

This guide is for the Microsoft Entra ID administrator at your organization. When you finish, your people will sign in to ClickCerts with their Microsoft work account and no ClickCerts password. You need the Cloud Application Administrator role or higher.

1 Create the application

In the Microsoft Entra admin center open **Enterprise applications**, choose **New application**, then **Create your own application**. Name it **ClickCerts**, select **Integrate any other application you don't find in the gallery (Non-gallery)**, and click **Create**.

2 Set up SAML sign-on

In the application, open **Single sign-on** and choose **SAML**. In section 1, **Basic SAML Configuration**, click **Edit** and enter the two values below exactly. Leave **Sign on URL**, **Relay State** and **Logout URL** blank. **Save**.

```
Identifier (Entity ID)
https://vyiawiutnzdrwjcazxc.supabase.co/auth/v1/sso/saml/metadata
Reply URL (Assertion Consumer Service URL)
https://vyiawiutnzdrwjcazxc.supabase.co/auth/v1/sso/saml/acs
```

3 Add the display-name claim

In section 2, **Attributes & Claims**, click **Edit**, then **Add new claim**. Name: **displayname**. Namespace: blank. Source attribute: **user.displayname**. **Save**. Leave the default claims as they are; ClickCerts reads the user's email from **emailaddress**, so each user must have a mail address in Entra.

4 Assign your users

Open **Users and groups** and add the people (or group, where your plan allows) who will use ClickCerts. Anyone not assigned here will be refused by Microsoft at sign-in.

5 Send us the metadata URL

Back in **Single sign-on**, section 3, **SAML Certificates**, copy the **App Federation Metadata Url**. Send that URL and the email domain(s) your people sign in with to your ClickCerts contact. GCC High tenants will see a URL beginning with **login.microsoftonline.us**; that is expected.

What happens next

ClickCerts registers your connection, usually the same business day, and confirms by email. From then on, anyone at your domain who opens the ClickCerts sign-in page and enters their work email is sent to Microsoft to authenticate and returned to their training dashboard. Existing users keep their history. New users are invited by your ClickCerts administrator as before, and activate by signing in with Microsoft.

If sign-in fails: check the two values in step 2 for a stray character, confirm the user is assigned in step 4, and confirm the user's email domain was sent to ClickCerts in step 5. Microsoft's own error text (AADSTS...) will name which of these it is.