

Users are people who can log in to your marketing platform to create audiences, design and schedule emails, and view reporting and customer data. Learn how to manage users in Ascent360.

User account creation can be requested via our Help Desk (by emailing support@ascent360.com or creating a ticket from within the platform).

Provide the following information in your request:

- Your organization name
- The new user's:
 - Email Address
 - First and Last name
 - Start Date / Desired Access Date
- Any pages that should be restricted for the user

Disabling access to the Ascent360 platform is accomplished by the Ascent360 support team. Contact our Help Desk by emailing support@ascent360.com or creating a ticket from within the platform.

Provide the following information:

- Your organization's name(s)
- The email address, first and last name of the user account to disable
- The date by which the user needs removed/disabled

Forgot your password? Follow these steps to reset it:

1. Navigate to the [Ascent360 Login Page](#)
2. On the login screen, click [Forgot Password?](#)

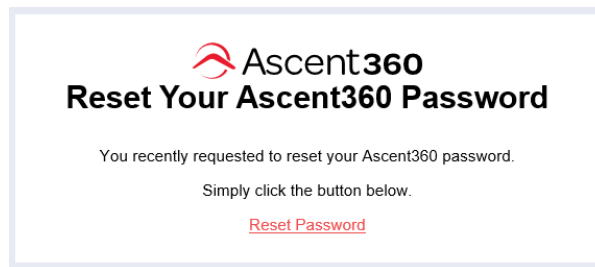
3. Enter the email address associated with your account and click **submit**.

Forgot your password?

Enter Your Email

Email

4. Check your inbox for an email from Ascent360 Support (noreply@ascent360.com)
5. Click on the **Reset Password** button in the email or copy the URL into your browser. This link will expire after **1 hour**.



6. Complete the password reset by entering your email, new password and confirming your password.

Reset password

Email

Password

Confirm password

7. You will be redirected to a confirmation page. Click on Login to return to the login page.

Reset password confirmation

Your password has been reset. Please [click here to Log In](#)

8. Login to your account using your new password.

Need additional help? Email support@ascent360.com for assistance.

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:

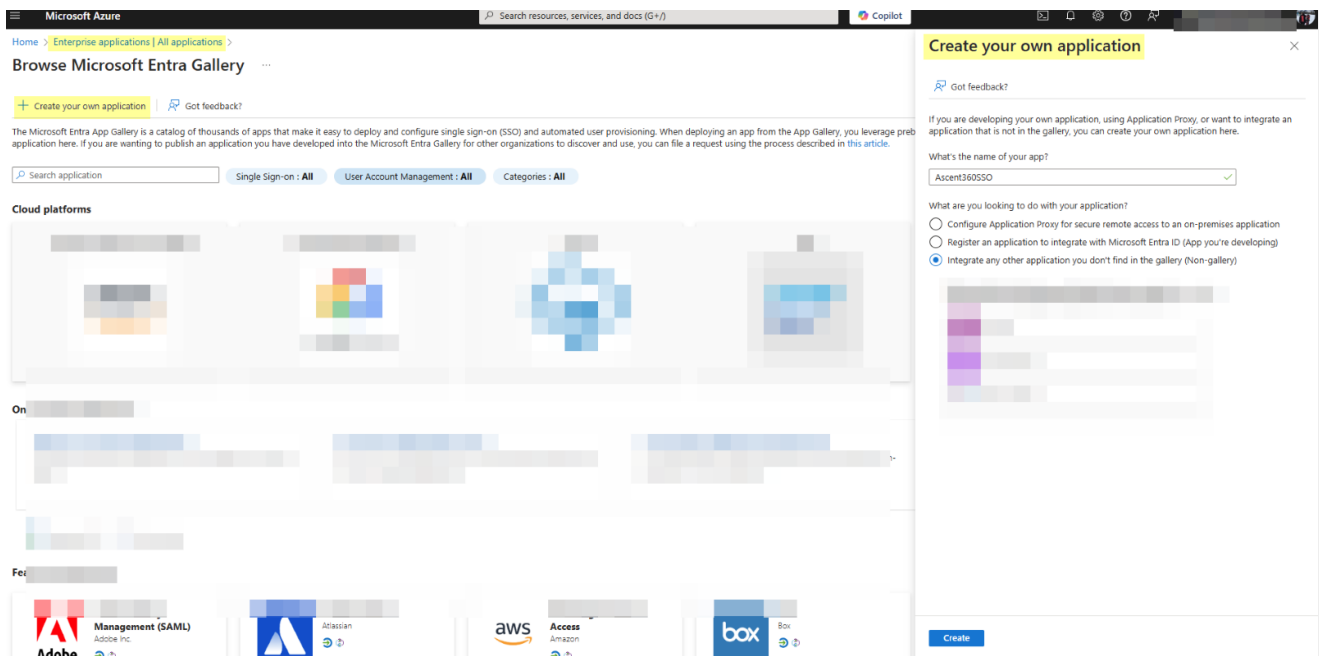
1. **Identity Provider (IdP) Details:** URL of your Identity Provider or Microsoft Entra Identifier.
2. **Login URL:** The login URL for the IdP.
3. **Logout URL:** The logout URL for the IdP (optional and may be the same as the login URL).
4. **One of the following:**
 1. **Metadata URL:** In Entra,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

- 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)	https://auth.ascent360.com/sp
Reply URL (Assertion Consumer Service URL)	https://auth.ascent360.com/Saml2/acs
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**

Token signing certificate	Active
Status	8-...2C3
Thumbprint	
Expiration	1/13/2028, 2:00:33 PM
Notification Email	pdu dhagundi@ascent360.com
App Federation Metadata Url	https://login.microsoftonline.com/.../
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

[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.microsofton

Microsoft Entra Identifier

https://sts.windows.net/2

Logout URL

https://login.microsofton

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.