

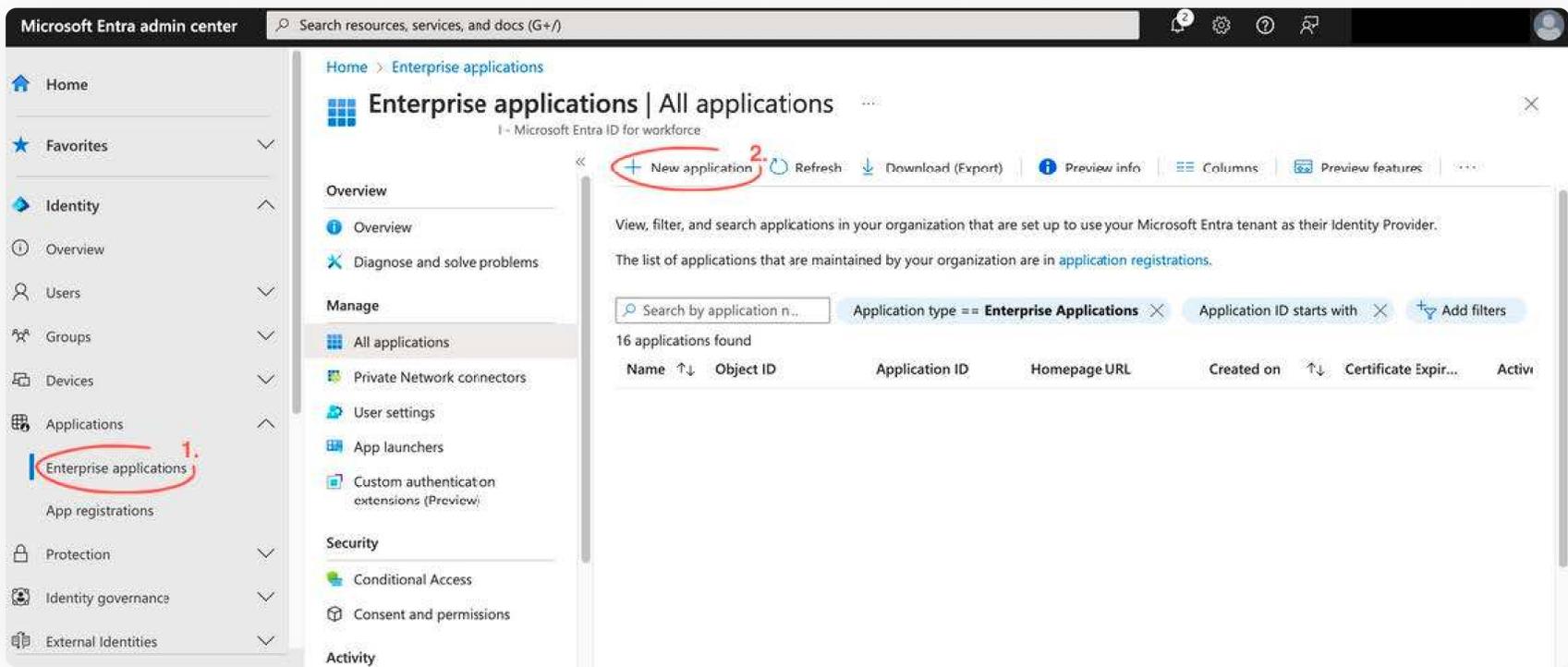


Step by step

# SSO / Entra (Azure) Integration

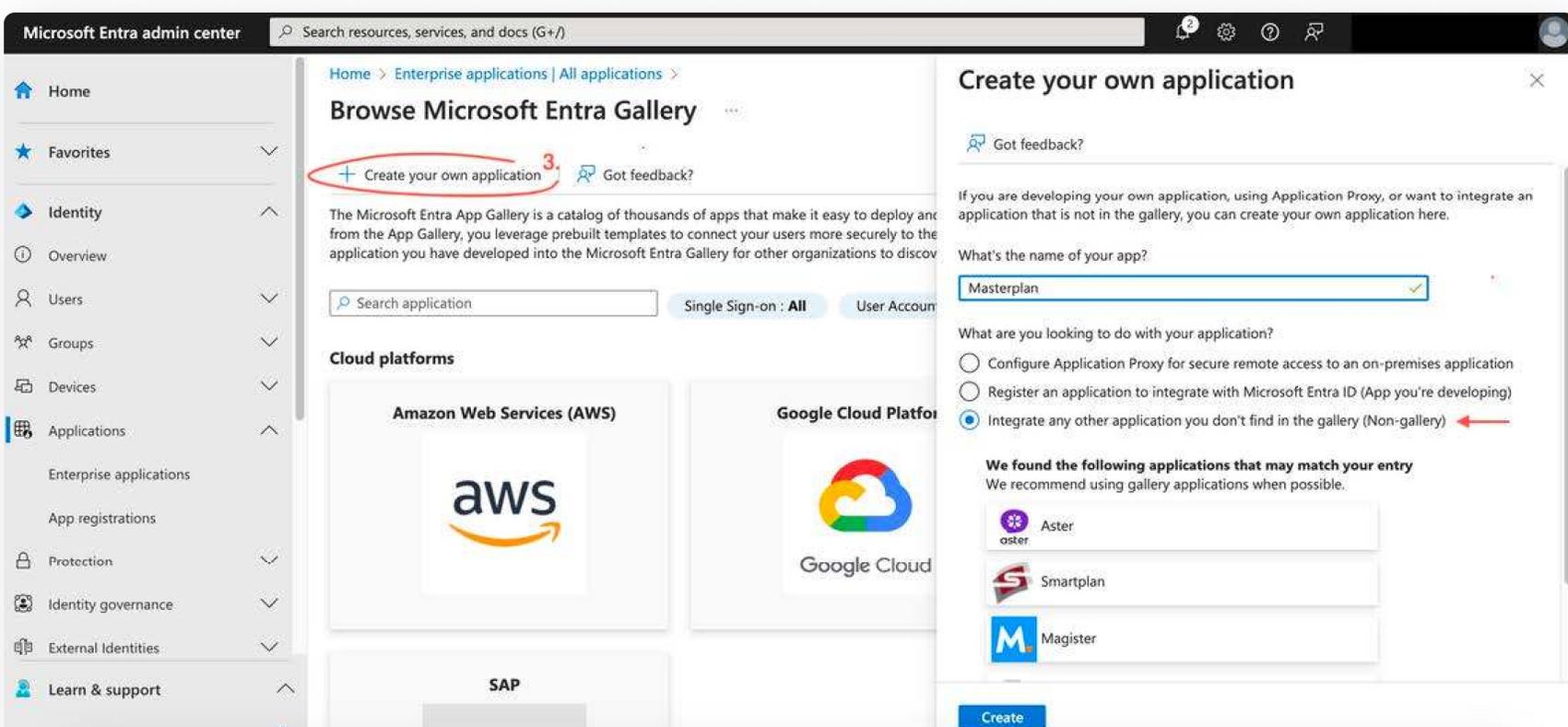
## 1 HINZUFÜGEN EINER NEUEN APPLICATION

Fügen Sie eine neue Application hinzu. Dazu wählen Sie links unter dem Punkt Applications den Unterpunkt Enterprise applications (1.) und klicken dann auf New application (2.):



## 2 ERSTELLEN EINER EIGENEN APPLICATION

Erstellen Sie ihre eigene Application, dazu wählen Sie selbigen Punkt in der Übersicht (3.), da wir kein Teil des Katalogs sind. Dann vergeben Sie für unsere Application einen Namen (im Optimalfall Masterplan) und wählen den dritten Punkt aus (siehe Pfeil). Im Anschluss klicken Sie auf "Create":



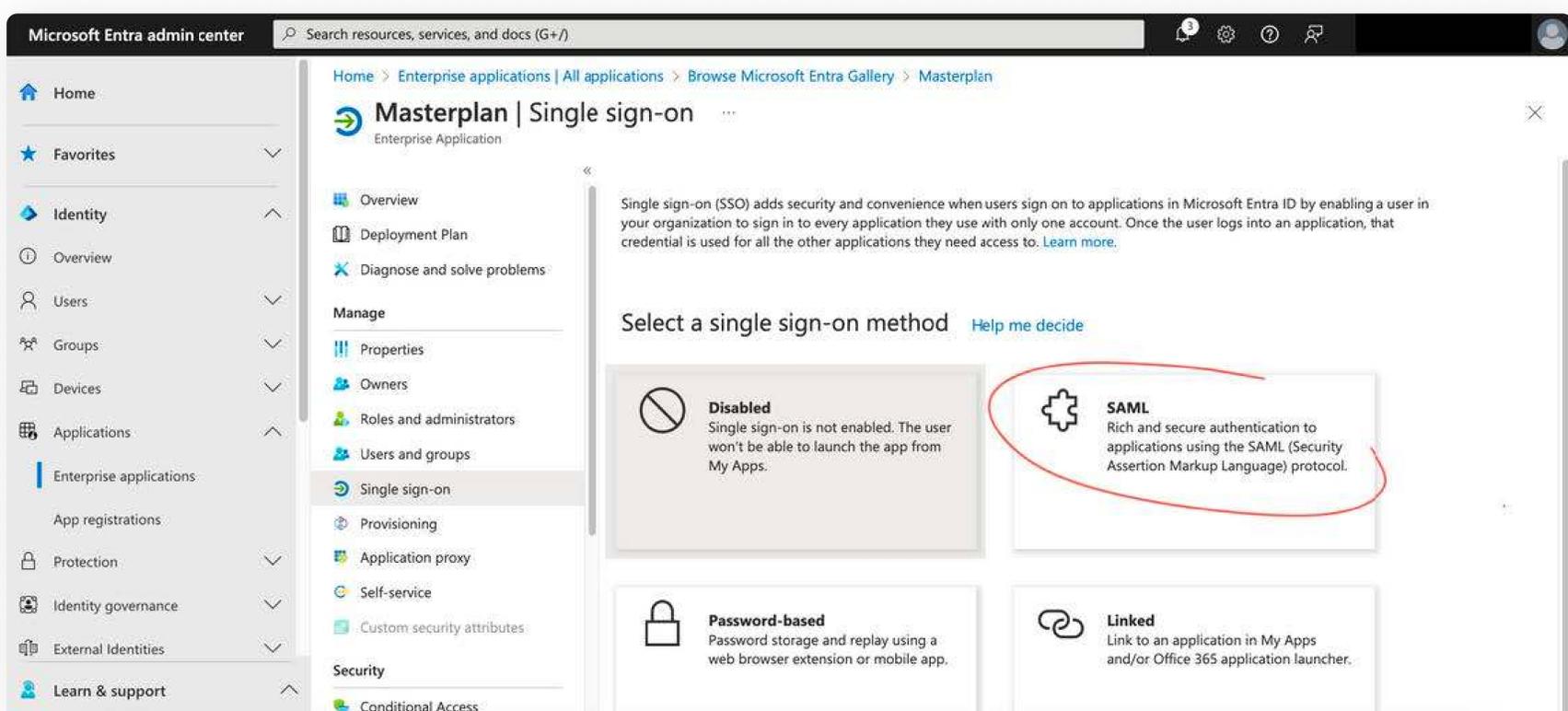
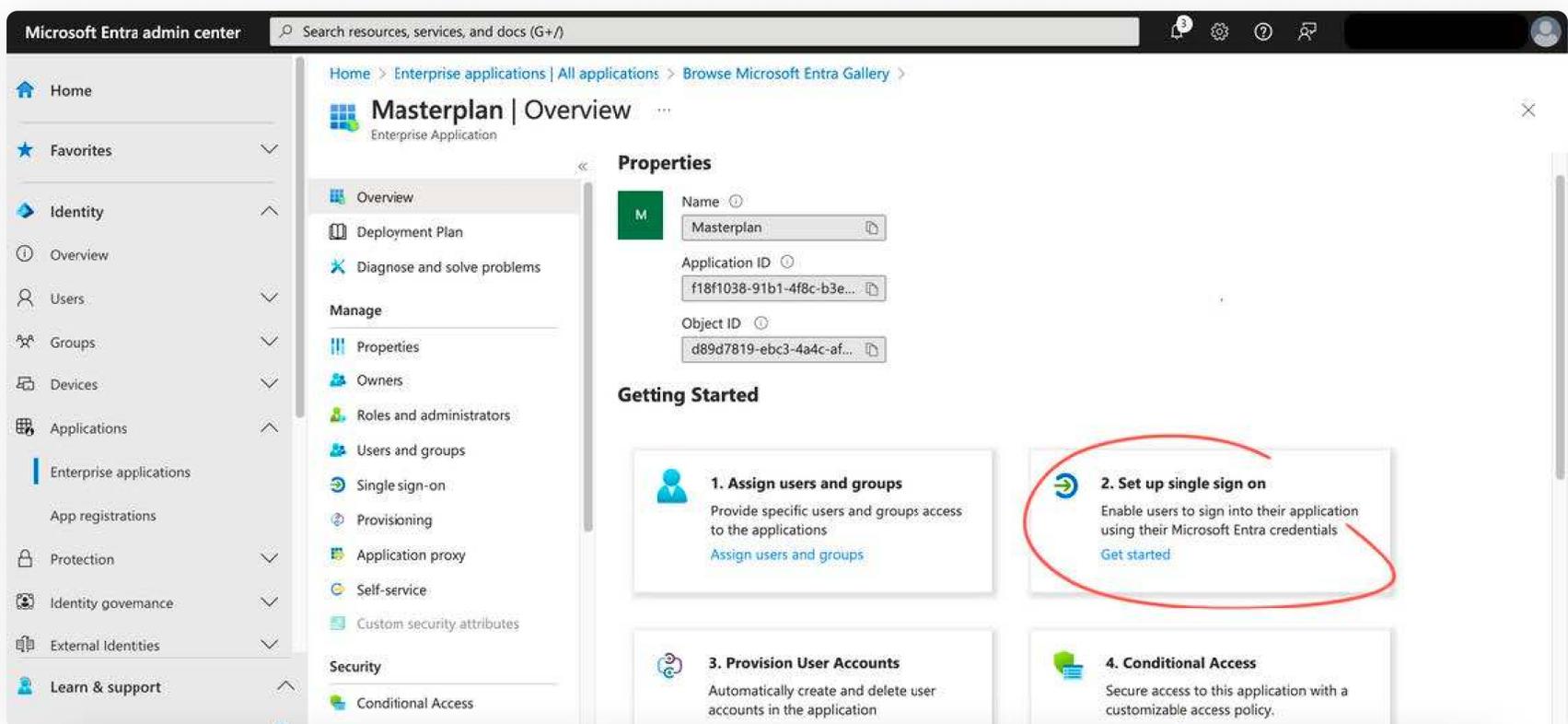


Step by step

# SSO / Entra (Azure) Integration

## 3 AUSWÄHLEN DER MASTERPLAN APPLICATION & SET UP SINGLE-SIGN-ON MIT SAML

Nun werden Sie Masterplan als Application in der Übersicht finden können und wählen diese aus. Im Nächsten Schritt können Sie unter "1.Assign users and groups" die dementsprechende Berechtigungsgruppe erstellen in welcher die passenden Personen eingepflegt sein müssen um SSO für Masterplan nutzen zu können. Danach wählen Sie den Punkt "Set up single sign on" aus und anschließend "SAML":



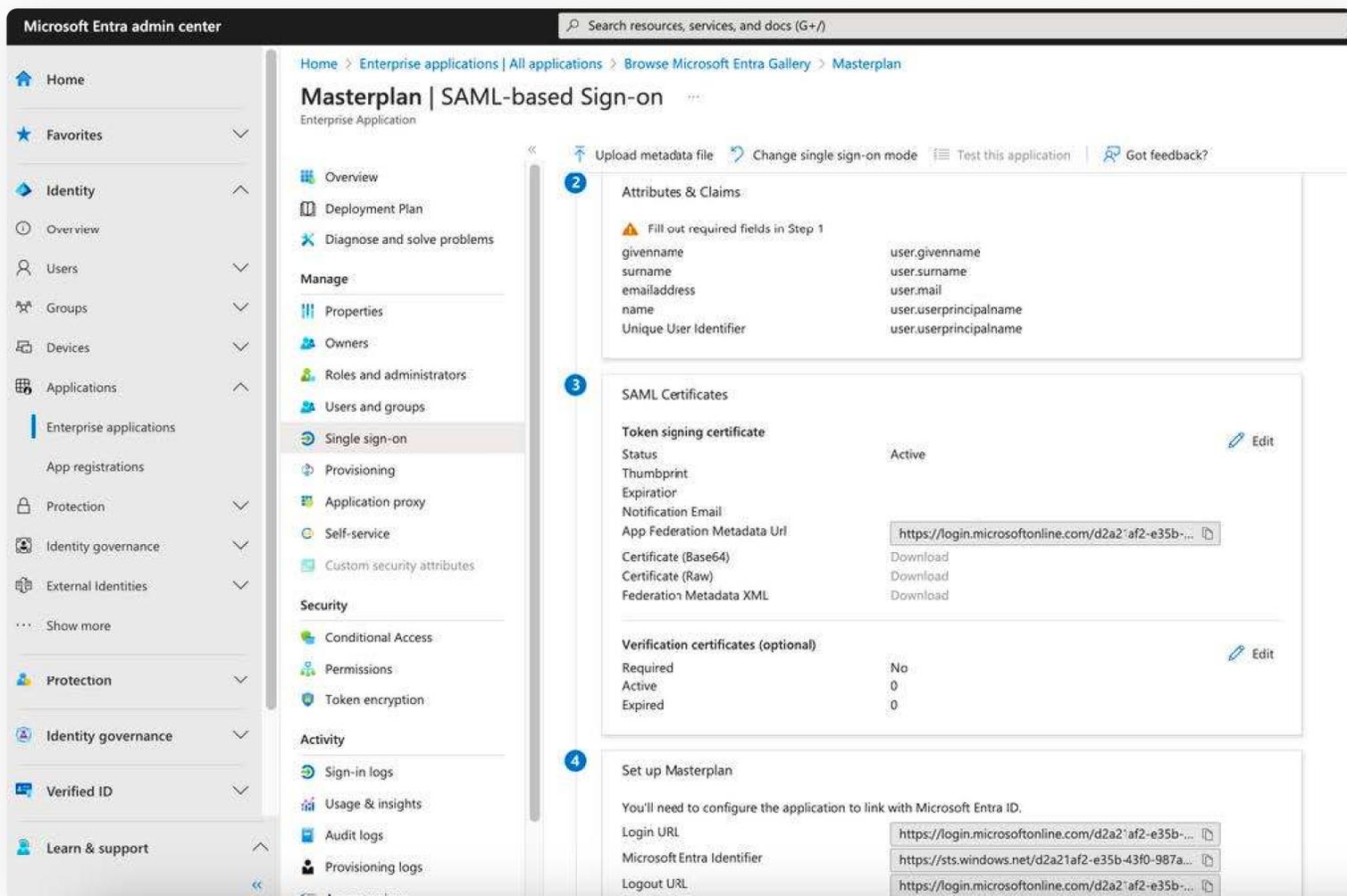


Step by step

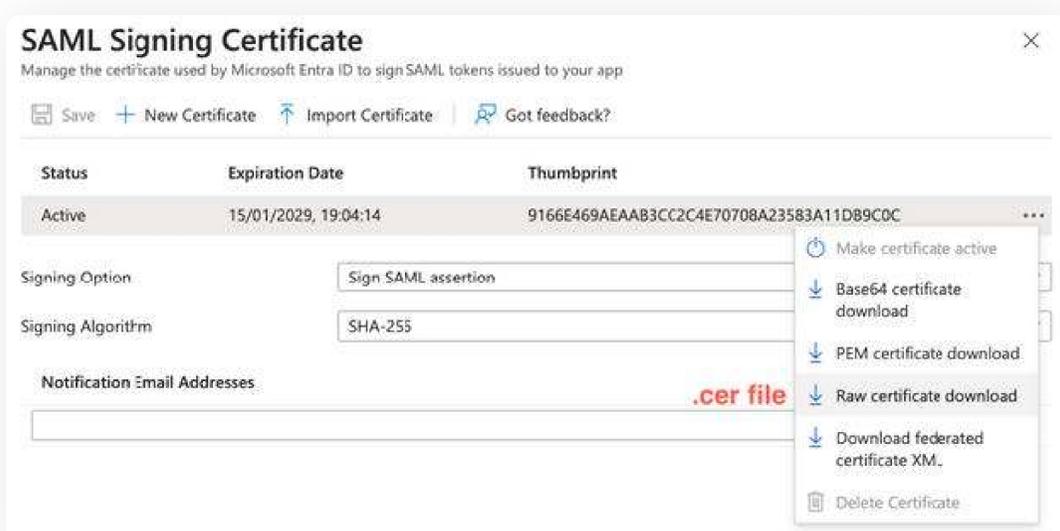
# SSO / Entra (Azure) Integration

## 4 ERSTELLUNG & BEREITSTELLUNG DER NÖTIGEN DATEN FÜR MASTERPLAN

Alle für uns relevanten Informationen können Sie unter den Punkten 2-4 (siehe Screenshot) finden, wie z.B. die App Federation Metadata URL bzw. die Federation Metadata XML, das SAML Signing Certificate, auch die Login URL und Logout URL + MS Entra ID.



Zum Zertifikat gelangen Sie durch Auswahl des Buttons "Edit" unter Punkt 3. Laden Sie das Zertifikat herunter und stellen es uns ebenfalls zur Verfügung. (wie auf dem nachfolgenden Screenshot abgebildet)





Step by step

# SSO / Entra (Azure) Integration

## 5 FERTIGSTELLUNG DER KONFIGURATION IN ENTRA (AZURE)

Nachdem wir alle für uns nötigen Informationen für die Konfiguration erhalten haben, werden wir Sie nachträglich mit den auszufüllenden Daten auf Ihrer Seite versorgen, sodass Sie in der Lage sein werden alle Felder unter Punkt 1 des SSO Set Ups auszufüllen.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation options like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, App registrations, Protection, Identity governance, External Identities, and Learn & support. The main content area displays the 'Basic SAML Configuration' for an application named 'Masterplan | SAML-based'. The configuration fields are as follows:

- Identifier (Entity ID):** A text input field containing 'Masterplan Entity ID'. A note below states: 'The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.'
- Reply URL (Assertion Consumer Service URL):** A text input field containing 'ACS URL'. A note below states: 'The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.'
- Sign on URL (Optional):** A text input field containing 'e.g. masterplan.com/sso/company'. A note below states: 'Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.'

## 6 FINALES TESTING UND ABSCHLUSS DER INTEGRATION

Die Konfiguration sollte nun auf beiden Seiten abgeschlossen sein. Zum Schluss findet ein finaler Test statt und der Vorgang wird geschlossen. Das SSO kann nun für Masterplan genutzt werden.

