Logging in with Single Sign-On (SSO) through Okta

Contents

All ePMX users have the ability to configure a default Identity Provider to power Single Sign On (SSO). This document details how to configure Okta as the primary Identity Provider to facilitate SSO with the ePMX application.

Supported Features

- Service Provider (SP)-Initiated Authentication (SSO) Flow - This authentication flow occurs when the user attempts to log in to the application from Cerby.
- Identity Provider (IDP)-Initiated Authentication (SSO) Flow - This authentication flow occurs when the user attempts to log in to Cerby from Okta.

Requirements

In order to proceed with configuring login with SSO through Okta, you must:

- Have access to an Okta tenant
- Be an Okta administrator to that tenant
- Have completed ePMX onboarding

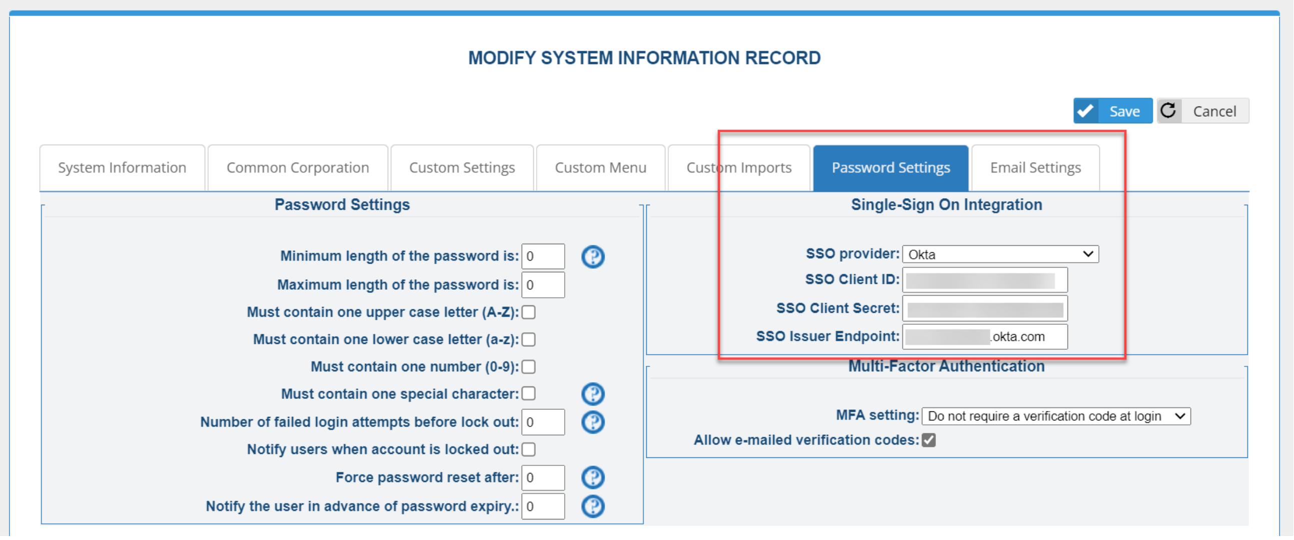
If you have not yet completed ePMX onboarding, please email customersuccess@bellwethercorp.com for assistance.

Configuration Steps

The following steps will walk you through the configurations needed to set up the OIDC integration Okta and ePMX.

1. Enabling the Single Sign On Integration

1. Login to your ePMX as an Administrator.
2. Navigate to Master Files System Information.
3. Click onto the Password Settings tab.
4. Under Single-Sign On Integration, select “Okta” in the SSO provider dropdown.
   You will notice three fields which need data from your Okta account: SSO Client ID, SSO Client Secret and SSO Issuer Endpoint.



MODIFY SYSTEM INFORMATION RECORD

Password Settings

Minimum length of the password is: 0
Maximum length of the password is: 0
Must contain one upper case letter (A-Z): □
Must contain one lower case letter (a-z): □
Must contain one number (0-9): □
Must contain one special character: □
Number of failed login attempts before lock out: 0
Notify users when account is locked out: □
Force password reset after: 0
Notify the user in advance of password expiry.: 0

Single-Sign On Integration

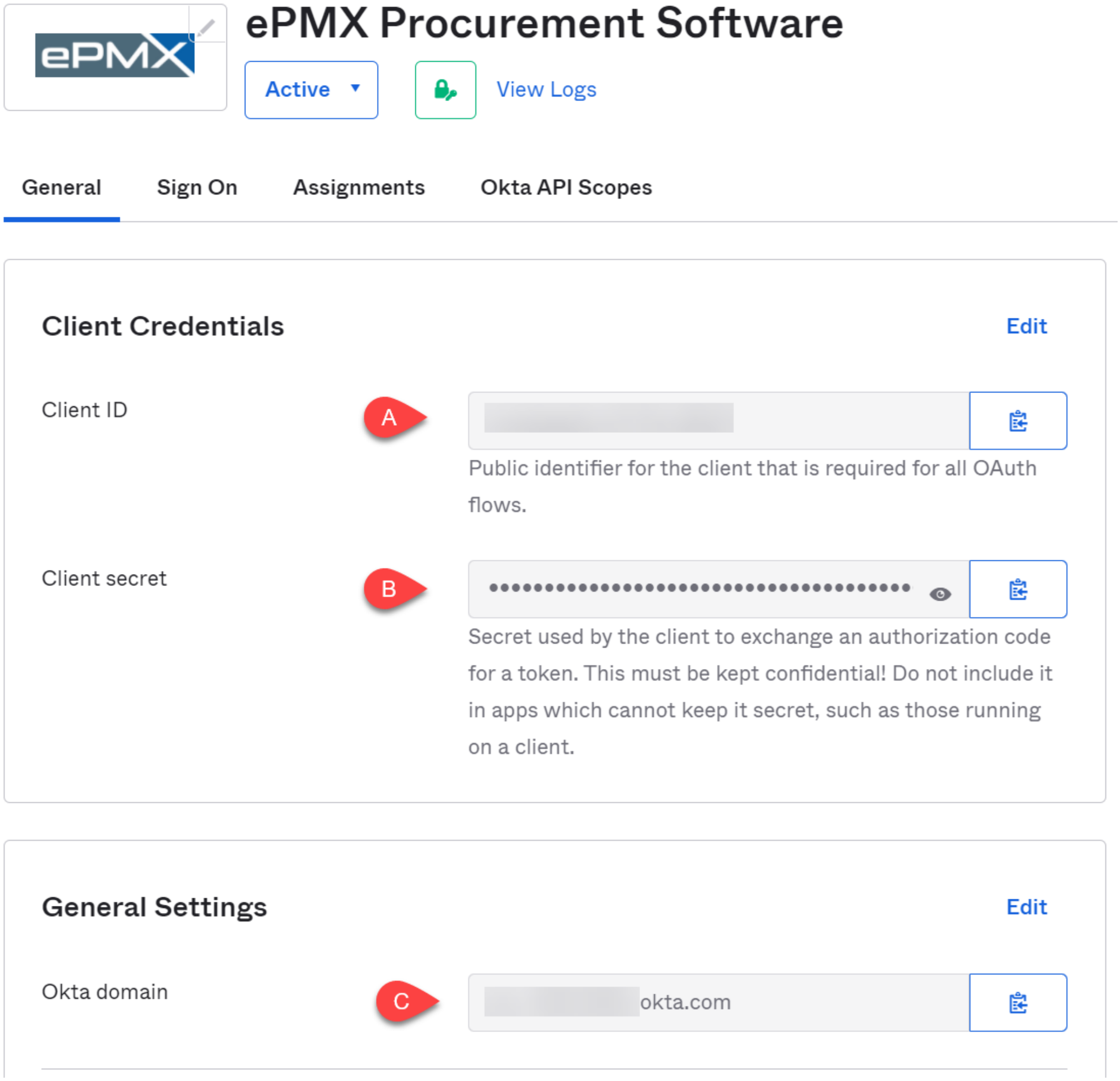
SSO provider: Okta
SSO Client ID: [redacted]
SSO Client Secret: [redacted]
SSO Issuer Endpoint: [redacted].okta.com

Multi-Factor Authentication

MFA setting: Do not require a verification code at login
Allow e-mailed verification codes: ☑

For steps 5 and 6, <u>you will need to log into your Okta account as an Okta Administrator.</u>

5. In Okta, go to Applications->ePMX Procurement Software and find the required data.
   a. SSO Client ID – Enter ePMX's Okta Application's "Client ID", found under "Client Credentials".
   b. SSO Client Secret – Enter ePMX's Okta Application's "Client secret", found under "Client Credentials".
   c. SSO Issuer Endpoint – Enter ePMX's Okta Application's "Okta domain", found under "General Settings".



ePMX Procurement Software

Client Credentials

Client ID [redacted]

Public identifier for the client that is required for all OAuth flows.

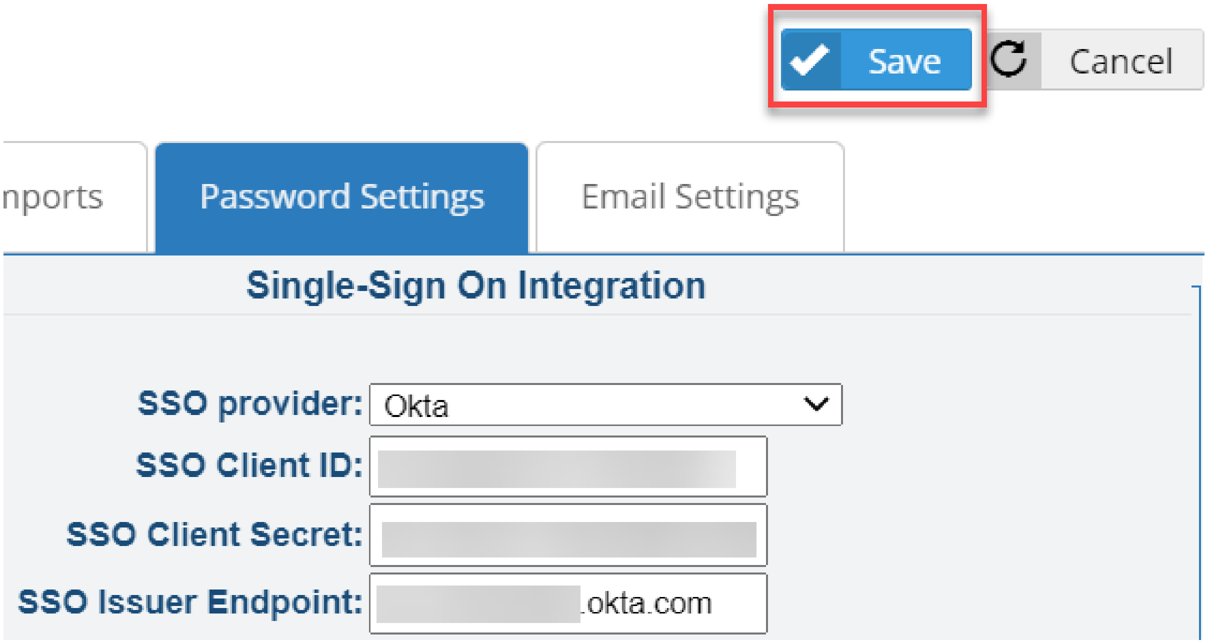
Client secret ••

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

General Settings

Okta domain [redacted]okta.com

   d. In ePMX, click the blue Save button located above the Password Settings tab.



Single-Sign On Integration

SSO provider: Okta

SSO Client ID: [redacted]

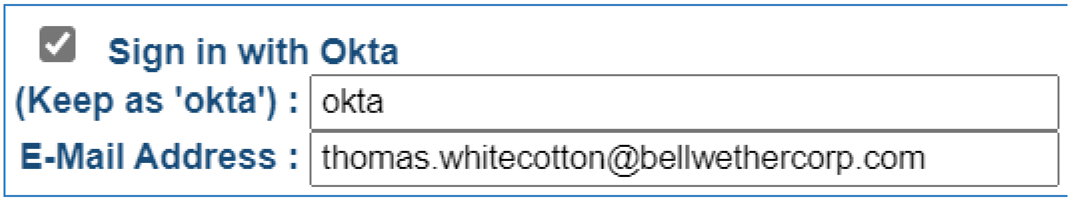
SSO Client Secret: [redacted]

SSO Issuer Endpoint: [redacted].okta.com

6. In Okta, while still on Applications->ePMX Procurement Software, click the Assignments tab.
   a. Click **Assign** and then select either **Assign to People** or **Assign to Groups**.
   b. Enter the appropriate people or groups that you want to have Single Sign-On into your application, and then click **Assign** for each.
   c. For any people that you add, verify the user-specific attributes, and then select **Save and Go Back**.
   d. Click **Done**.

2. Populate Employee Okta E-Mail Addresses

1. Login to your ePMX as an Administrator.
2. Navigate to Master Files Employee record.
3. Select the user you want to allow Okta SSO for, then click the Modify button.
4. If not already checked, check the box at the bottom right which says “Sign in with Okta”.
5. The first box should remain “okta” (without the quotes).
6. Type in the employee’s correct Okta e-mail address in the second box.



☑ Sign in with Okta

(Keep as 'okta') : okta

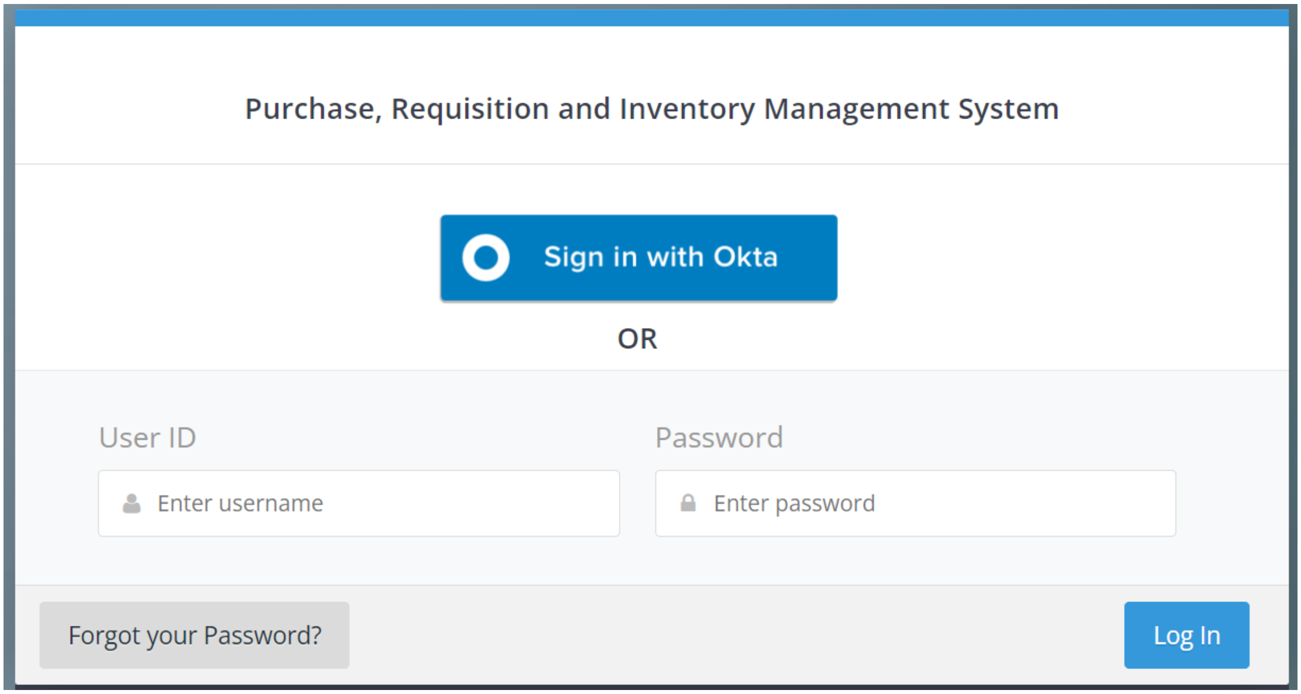
E-Mail Address : thomas.whitecotton@bellwethercorp.com

7. Click the blue Save button located at the top right of the page.

Notes

Signing into ePMX with Okta

1. Open the ePMX URL to bring up the login screen.
2. Click the “Sign in with Okta” button.



3. If you are already signed into Okta, you will automatically logged into ePMX as your user. Otherwise, you will need to sign into Okta first, and you will redirect straight into ePMX.

Permissions

ePMX’s integration with Okta leverages Okta only for authentication. To assign permissions for ePMX, users must do so directly within ePMX. For assistance with ePMX user permissions, please contact support@bellwethercorp.com