Users & passwords

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.

Request access for a new user

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

Disable a user account

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:

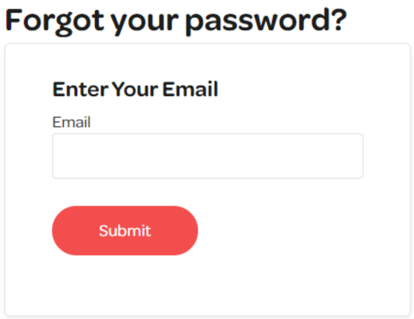
- Your organization's name(s)
- The email address, first and last name of the user account to disable
- The date by which the user needs removed/disabled

Reset Your Password

Forgot your password? Follow these steps to reset it:

1. Navigate to the Ascent360 Login Page
2. On the login screen, click Forgot Password?

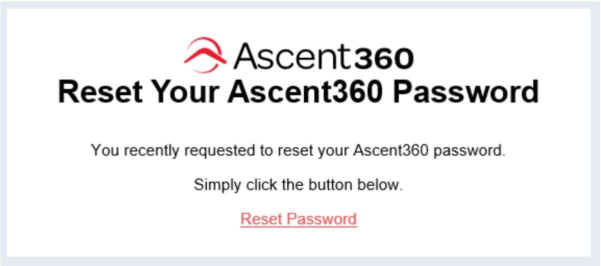
3. Enter the email address associated with your account and click submit.



Forgot your password?

Enter Your Email

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.**



Ascent360

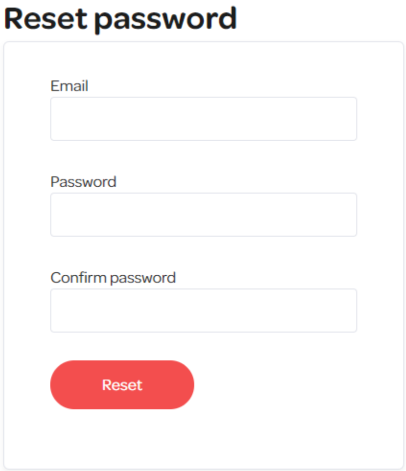
Reset Your Ascent360 Password

You recently requested to reset your Ascent360 password.

Simply click the button below.

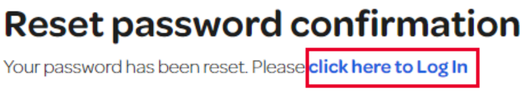
Reset Password

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



Reset 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.

In this article:

Overview

Single Sign-On (SSO) allows users to securely access multiple applications with one set of login credentials. Enabling SSO for the Ascent360 platform can streamline your users' access, simplifying the login process and reducing the need to remember yet another password. (It also improves security!)

Requesting SSO for your Organization

SSO for Ascent360 is available by request only. Please submit your request 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.

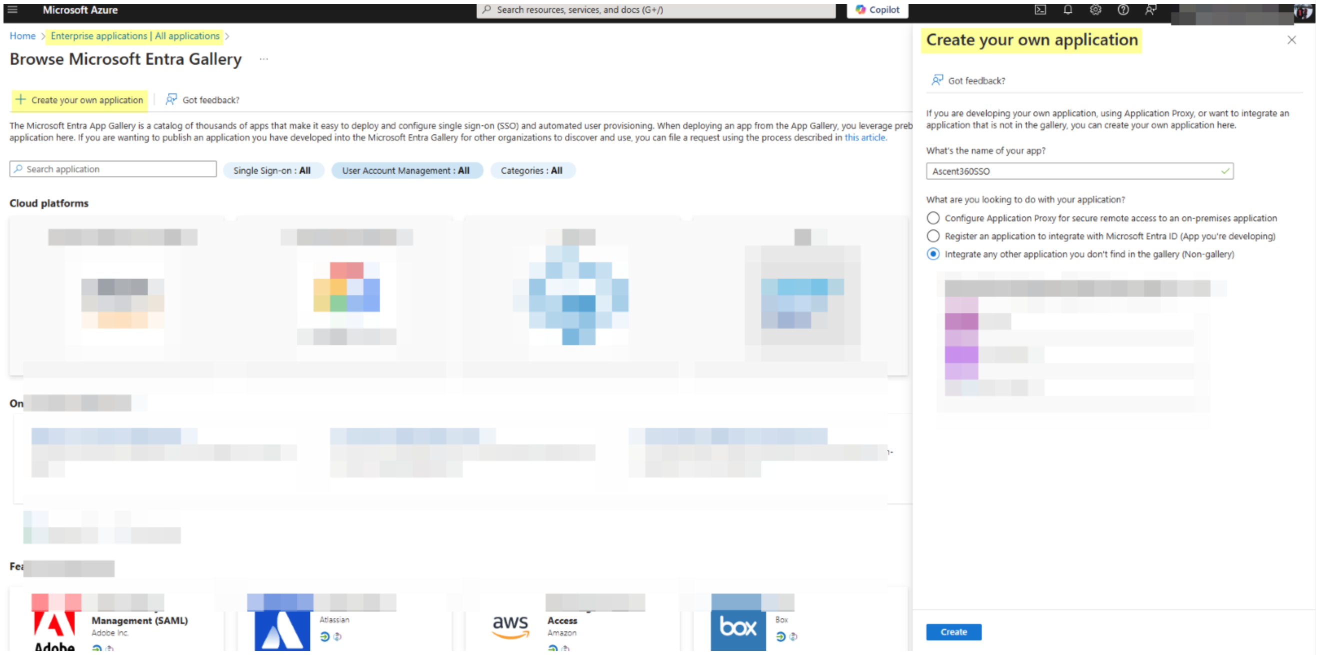
Note: We need the Metadata URL **or** Certificate, not both.

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

The client contact requesting SSO will be the "tester" of the functionality once it's enabled.

Microsoft Azure Instructions

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



Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery ...

+ Create your own application | Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage preb application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Ascent360SSO

What are you looking to do with your application?

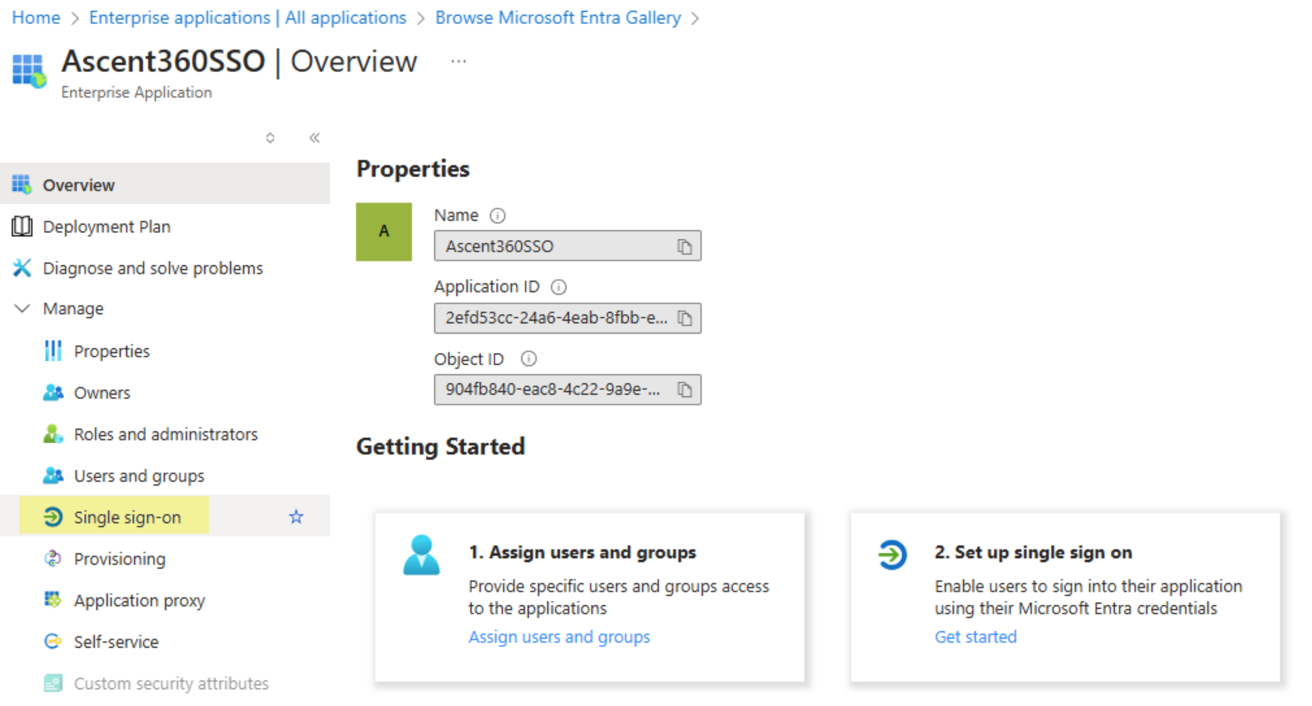
○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Microsoft Entra ID (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

Create

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



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

Ascent360SSO | Overview ...

Enterprise Application

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

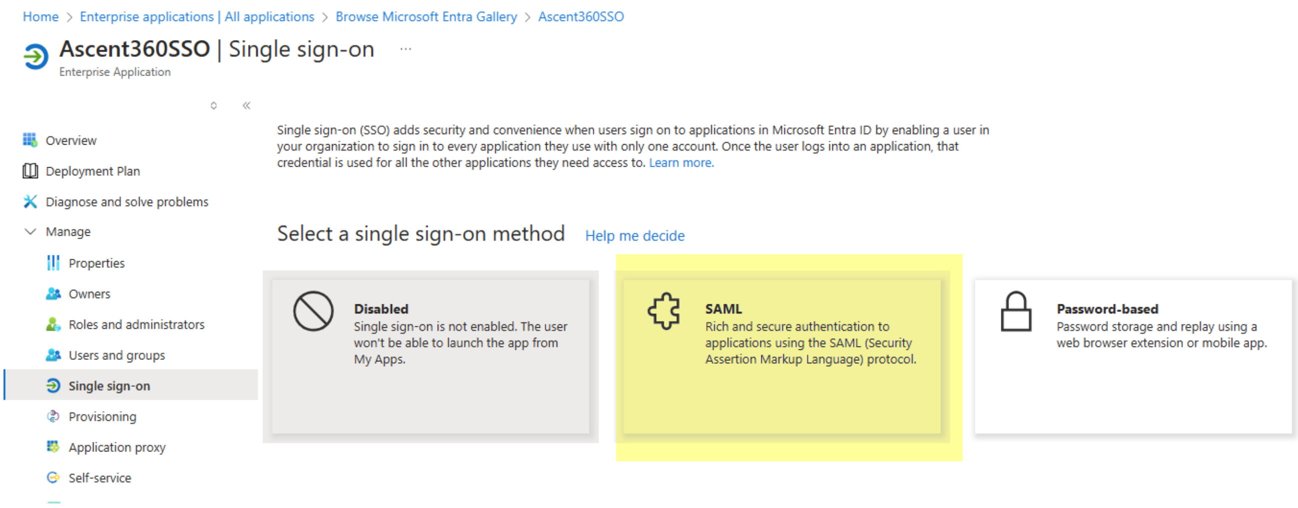
Assign users and groups

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

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.

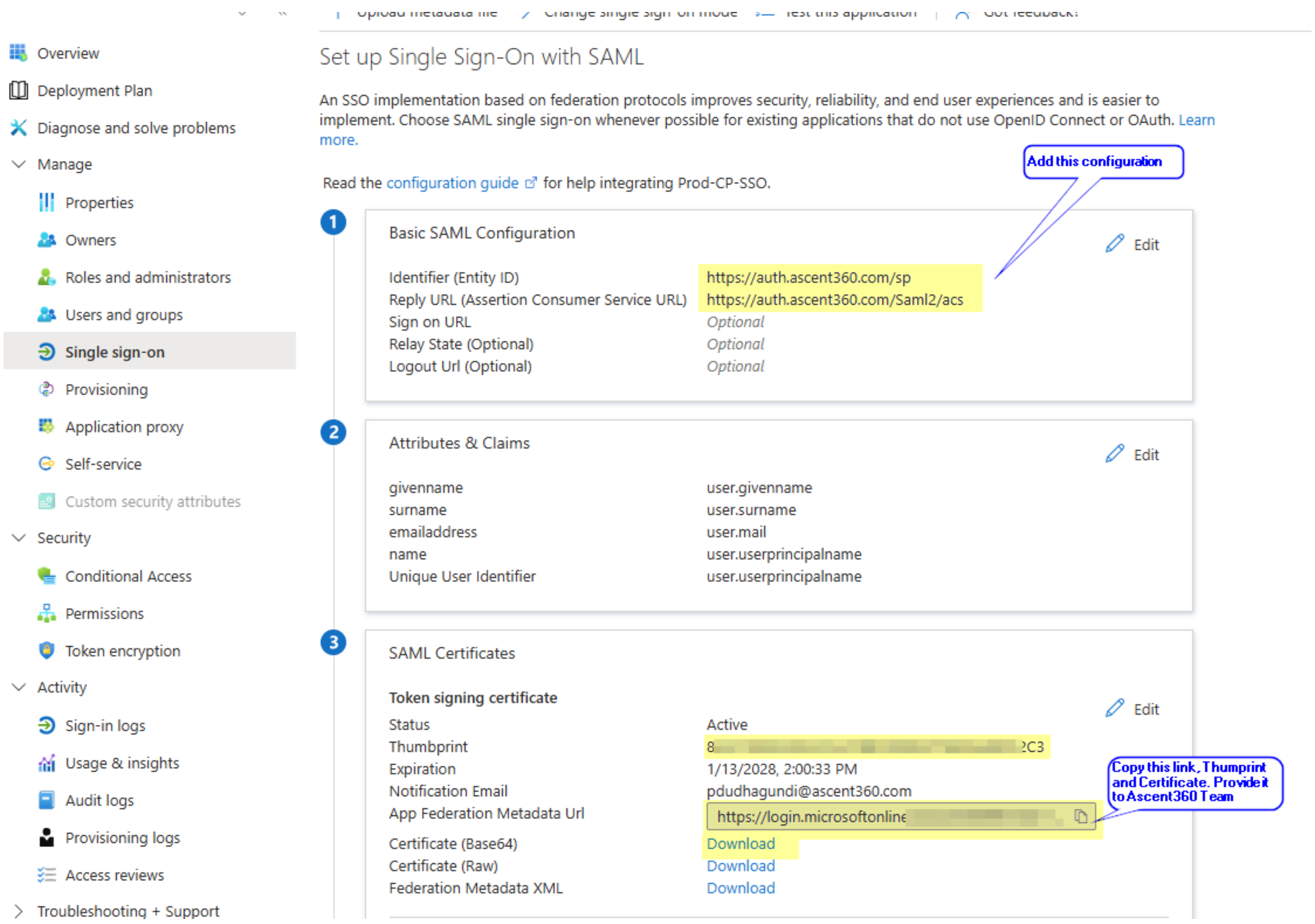
Select a single sign-on method Help me decide

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.

1 Basic SAML Configuration — Edit

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*

2 Attributes & Claims — Edit

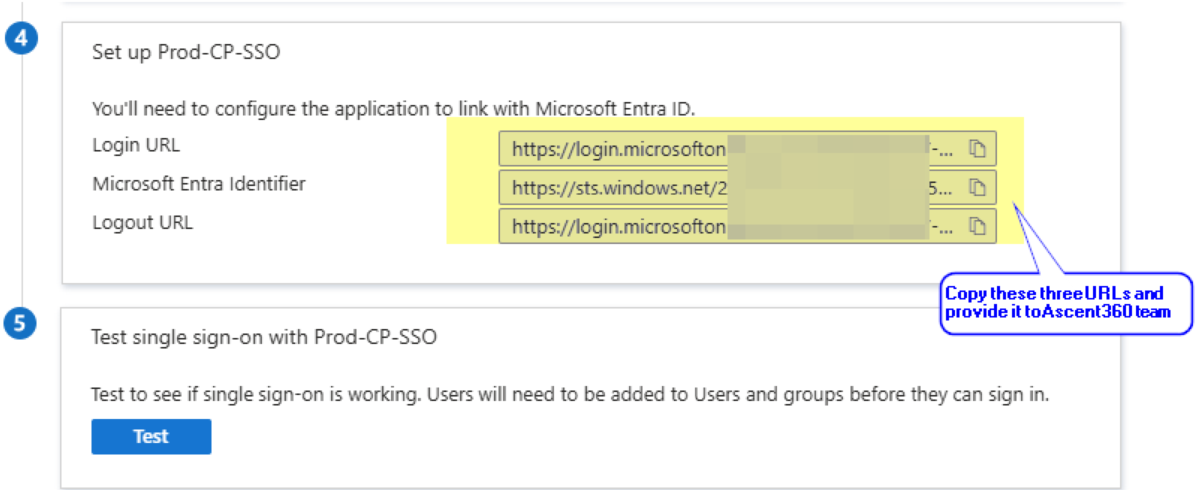
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate — Edit

Status	Active
Thumbprint	8[redacted]2C3
Expiration	1/13/2028, 2:00:33 PM
Notification Email	pdudhagundi@ascent360.com
App Federation Metadata Url	https://login.microsoftonline[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

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[redacted]-...
Microsoft Entra Identifier	https://sts.windows.net/2[redacted]5...
Logout URL	https://login.microsofton[redacted]-...

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.

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