Microsoft Entra ID (SSO and User Provisioning)

11/15/2024 12:32 pm MST

Single Sign On (SSO) is available for DocBoss. If enabled, users with the company domain will be redirected to their identity provider to sign in to access DocBoss. The instructions below outline how to set up SSO with DocBoss when using **Microsoft Entra ID** as the identity provider.

Set up

Requirements

The first step is to contact DocBoss Support and request that Single Sign On is enabled.

We will ask for some information. Your IT will need to gather this:
- Domain (users with email from this domain will be redirected to identity provider)
- Type of the application they use (ie. Microsoft Azure)
- Supported account types, if applicable *(see below, Azure example step 2)*
- Application (client) ID *(example step 3)*
- Client Secret *(example step 4)*
- Endpoints (Authorization, Token, Issuer) *(example step 6)*

After this information is provided, DocBoss Support will provide a **redirect URI** for your application. This will redirect users back to DocBoss after authentication in your identity provider. This must be added in your identity provider application by your IT.

Steps

The example below uses Microsoft Entra ID as the identity provider. If you are using a different provider, refer to their documentation for how to set up Single Sign On.

1. Log into Microsoft Azure and select **App registrations** > **Register an application**.

2. Enter the **display name** and **account type**. Make note of the account type to advise DocBoss Support.
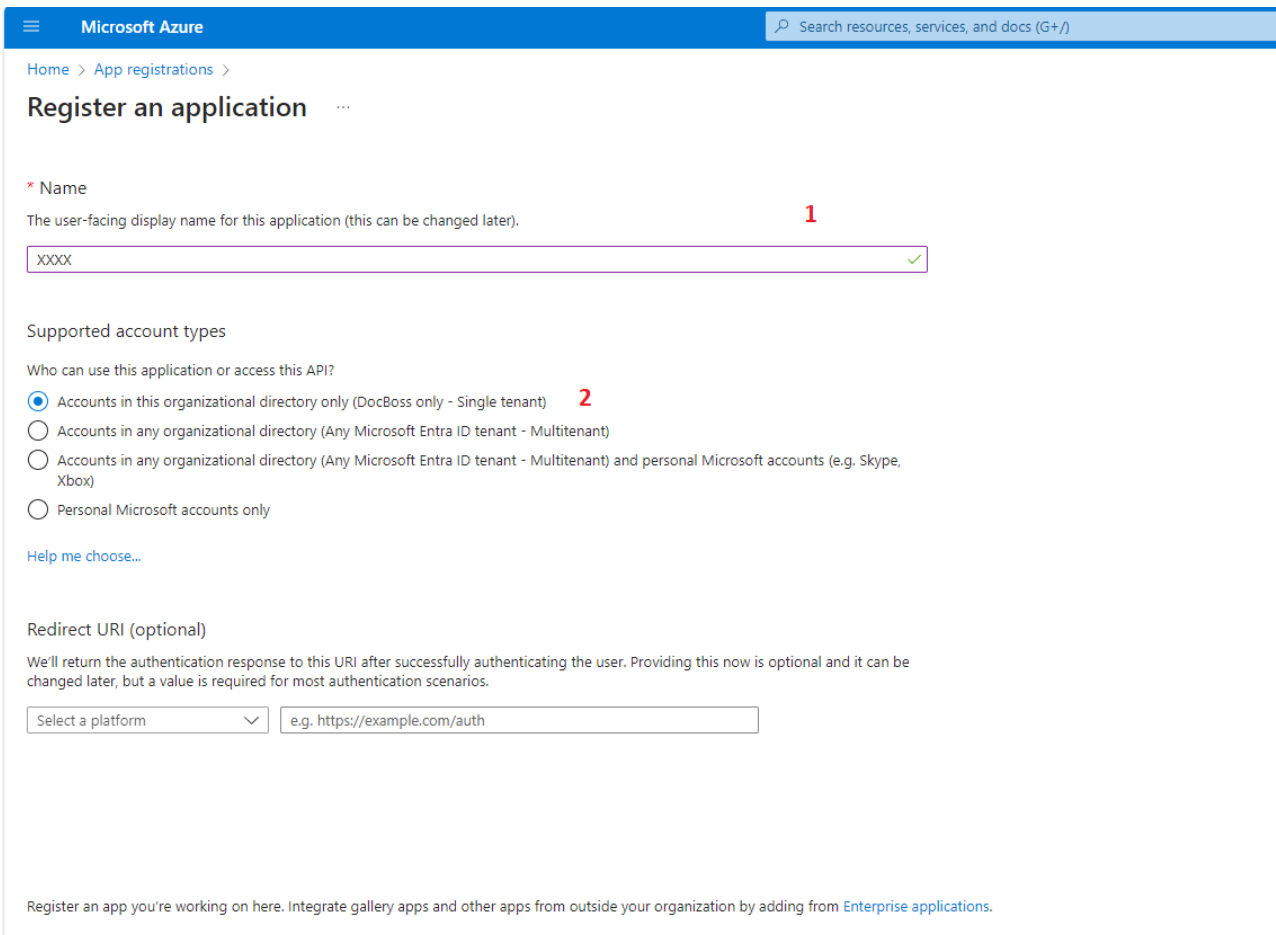
3. On the next screen, under the **Essentials** tab, copy the **Application (client) ID**. Make note of this to provide DocBoss Support.

4. On the **Client credentials** option, select **Add a certificate or secret**. Add a certificate and copy the secret to provide DocBoss Support.
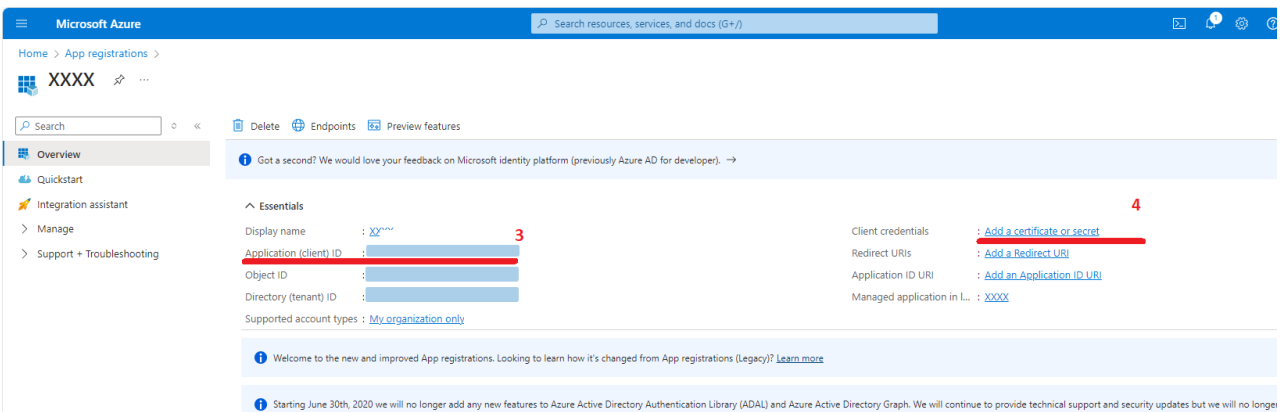

5. Select the **Endpoints** tab.

6. Copy the link for the **OpenID Connect metadata document** to provide DocBoss Support. This includes all of the endpoints (Authorization, Token, Issuer) DocBoss requires information on.
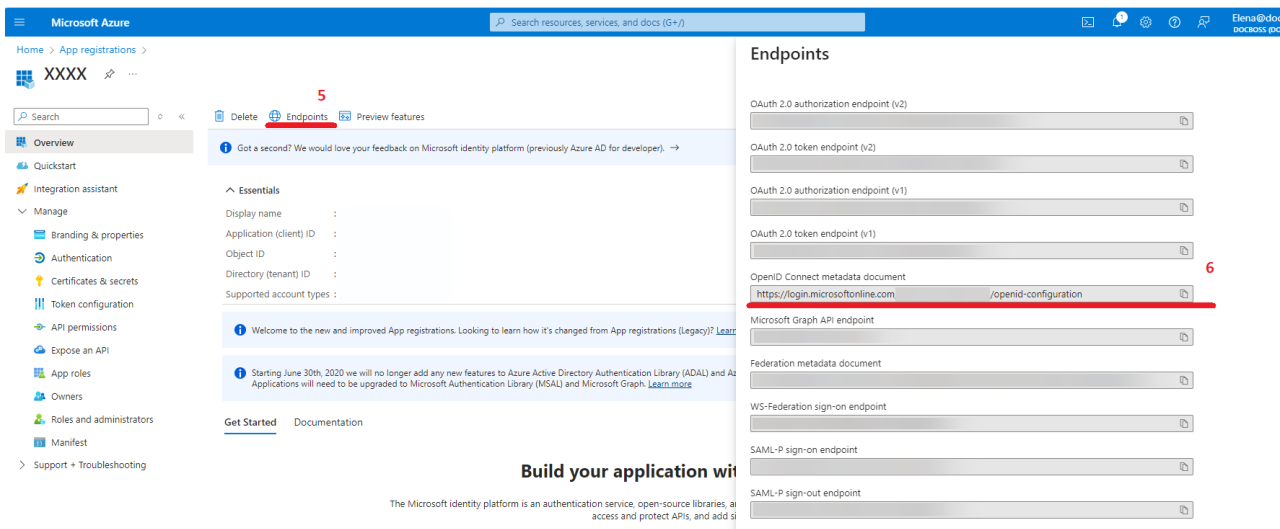
The next step is only available after providing the information from the previous steps to DocBoss Support:

7. After DocBoss Support provides **redirect URI**, navigate to the **Essentials** section of this app in Azure and select **Add a redirect URI**. Paste the redirect URI provided by DocBoss.
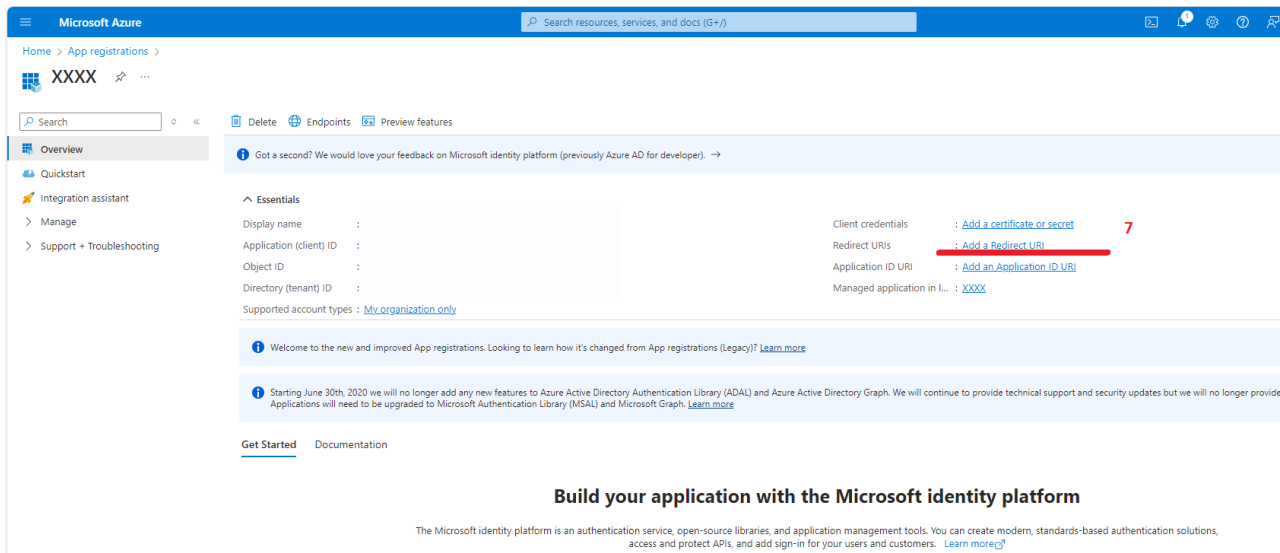
Implementing

Once the steps above are complete and you have provided the information to DocBoss as noted in them, reach out to DocBoss Support and we will schedule a meeting to enable SSO (and user provisioning, if using). Our Support will also provide a redirect URI for your application. This will redirect users back to DocBoss after authentication in your identity provider. This must be added in your identity provider application for SSO to function.

If you want to try the function, then schedule a roll out for your users we can schedule the meeting to enable, test (have a user login), then disable within a few minutes. Already logged in users would not be affected. You can then communicate to your user base with a timeline for the switch. Alternatively, we can just leave it enabled after the test is successful.