

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:

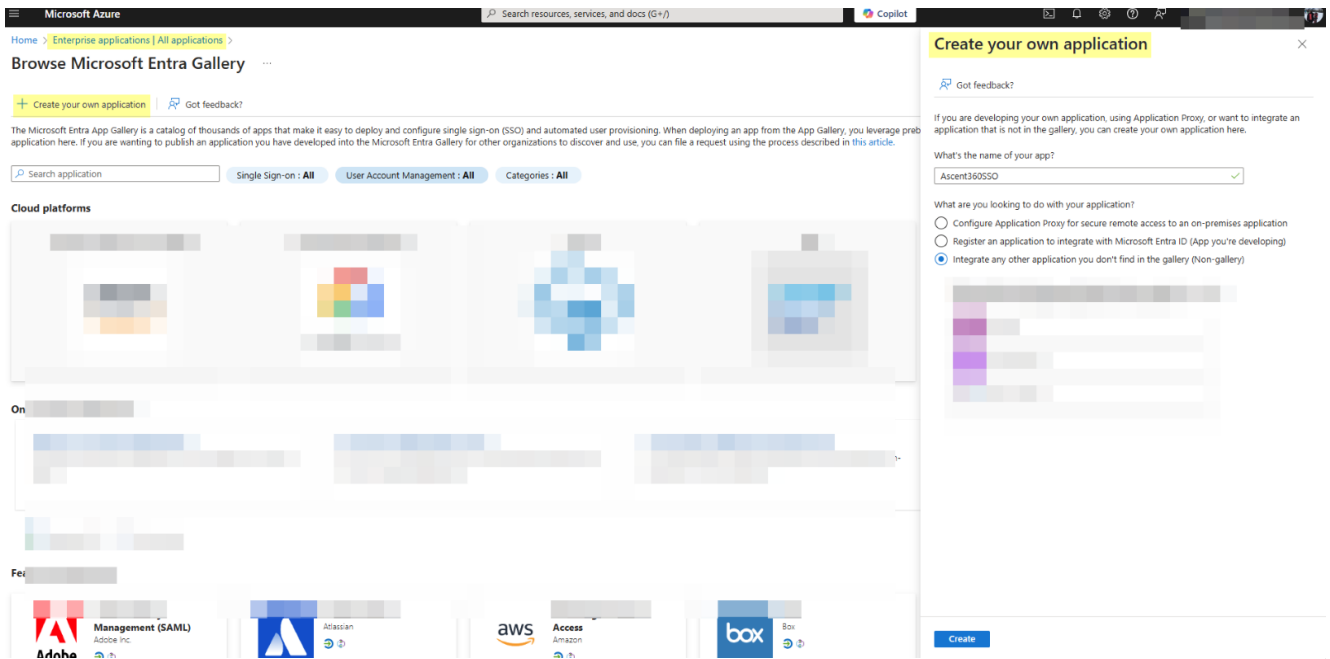
1. **Identity Provider (IdP) Details:** URL of your Identity Provider or Microsoft Entra Identifier.
2. **Login URL:** The login URL for the IdP.
3. **Logout URL:** The logout URL for the IdP (optional and may be the same as the login URL).
4. **One of the following:**
  1. **Metadata URL:** In Entra, 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:

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

## Ascent360SSO | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on** ☆
  - Provisioning
  - Application proxy
  - Self-service
  - Custom security attributes

### Properties

**A** Name ⓘ  
Ascent360SSO

Application ID ⓘ  
2efd53cc-24a6-4eab-8fbb-e...

Object ID ⓘ  
904fb840-eac8-4c22-9a9e-...

### Getting Started

**1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)

**2. Set up single sign on**  
Enable users to sign into their application using their Microsoft Entra credentials  
[Get started](#)

The method must be SAML:

# Ascent360SSO | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on**
  - Provisioning
  - Application proxy
  - Self-service

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

## Select a single sign-on method [Help me decide](#)

**Disabled**  
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

**SAML**  
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

**Password-based**  
Password storage and replay using a web browser extension or mobile app.

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

### Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Prod-CP-SSO.

[Add this configuration](#)

- Basic SAML Configuration**

Identifier (Entity ID)	<code>https://auth.ascent360.com/sp</code>
Reply URL (Assertion Consumer Service URL)	<code>https://auth.ascent360.com/Saml2/acs</code>
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims**

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**

<b>Token signing certificate</b>	Active
Status	Active
Thumbprint	8-...-2C3
Expiration	1/13/2028, 2:00:33 PM
Notification Email	pdudhagundi@ascent360.com
App Federation Metadata Url	<code>https://login.microsoftonline</code>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

[Copy this link, Thumbprint and Certificate. Provide it to Ascent360 Team](#)

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

4

#### Set up Prod-CP-SSO

You'll need to configure the application to link with Microsoft Entra ID.

Login URL

<https://login.microsoft.com>

Microsoft Entra Identifier

<https://sts.windows.net/2>

Logout URL

<https://login.microsoft.com>

Copy these three URLs and provide it to Ascent360 team

5

#### Test single sign-on with Prod-CP-SSO

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

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