Enabling Single Sign-on (SSO)

Single sign-on (SSO) to the Ascent360 platform is available by request only. Please submit your request either through your CSM or the help desk.

The following information must be provided:

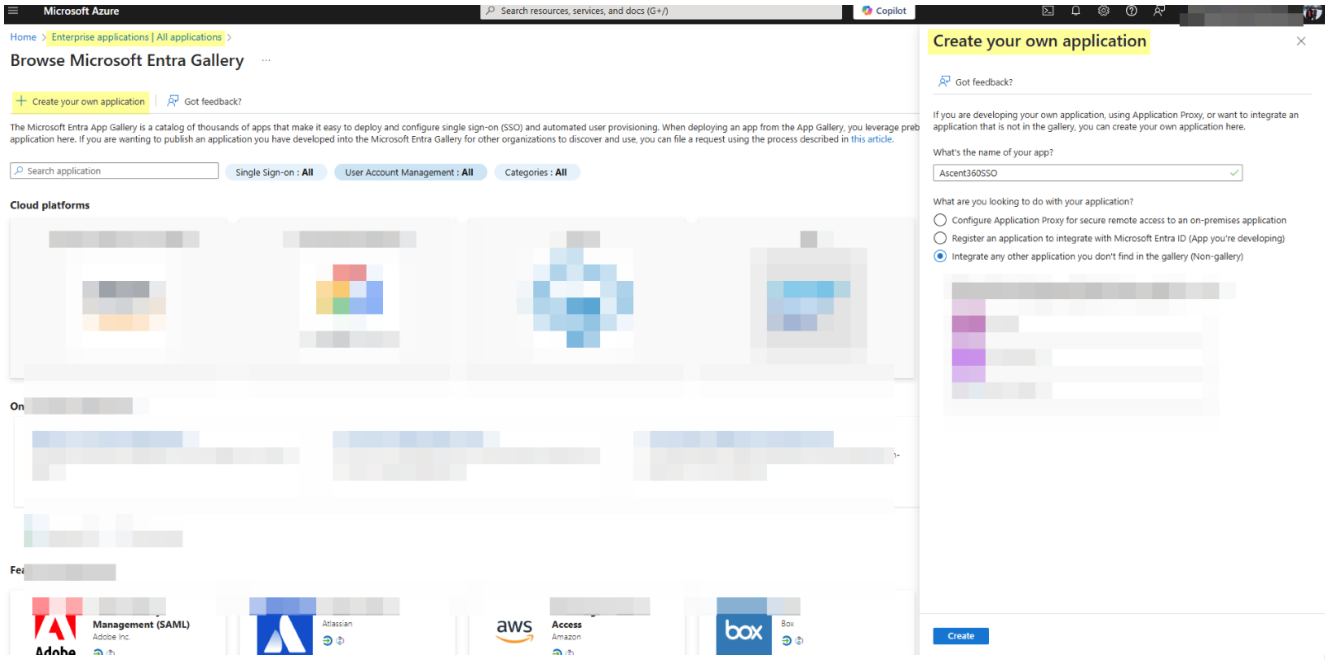
1. **Identity Provider (IdP) Details:** URL of your Identity Provider or Microsoft Entra Identifier.
2. **Login URL:** The login URL for the IdP.
3. **Logout URL:** The logout URL for the IdP (optional and may be the same as the login URL).
4. **One of the following:**
    1. **Metadata URL:** In Entra, this is also called the App Federation Metadata URL.
    2. **Certificate:** The public certificate used by the IdP for signing SSO assertions.

> Note: We need the Metadata URL **or** Certificate, not both.

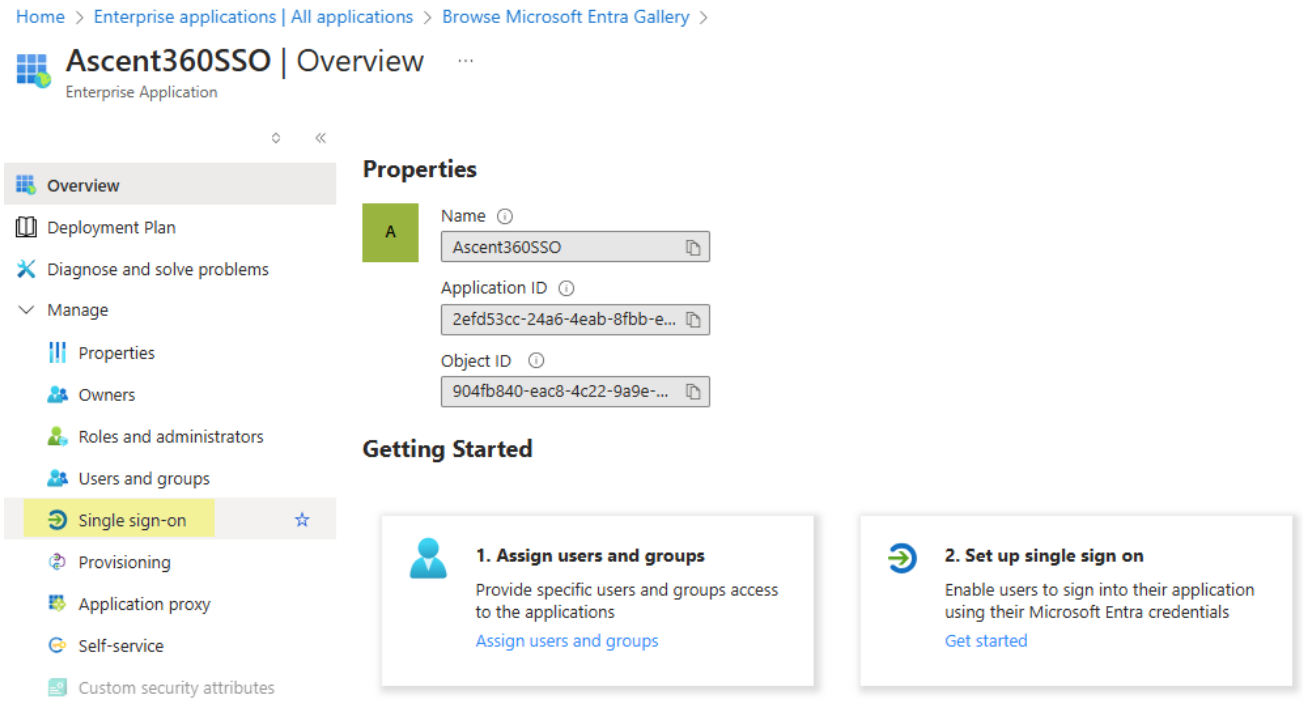
By default, we use email addresses as the usernames for our system, so no changes will need to be made here. Note that SSO is enabled per **domain**, so if you use multiple domains at your company, please give us the one you'd like associated with the SSO functionality.

The person submitting the "Enable SSO" request (from the client side) will be the "tester" of the functionality once it's enabled. If you'd like someone else to do the testing on your side, please let us know who that will be.

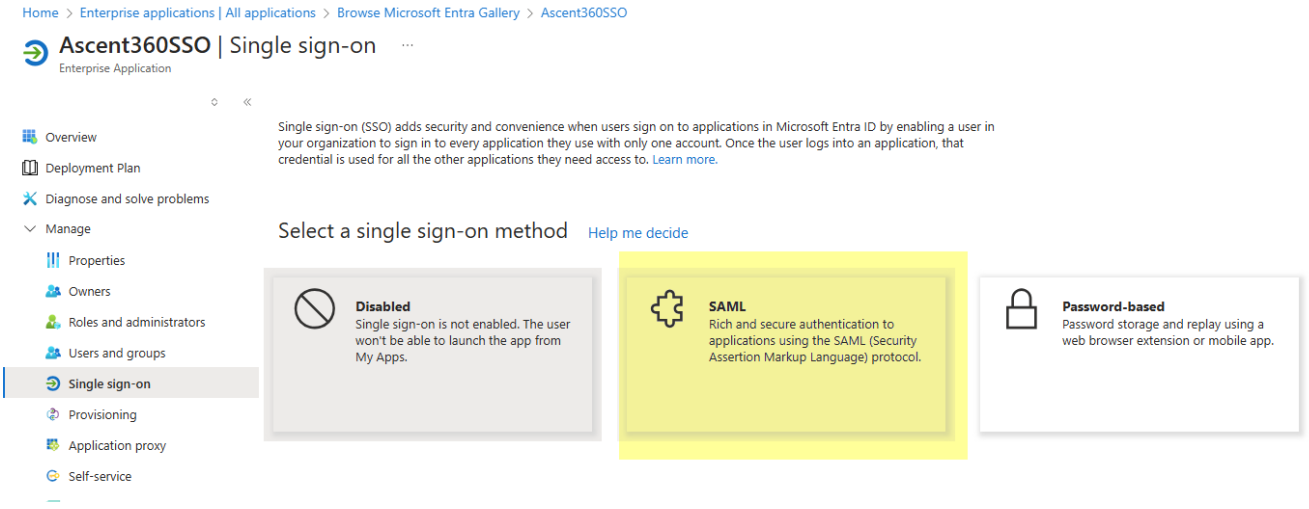
Here are instructions for those who use **Microsoft Azure**:



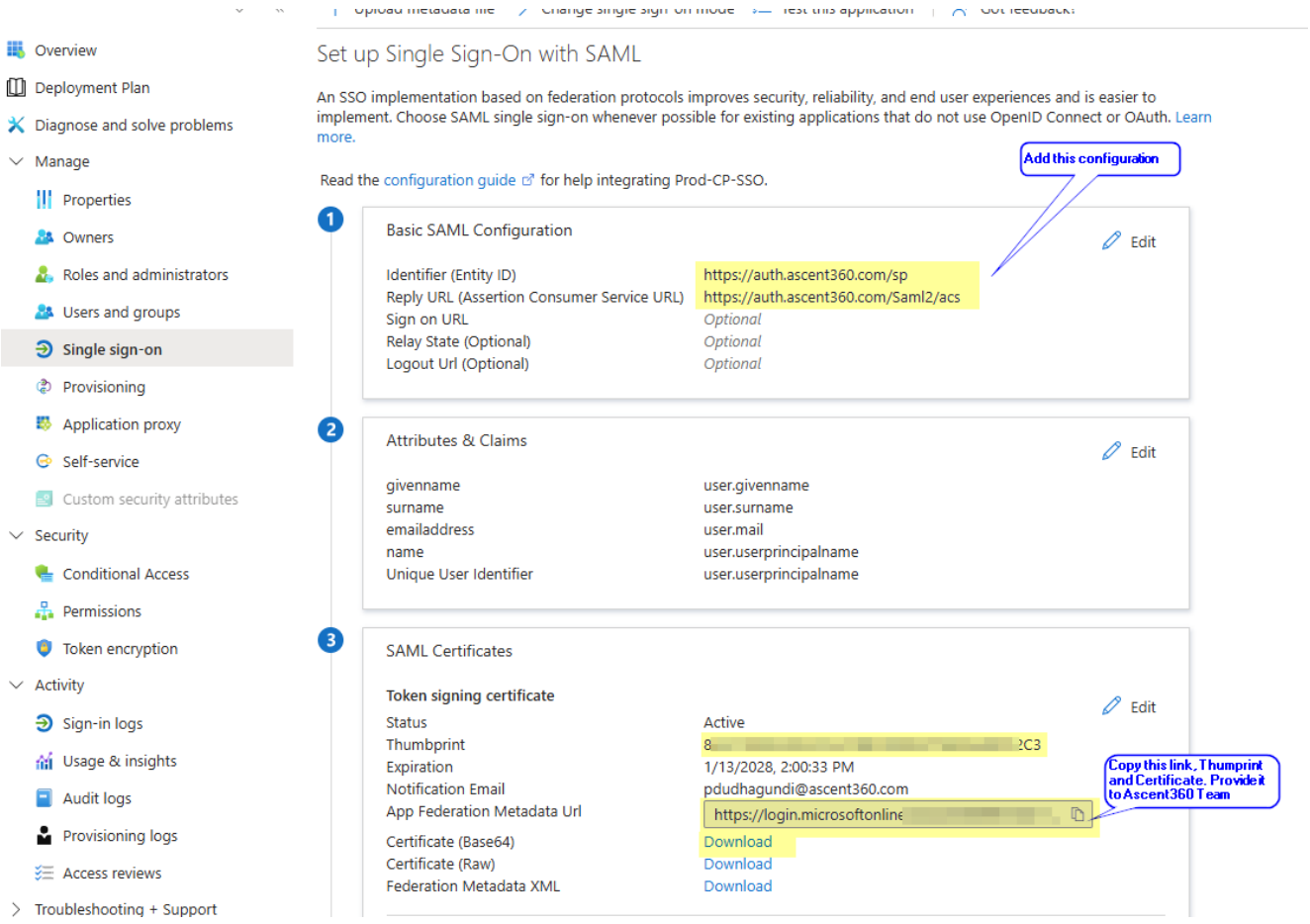
Once you click "Create", please fill out the Properties like this:



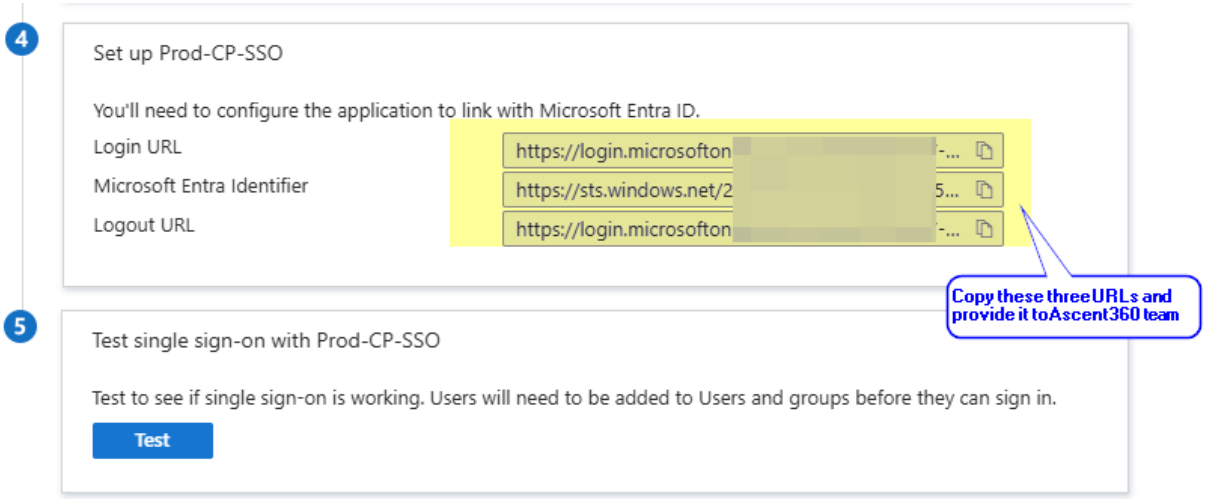
The method must be SAML:



Then, please add this configuration (highlighted in yellow below):



Copy the following three URLs and provide them back to Ascent360:



Ascent360 will then test the configuration and ask someone from the client side to also test.