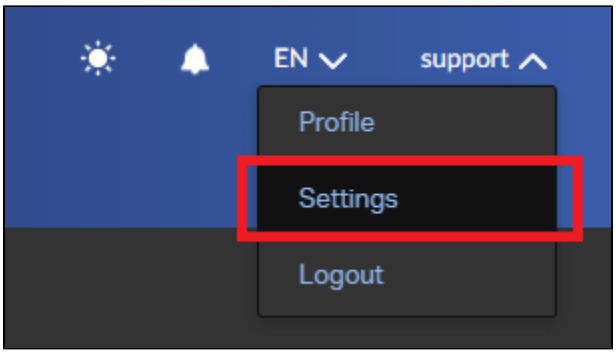
Configure single sign-on with Management Portal

Created date	Updated date	Affects version	Fix version
29 Nov 2023	24 Jun 2024	Management Portal	N/A

Description

Single sign-on simplifies the login process, enhances security and improves the overall user experience. This page introduces the single sign-on feature available in the Blancco Management Portal. Also set of instructions is available to configure and enable SSO for Microsoft Entra ID (Azure AD).

In Blancco Management Portal Single sign-on settings are available for manager users or user with a custom role granting "Configure SSO" authority. SSO settings are available under user's "Settings" which can be accessed by clicking your username from the top right corner of the screen.



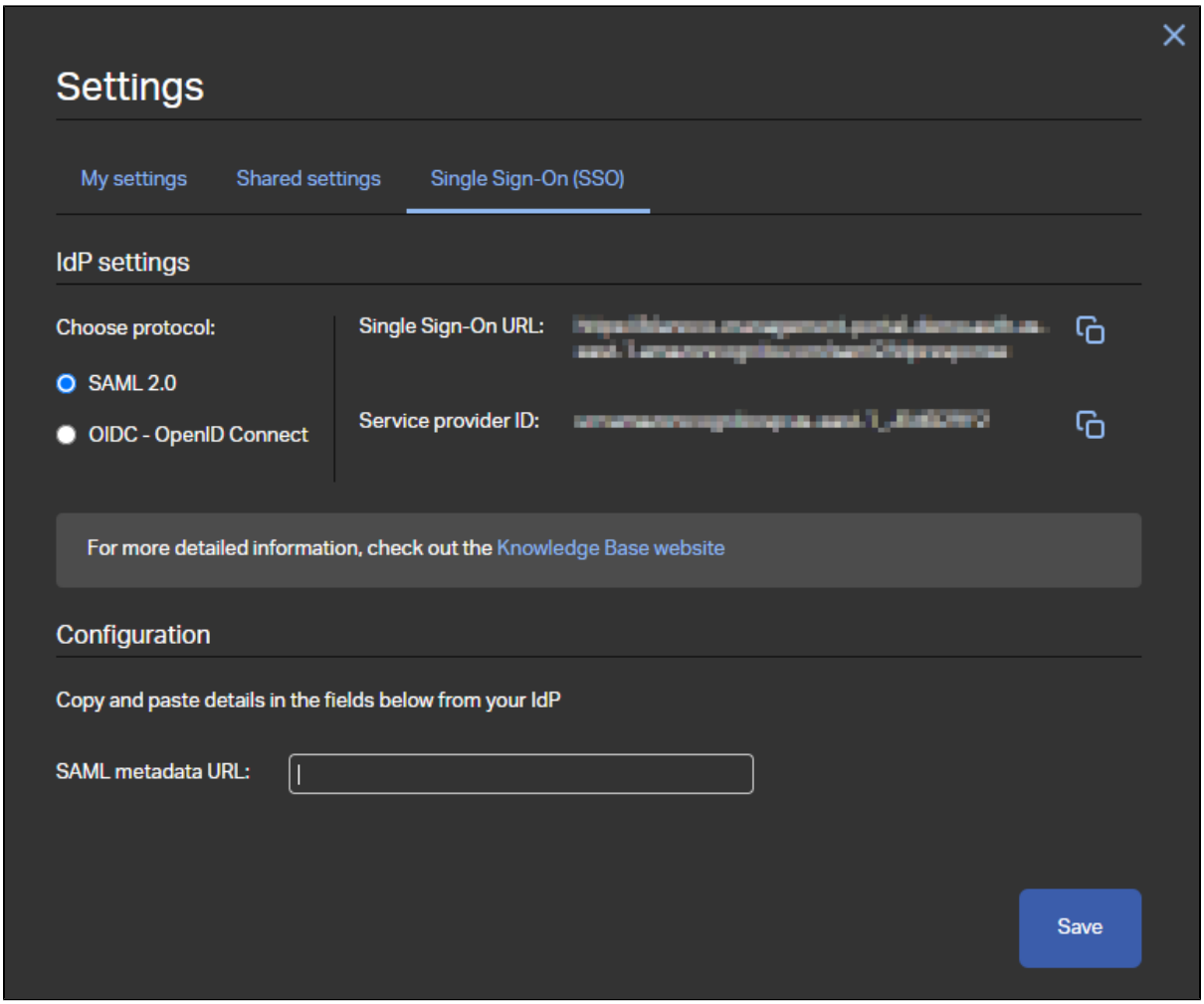
If the user has authority to configure the SSO setting a "Single Sign-On (SSO)" tab should be available. This tab contains all the SSO related settings and provides all the required details to set it up.

Single sign-on in Blancco Management Portal also supports user provisioning. This allows Blancco Management Portal to create user automatically to the corresponding tenant when they initially authenticate using single sign-on.
Note that single sign-on is not supported with Blancco erasure products such as Blancco Drive Eraser or Blancco Mobile Diagnostics and Erasure. Communication between an erasure client and Management Portal requires an internal password of the account to be used.

Single sign-on is only supported when logging in to the Management Portal at https://portal.blancco.cloud

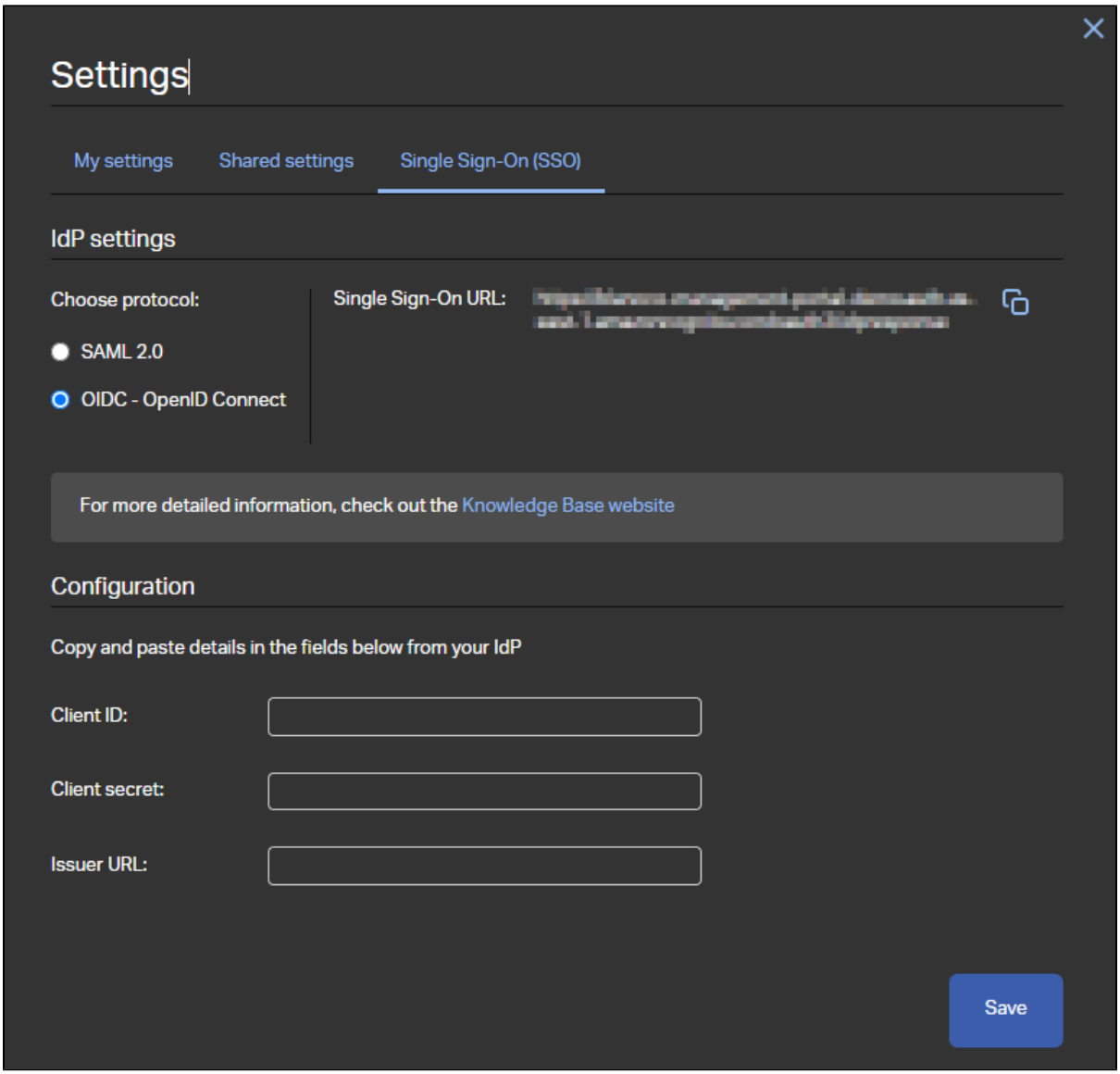
Settings available for SAML 2.0

- Single Sign-On URL - This URL is used as the reply URL/assertion URL as well as the sign on URL on the identity provider configuration.
- Service Provider ID - This value is used as the identifier or the entity ID on the identity provider configuration when setting up SAML SSO.
- SAML metadata URL - User needs to provide a valid URL from where the corresponding metadata for the SAML can be found. This URL should be available from the identity provider details after configuring the SSO.



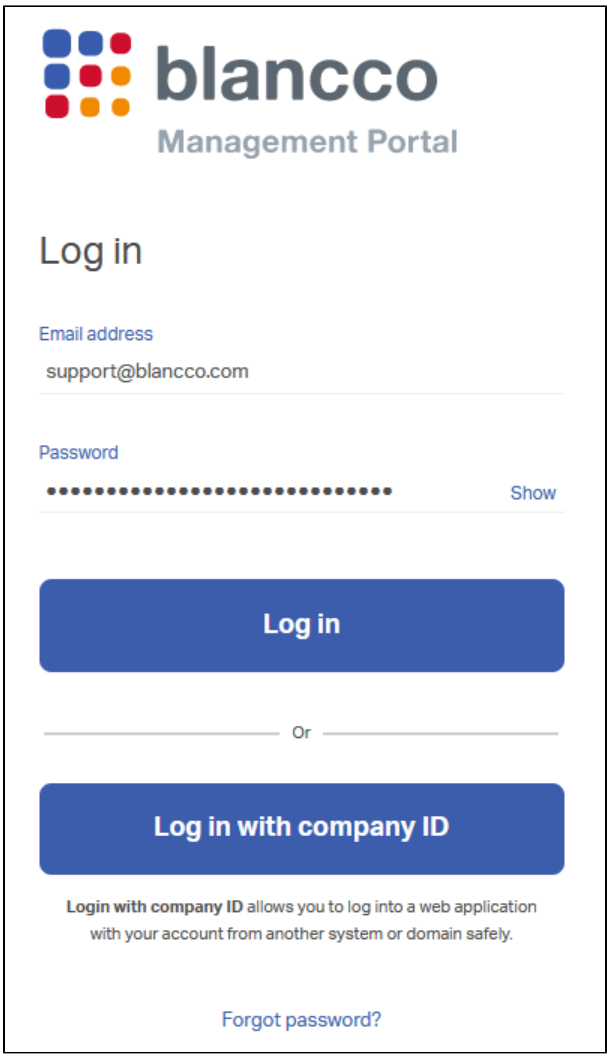
Settings available for OpenID Connect

- Single Sign-On URL - This URL is used as the reply/redirect URL when configuring the SSO settings on the identity provider side.
- Client ID - Application/Client ID of the identity provider.
- Client secret - A string based key used as the authentication technique.
- Issuer URL - Similar to *https://login.microsoftonline.com/GUID/v2.0* where GUID corresponds to Entra/Azure tenant ID.



Log in using Single Sign-On

After single sign-on is configured and available for the user, "Log in with company ID" button appears on the Management Portal login screen.



If no email address is provided or the user account in question doesn't have SSO configured this button is not available.

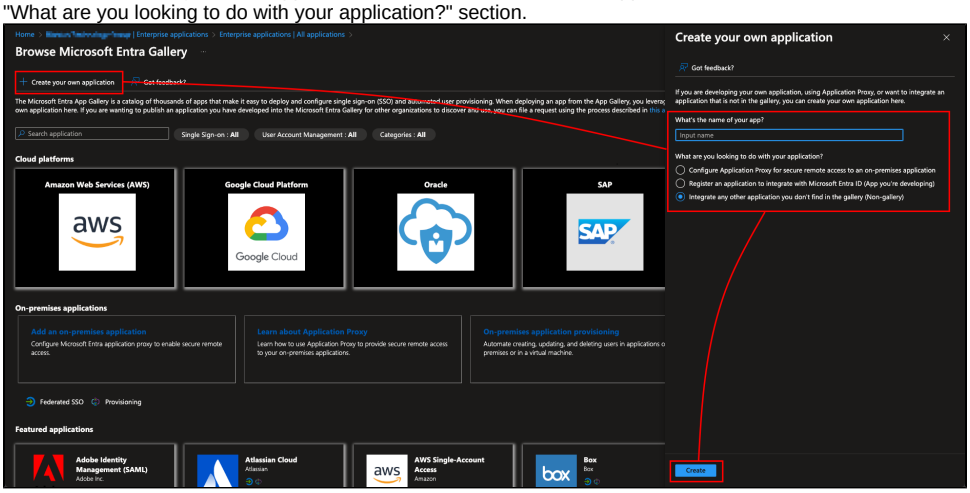
Using the "Log in" button authenticates the user using the internal password of the account and not through the single sign-on.

Microsoft Entra ID/Azure AD - SSO with SAML 2.0

Follow these steps to set up single sign-on with Azure AD using SAML 2.0.

1. Create a new enterprise application by opening Entra ID "Enterprise applications" "New application".

Then select "Create your own application" and fill in the name of the application. Also make sure to select the "Non-gallery" option under the "What are you looking to do with your application?" section.

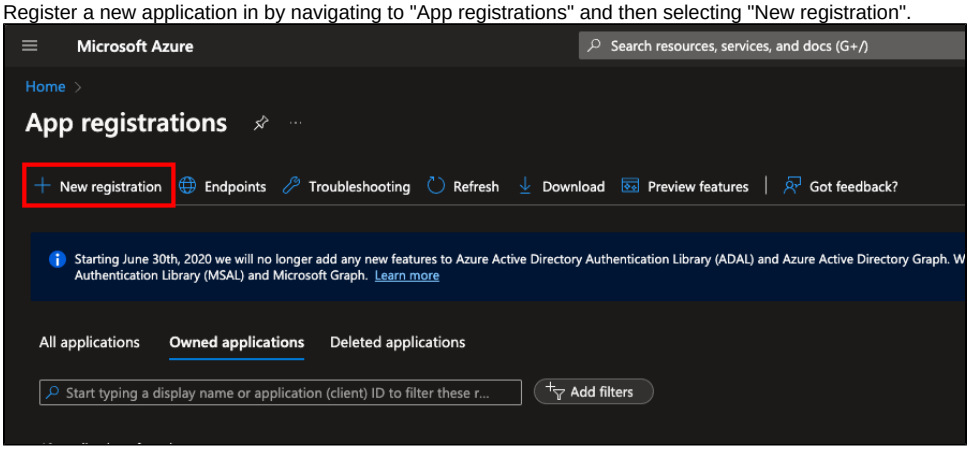


2. Assign corresponding users/groups to the newly created application (this defines the list of users who are allowed to sign in using SSO). Alternatively you can disable the Properties option "Assigment required?" to allow any user in your Entra ID tenant to login using SSO.
3. Configure required settings under the "Single sign-on" tab (make sure to select "SAML" as the sign-on method)
    a. Under the "Basic SAML Configuration" define "Identifier (Entity ID)", "Reply URL (Assertion Consumer Service URL)" and "Sign on URL".
        i. "Identifier (Entity ID)" corresponds to "Service Provider ID" available in the BMP SSO settings
        ii. "Reply URL (Assertion Consumer Service URL)" and "Sign on URL" both correspond to Single Sign-On URL available in the BMP SSO settings.
    b. Under "Attributes & Claims" the "name" attribute should be set to "user.displayname" (by default this is set to "user.userprincipalname").
    c. Acquire "App Federation Metadata Url" which is available under "SAML Certificates" section and copy the URL to BMP SSO settings to the "SAML metadata URL" field.

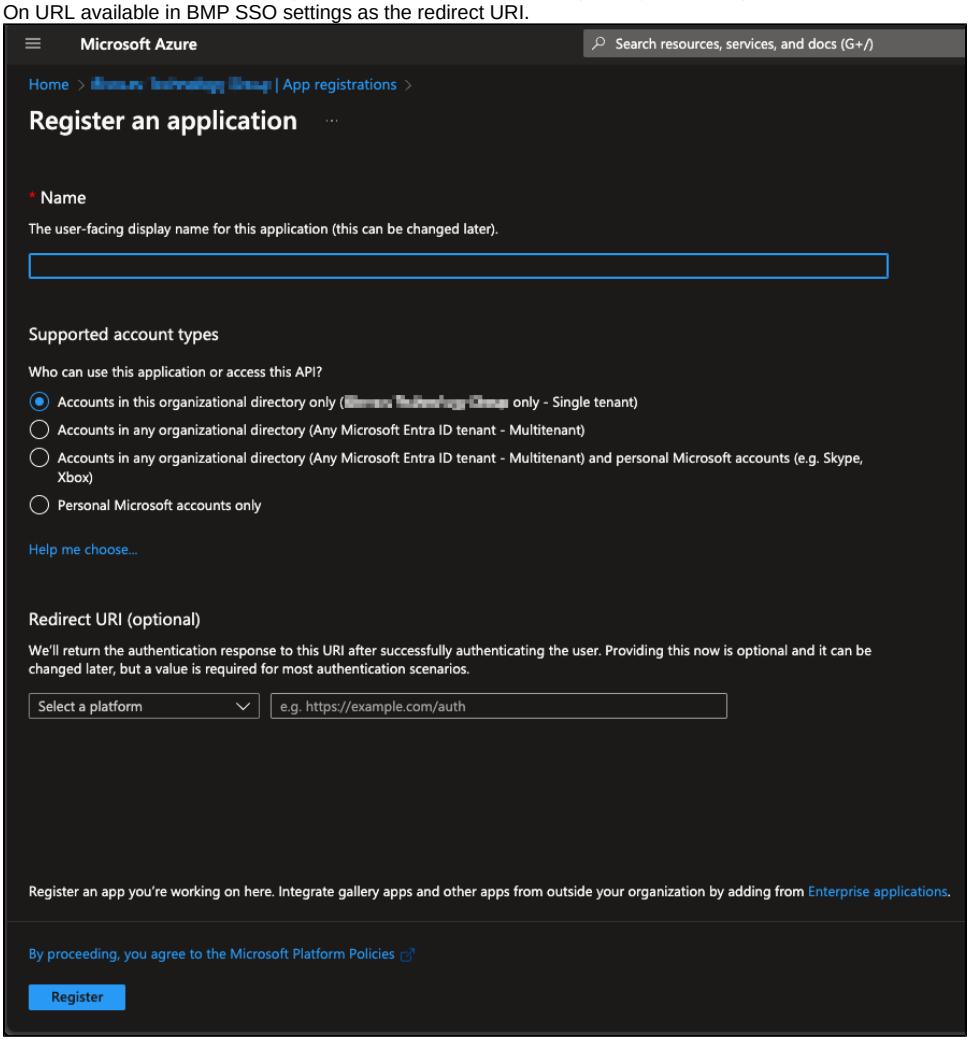
Microsoft Entra ID/Azure AD - SSO with OpenID Connect

Follow these steps to set up single sign-on with Azure AD using OpenID Connect.

1. Register a new application in by navigating to "App registrations" and then selecting "New registration".



Fill in the name and select appropriate account type, in this example single tenant option is selected. Set the "Redirect URI", use the Single Sign-On URL available in BMP SSO settings as the redirect URI.



2. After registering the app copy "Application (client) ID" from the app to the BMP SSO settings "Client ID" field.
3. Navigate to "Certificates & secrets" to generate new client secret by selecting "New client secret" under the "Client secrets" -tab.
    a. Define description and expiration for the secret and click "Add".
    b. After creating a new secret copy secret's value and enter it as the "Client secret" in BMP SSO settings.

    Note that the secret value is only shown right after creating a secret. If the value is already hidden and wasn't copied over a new secret needs to be created.
4. Navigate to "API permissions" and grant admin consent for the "User.Read" API/Permission. This enables the system to check required user attributes need for the SSO authentication.
5. Navigate to "Authentication" and make sure "Redirect URIs" is configured. If this was already configured when creating new app registration, this step can be ignored.
    a. Use the Single Sign-On URL available in BMP SSO settings as the redirect URI.
6. Acquire "Issuer URL" from the "OpenID Connect metadata document".
    a. Open the document and locate "issuer" field from the document and copy the value to "Issuer URL" field in BMP SSO settings.

Limiting user and group access for the OpenID Connect SSO

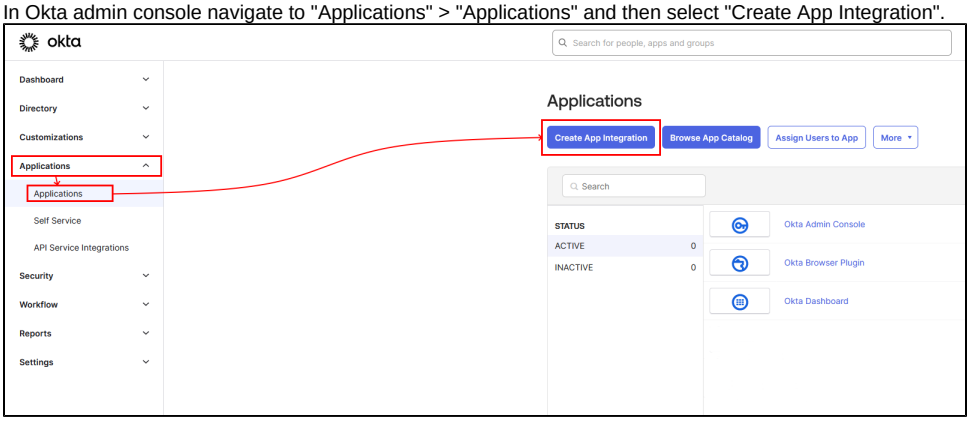
When the new application was registered as part of the previous steps, the system should have created an Enterprise Application with the same name automatically. This Enterprise Application can be used to control the list of users and groups who are allowed to use the SSO (similarly as with the SAML).

1. Go to "Enterprise Applications" and locate the correct app, it should have the same name as the App registration which was created on the above steps.
2. Navigate to "Properties" and set "Assignment required?" to "Yes".
3. Navigate to "Users and groups" and define the list of users and/or groups allowed to sign in using SSO.

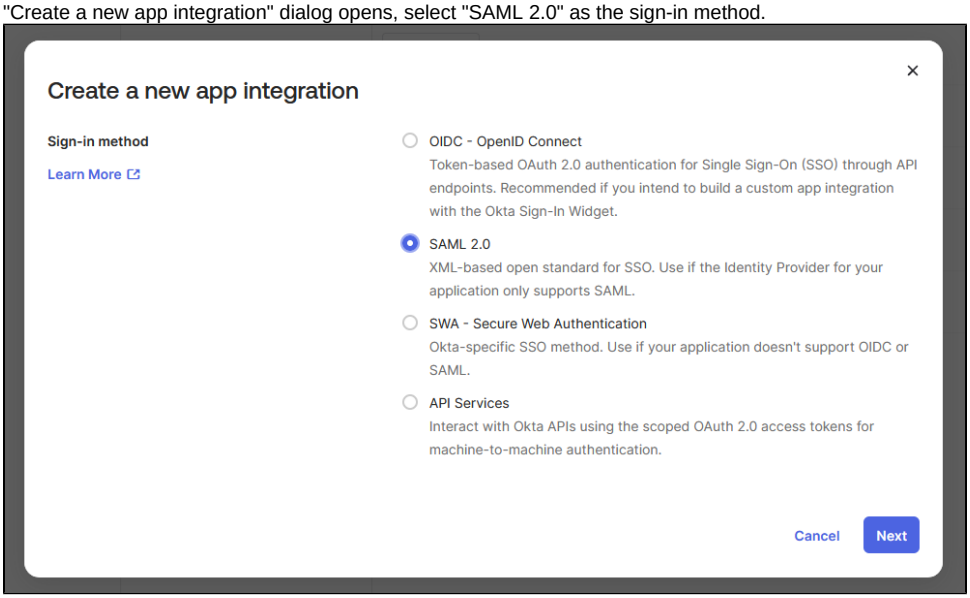
Okta - SSO with SAML 2.0

To set up Okta SSO authentication, access the Okta admin console and follow below steps to set up a new app integration:

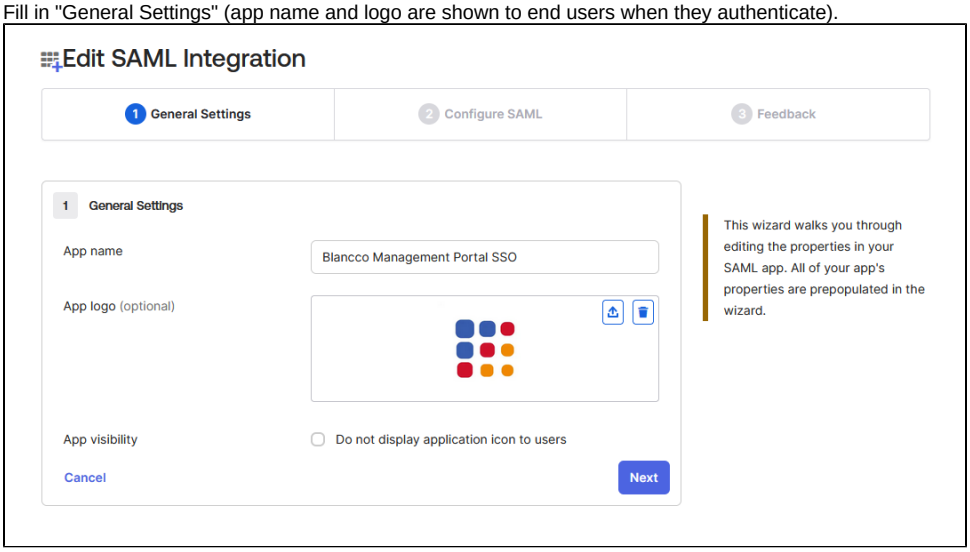
1. In Okta admin console navigate to "Applications" > "Applications" and then select "Create App Integration".



2. "Create a new app integration" dialog opens, select "SAML 2.0" as the sign-in method.



3. Click "Next".
4. Fill in "General Settings" (app name and logo are shown to end users when they authenticate).

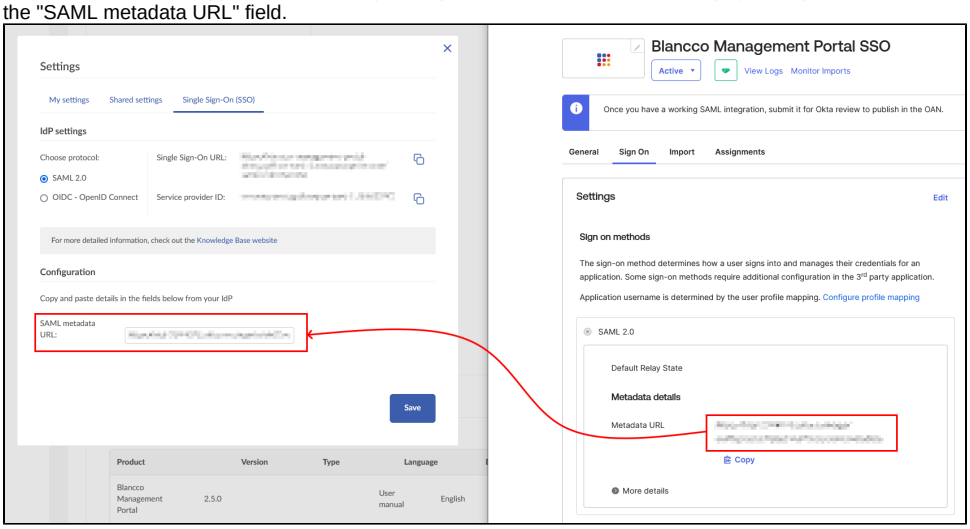


5. Click "Next".
6. Fill "SAML Settings" as stated below:
   a. General:
      i. Make sure "Use this for Recipient URL and Destination URL" is selected and fill in "Single sign-on URL" using "Single Sign-On URL" available on Blancco Management Portal SSO settings page.
      ii. Enter "Audience URI (SP Entity ID)" using "Entity ID" available on Blancco Management Portal SSO settings page.
   b. Attribute Statements:
      i. Add a new attribute statements using below details.

Name	Name	Value

	format	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims /emailaddress	Unspecified	user.email
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Unspecified	user.firstName + " " + user. lastName

7. Click "Next".
8. Fill in the "Feedback" section and click "Finish".
9. "Sign On" -tab for the application should open, copy the Metadata URL from the page and paste it to Blancco Management Portal SSO settings to the "SAML metadata URL" field.



10. Click "Save".

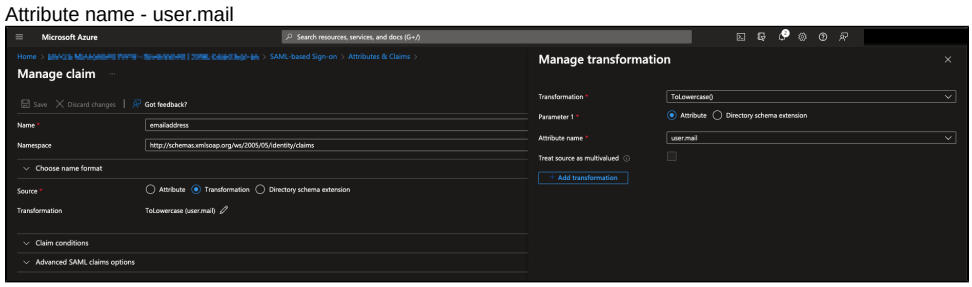
Once the configuration is finished, remember to assign the application to appropriate users and groups in order to allow users to authenticate to BMP using Okta.

Lowercase transformation for user email address

Blancco Management Portal requires user email address to be provided in lower case characters. Upper case characters within the users email address will prevent the system from working correctly. To mitigate this additional transformation rule needs to be created to treat the email address in lower case characters.

Below steps explain how to set up the needed transformation rule for the email address claim in Entra ID:

1. Open the Enterprise Application dedicated for the BMP SSO and navigate to "Single sign-on" and then to "Attributes & Claims" and edit the claims.
2. Open and edit the "emailaddress" claim (value set to user.mail) available under the "Additional Claims" section and change claims "Source" to "Transformation".
3. In the "Manage transformation" dialog configure settings as follows:
   a. Transformation - ToLowercase()
   b. Parameter 1 - Attribute
   c. Attribute name - user.mail



4. Save the changes.

5. Attributes & Claims show now look similar to below (the transformation rule applied to the email address claim)