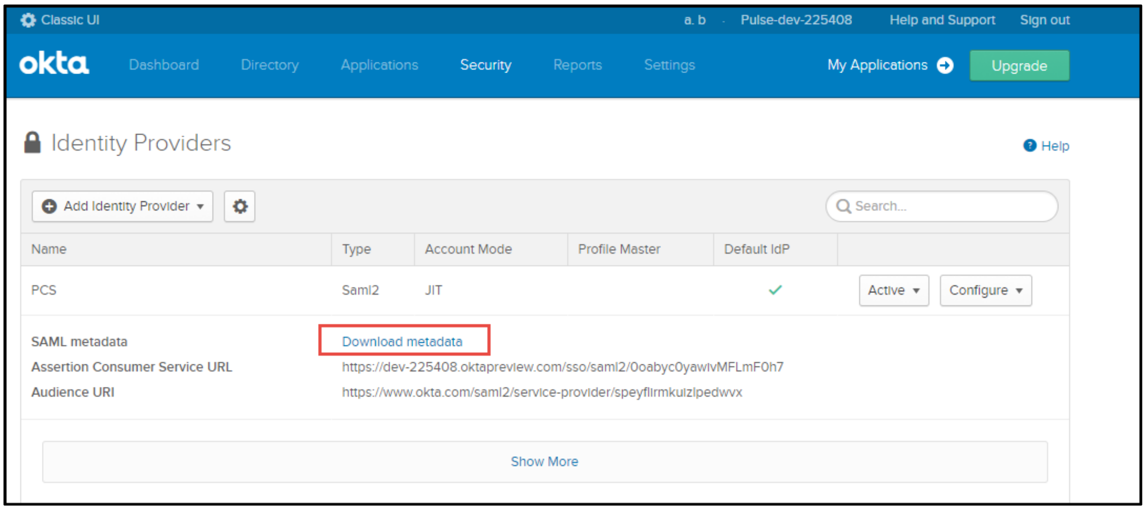
Default Identity Provider: PCS ×

All unauthenticated users will be redirected to this endpoint for authentication.

Login Error Page
● Use the default Okta error page
○ Use a custom error page

7. After adding Identity Provider, click **Download Metadata** and save the xml file.

Figure 5 Download SAML Metadata

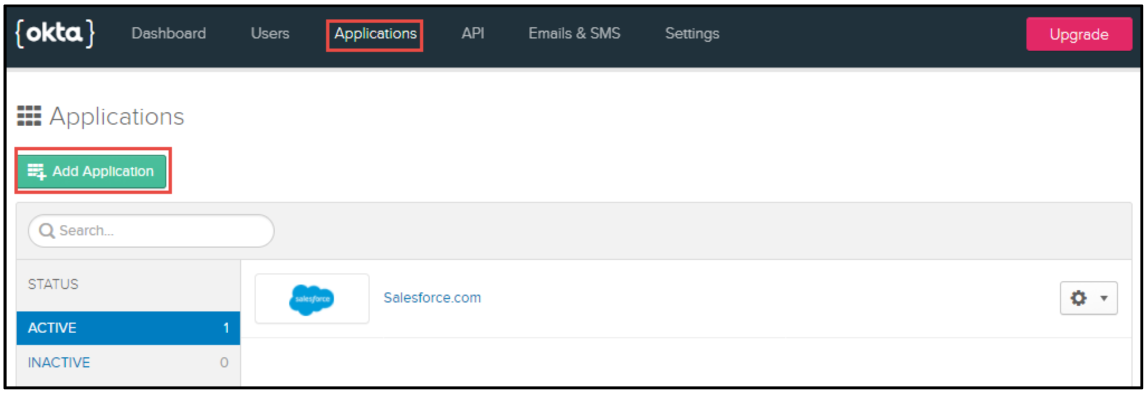


Name	Type	Account Mode	Profile Master	Default IdP
PCS	Saml2	JIT		✓

SAML metadata: Download metadata
Assertion Consumer Service URL: https://dev-225408.oktapreview.com/sso/saml2/0oabyc0yawlvMFLmF0h7
Audience URI: https://www.okta.com/saml2/service-provider/speyflirmkulzlpedwvx

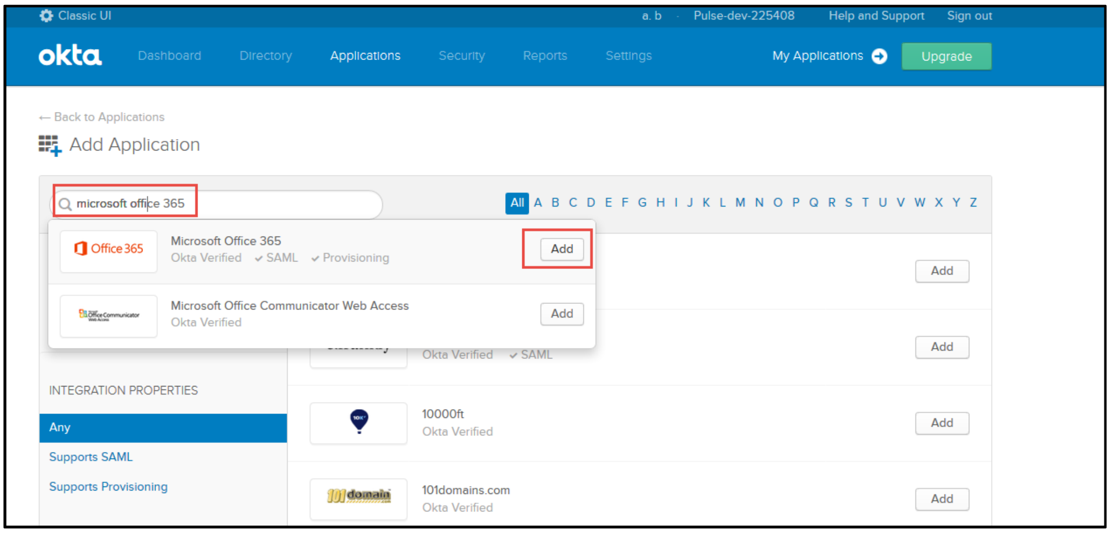
8. To add O365 application in Okta for SSO, do the following:
   a. Navigate to **Applications > Applications**.
   b. Click **Add Application**.

Figure 6 Add Application



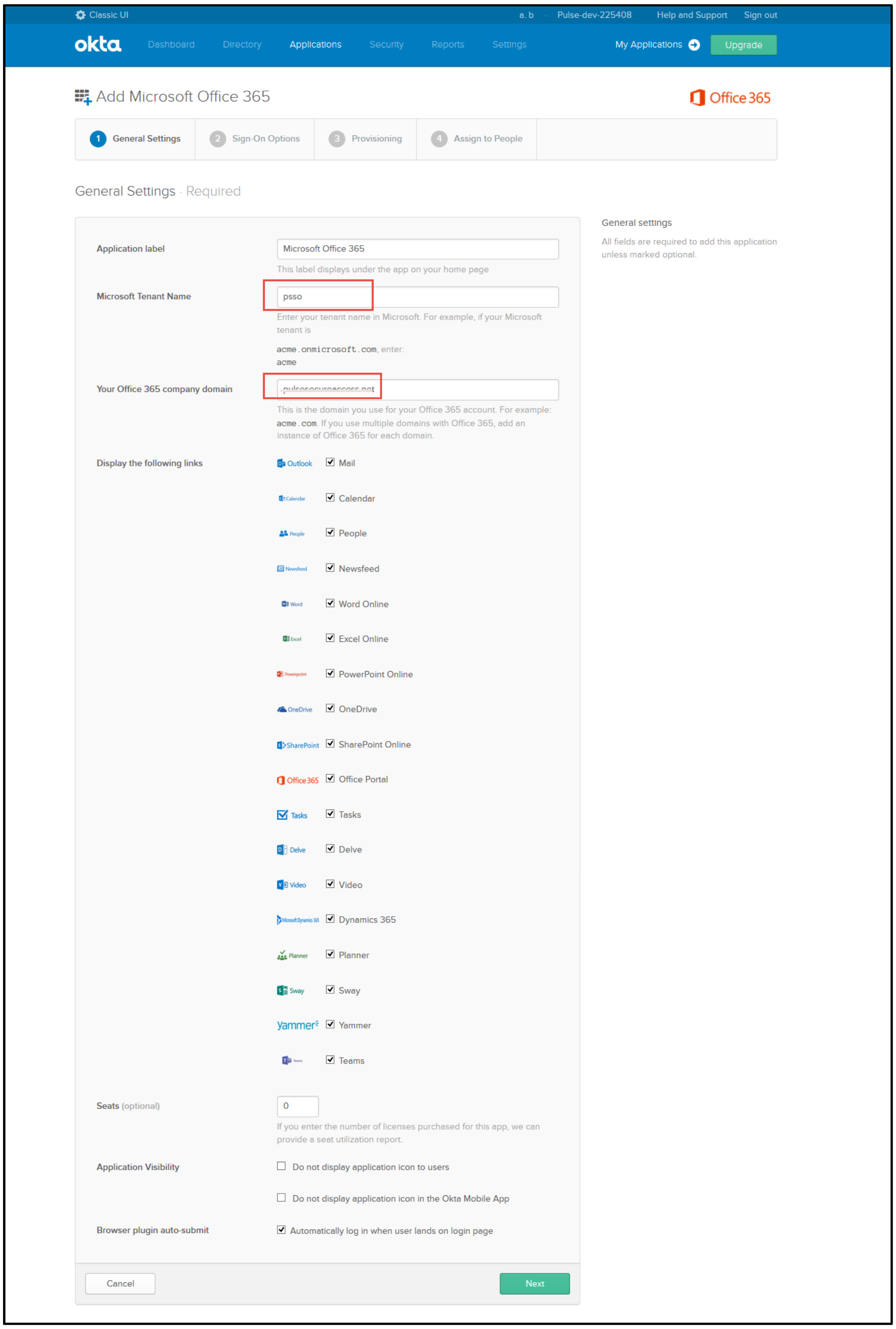
   c. Type **Microsoft Office 365** in search list and click **Add** on the Okta Verified O365 application.

Figure 7 Add Microsoft Office 365



d. Provide the Microsoft tenant name and O365 domain details and click **Next**.

Figure 8 General Settings



Add Microsoft Office 365

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

General Settings · Required

General settings

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

Application label: Microsoft Office 365

This label displays under the app on your home page

Microsoft Tenant Name: psso

Enter your tenant name in Microsoft. For example, if your Microsoft tenant is

`acme.onmicrosoft.com`, enter:
`acme`

Your Office 365 company domain: pulsesecureaccess.net

This is the domain you use for your Office 365 account. For example: `acme.com`. If you use multiple domains with Office 365, add an instance of Office 365 for each domain.

Display the following links

- Outlook ☑ Mail
- Calendar ☑ Calendar
- People ☑ People
- Newsfeed ☑ Newsfeed
- Word ☑ Word Online
- Excel ☑ Excel Online
- Powerpoint ☑ PowerPoint Online
- OneDrive ☑ OneDrive
- SharePoint ☑ SharePoint Online
- Office 365 ☑ Office Portal
- Tasks ☑ Tasks
- Delve ☑ Delve
- Video ☑ Video
- Microsoft Dynamics 365 ☑ Dynamics 365
- Planner ☑ Planner
- Sway ☑ Sway
- yammer ☑ Yammer
- Teams ☑ Teams

Seats (optional): 0

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

Cancel   Next

e. Under Sign-On Methods:

- Select **WS Federation** for Office 365, enter the admin credentials, and Select Application user name format as **Email**.

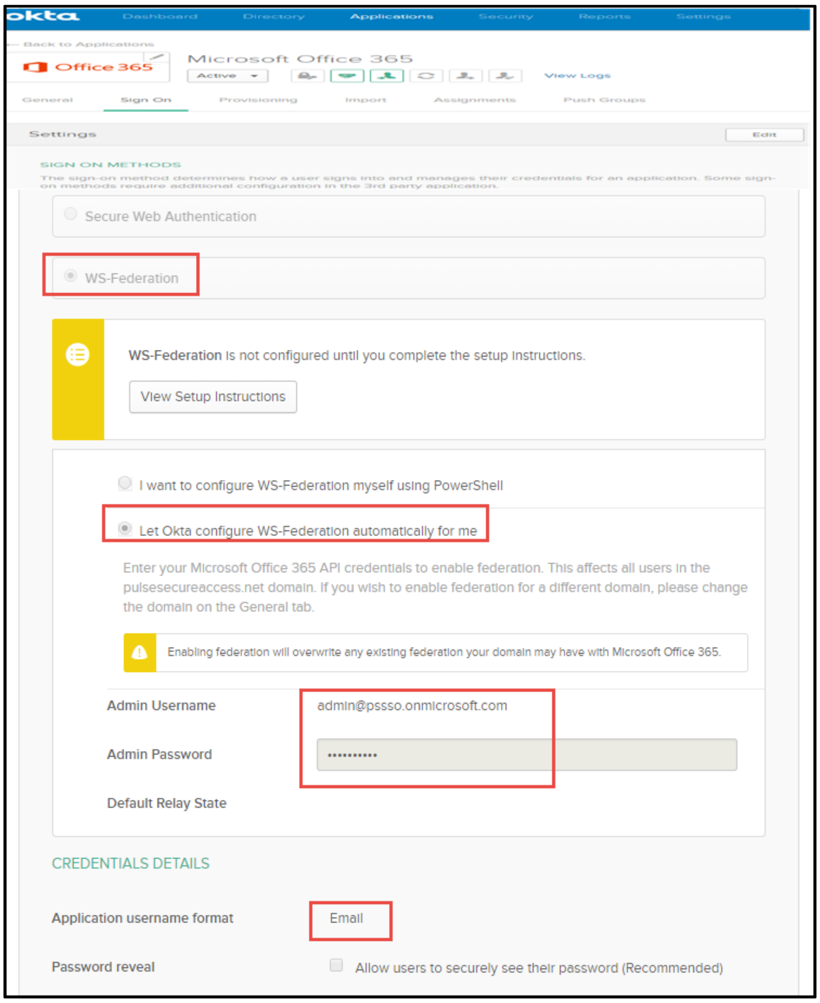
  Note: Select **SAML 2.0** for all the other applications.

- Select **Let Okta configure WS-Federation automatically for me** to automatically configure O365.

f. Click **Done**.

Note: If you select **I want to configure WS-Federation myself using powershell** then you have to configure office 3635 manually.

Figure 9 Sign--On



Microsoft Office 365

Settings

SIGN ON METHODS

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

○ Secure Web Authentication

● WS-Federation

WS-Federation is not configured until you complete the setup instructions.

View Setup Instructions

○ I want to configure WS-Federation myself using PowerShell

● Let Okta configure WS-Federation automatically for me

Enter your Microsoft Office 365 API credentials to enable federation. This affects all users in the pulsesecureaccess.net domain. If you wish to enable federation for a different domain, please change the domain on the General tab.

Enabling federation will overwrite any existing federation your domain may have with Microsoft Office 365.

Admin Username: admin@pssso.onmicrosoft.com

Admin Password: ••••••••••

Default Relay State

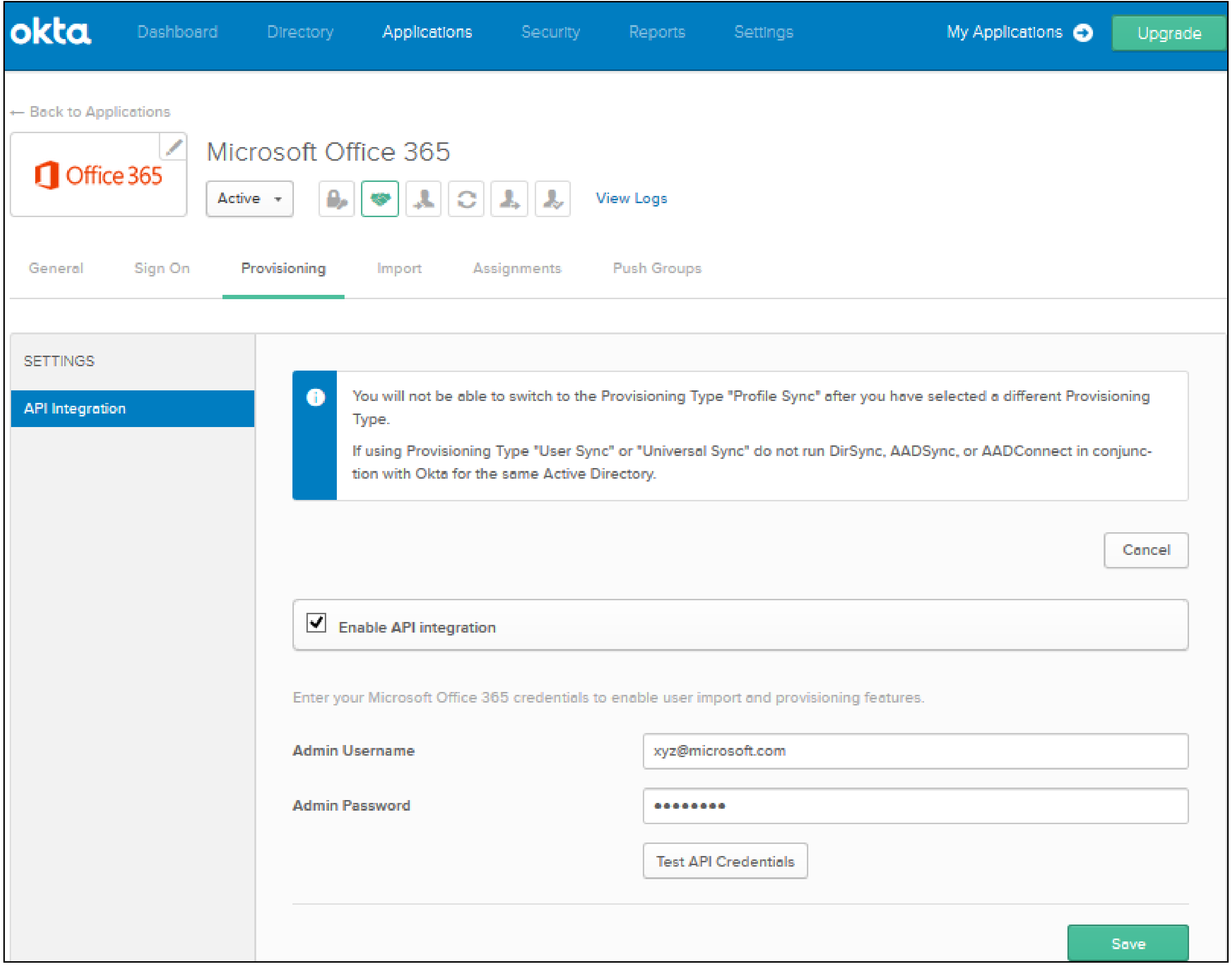
CREDENTIALS DETAILS

Application username format: Email

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

g. Under Provisioning Settings, Click Configure API Integration and Select Enable API Integration, enter the O365 admin credentials and click Save at the end of the page.

Figure 10 Enable Provisioning Features



You will not be able to switch to the Provisioning Type "Profile Sync" after you have selected a different Provisioning Type.

If using Provisioning Type "User Sync" or "Universal Sync" do not run DirSync, AADSync, or AADConnect in conjunction with Okta for the same Active Directory.

☑ Enable API integration

Enter your Microsoft Office 365 credentials to enable user import and provisioning features.

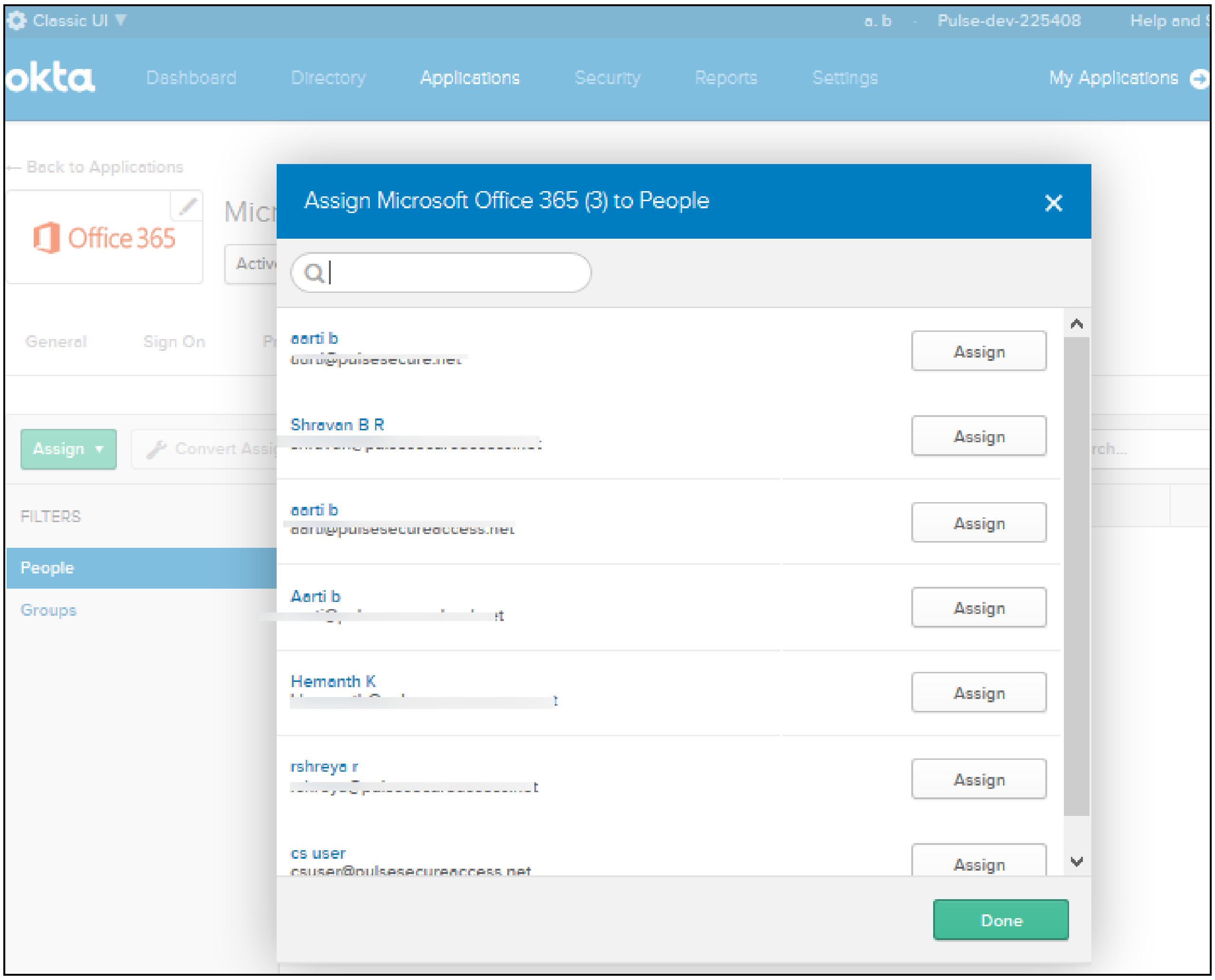
Admin Username: xyz@microsoft.com

Admin Password: ••••••••

h. Under **Assignments** > **Assign** > **Assign to People**. Click **Next**.

i. Select the user and click **Assign**.

Figure 11 Assign O365



Assign Microsoft Office 365 (3) to People

aarti b
[redacted]
Assign

Shravan B R
[redacted]
Assign

aarti b
[redacted]
Assign

Aarti b
[redacted]
Assign

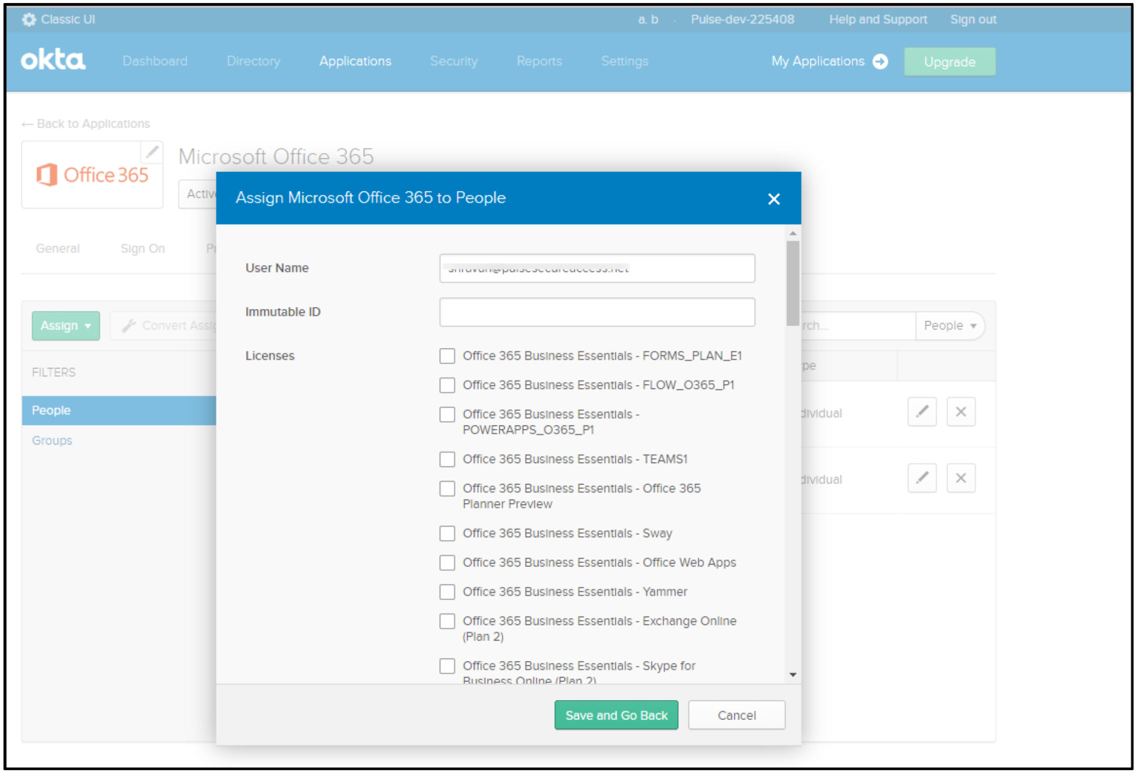
Hemanth K
[redacted]
Assign

rshreya r
[redacted]
Assign

cs user
csuser@pulsesecureaccess.net
Assign

j. Select the license from the O365 licenses list.

Figure 12 Assign O365 License Type



Assign Microsoft Office 365 to People

User Name: shravan@pulsesecureaccess.net

Immutable ID:

Licenses:

- □ Office 365 Business Essentials - FORMS_PLAN_E1
- □ Office 365 Business Essentials - FLOW_O365_P1
- □ Office 365 Business Essentials - POWERAPPS_O365_P1
- □ Office 365 Business Essentials - TEAMS1
- □ Office 365 Business Essentials - Office 365 Planner Preview
- □ Office 365 Business Essentials - Sway
- □ Office 365 Business Essentials - Office Web Apps
- □ Office 365 Business Essentials - Yammer
- □ Office 365 Business Essentials - Exchange Online (Plan 2)
- □ Office 365 Business Essentials - Skype for Business Online (Plan 2)

Save and Go Back | Cancel

k. Click **Save and Go Back**.

l. Click **Done** to complete the configuration.

Note: To login to Okta developer account as admin without Single Sign-On, use https://<Okta Domain>/login/do-login.

End-User Flow on Mobile Devices

Once the administrator completes the above configurations and creates a new user in Pulse Workspace, user has to follow the below steps to register the mobile device with Pulse Workspace and get seamless secure Single Sign-On access to O365 Application. For PWS registration, see Provisioning Devices.

1. Access O365 application and provide the domain details.
2. VPN tunnel will automatically get established for iOS, For Android devices, establish the Pulse VPN connection manually and then click the O365 application.
3. Single Sign-On will happen and user will get access to the O365 applications.

End-User Flow on Desktops

Once the administrator completes the above configurations, user can access O365 domain through browser from Windows/MAC OS X Desktops. Follow the below steps to enable Secure Single Sign-On browser-based access to O365 Cloud Service.

1. Launch Pulse Client and establish a VPN session with PCS.
2. Open any web browser on the desktop.
3. Access SSO enabled O365 domain.
    a. If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in and the PCS will send SAML response to Okta.
    b. If user did not establish Pulse VPN session as mentioned in Step 1, then the user will be redirected to Okta which in turn redirects the request to Pulse Connect Secure user login page or user will be prompted to select user certificate for authentication depending on the PCS configuration. Once authenticated, PCS will send SAML response to Okta.
4. Okta forwards the SAML response to O365 and user will be granted access to O365 Cloud Service.

Troubleshooting

Single Sign-On for a user can fail due to configuration issues on Pulse Connect Secure, O365, Okta or Pulse Workspace.

To troubleshoot issues with Single Sign-On:

- On PCS, under **Maintenance > Troubleshooting,** enable the event codes – “saml, auth” at level “50” and collect debug logs. Enable **Policy Tracing** and capture the Policy traces for the specific user.
- Check **System > Log/Monitoring > User Access > Log for SAML AuthNRequest and Response** for the specific user. Verify if **Subject Name** is proper in the SAML Response.
- Log in to Okta Domain as admin. Navigate to **Dashboard > Dashboard**. Check the recent activity events to debug the failures.
- On mobile device, open Pulse Client and Send Logs to your administrator.