

SINGLE SIGN ON (SSO) OVERVIEW

Owner

Amplifi.io Product Team

Summary

AMPLIFI.IO is a cloud-based digital asset management software designed to help product brands rapidly *organize, convert, manage and share* marketing content and digital assets.

Document Purpose

This document summarizes the concepts and set-up of the Amplifi.io SSO via SAML 2.0.

- **Benefits include:**
 - Single Sign On capabilities and security
 - Amplifi.io DAM system opens immediately for users and remembers user's collections
 - Admins can see user history
 - Streamlined bulk user onboarding
 - Ensure fast user access and broad system usability

Single Sign-On

Enterprise single sign-on allows employees in a company to access all the company applications with one set of credentials. Depending on the company, the credentials can include email, phone number or username along with the password. The company routes all logins through an IDP (Identity Provider) with which the company has a purchased license. The IDP usually hosts a login page for the employees to enter their company credentials before entering any application. Single Sign On provides better security with the central authentication point, limiting the possibility of phishing.

About enterprise single sign-on

When you enable enterprise single sign-on, you're bypassing Amplifi.io and authenticating your users externally. When users navigate to your Amplifi.io sign-in page or click a link to your Amplifi.io, they can authenticate by signing into a corporate server or a third-party identity provider.

If you're using enterprise single sign-on, your users' sign-in flow will follow the sequence below:

- 1) Users navigate to your Amplifi.io subdomain.
- 2) If not already authenticated, users are redirected to your corporate server or third party identity provider login page, depending on the enterprise SSO option you selected.
- 3) Users enter their sign-in credentials.
- 4) If valid, users are redirected back to the Amplifi.io home page.

Note: Users can also start the sign-on process from your corporate server or the third-party identity provider sign-in page. They will then be authenticated automatically when accessing Amplifi.io.

All users can sign in to your Amplifi.io using enterprise single sign-on.

The advantage to using enterprise single sign-on is that you have complete control over your users, behind your firewall. You authenticate your users once, against your own user authentication system, and then grant them access to many other resources both inside and outside of your firewall. This does not mean that your Amplifi.io user management is performed outside of your Amplifi.io subdomain, the user accounts must exist within Amplifi.io to allow access. So if you add a user account for a new employee, you will need to create the user using their email address on Amplifi.io.

By default, the only data that Amplifi.io stores for each user is their name and email address.

Enterprise single sign-on options

There are two types of enterprise single sign-on options available in Amplifi.io:

Secure Assertion Markup Language (SAML) is not enabled by default and requires proper licensing to be enabled. SAML is supported by many identity provider services, such as Okta, Active Directory, and LDAP.

Using SAML

Amplifi.io Support supports Secure Assertion Markup Language (SAML), which allows you to provide single sign-on (SSO) for your Amplifi.io Support account using enterprise identity providers such as Active Directory and LDAP. Single sign-on using SAML is available on Amplifi.io Professional and Enterprise edition.

Implementing single sign-on via SAML means that the sign in process and user authentication are handled entirely outside of Amplifi.io Support. Your users will not directly visit your Amplifi.io login page to sign in. Instead users sign in to the corporate system (authenticated by Active Directory or LDAP for example) and click a link to access Amplifi.io and are automatically signed in. No need to enter separate sign-in credentials for Amplifi.io.

The user data required to be stored in Amplifi.io is the user's name and email address. However, there are other fields available to enrich the user's information such as their geographical location. You do this by adding these attributes to your SAML assertion code. See User attributes that can be set in SAML. Amplifi.io does not store user passwords.

How SAML for Amplifi.io works

SAML for Amplifi.io works the way SAML does with all other service providers. The typical use case is that your users belong to a corporation and all user authentication is managed by your corporate authentication system (for example, Active Directory or LDAP), which is referred to generically as an identity provider (IdP). The service provider (SP), in this case Amplifi.io, establishes a trust relationship with IdP and allows that external IdP to authenticate users and then seamlessly sign them in to Amplifi.io. In other words, a user signs in at work and then has automatic access to the many other corporate applications such as email, your CRM, and so on without having to sign-in separately to those services. Aside from the convenience this provides to users, all user authentication is handled internally by a system that you have complete control over.

After you've enabled SAML as the type of single sign-on for Amplifi.io, users who visit your Amplifi.io account and attempt to sign in are redirected to your SAML server for authentication. Your users' identities can be stored either on the SAML server or can be validated by an identity directory such as Microsoft Active Directory or LDAP. Once authenticated, users are redirected back to your Amplifi.io account and automatically signed in.

Another supported workflow is having the user sign in to your own website directly rather than to your Amplifi.io instance. The website sends a request to the identity provider to validate the user. The website then sends the provider's response to the SAML server, which forwards it to your Amplifi.io instance, which grants a session to the user.

Returning visitors are automatically authenticated if their SAML assertions are cached. Assertions are packets of security information that are used to make access-control decisions.

Configuring Amplifi.io for new users

An Amplifi.io user profile is created for any new user who accesses your Amplifi.io account through SAML. Because they're authenticated with a non-Amplifi.io password, the profile is created without a password because they don't need to sign in to Amplifi.io.

Configuring your SAML implementation

You have a number of options when considering a SAML service, including building a SAML server in-house (for example, OpenAM) or choosing a SAML service such as Okta, OneLogin, and PingIdentity.

To set up SAML in your Amplifi.io, you'll need the following:

A SAML server with provisioned users or connected to an identity repository such as Microsoft Active Directory or LDAP

The Remote Login URL for your SAML server (sometimes called SAML Single Sign-on URL)

The SHA1 or SHA2 fingerprint of the SAML certificate from your SAML server. X.509 certificates are supported and should be in PEM or DER format. There is no upper limit on the size of the SHA fingerprint.

After you have your SAML server properly configured, you can use the remote login URL and the SHA fingerprint to configure SAML in Amplifi.io.

Required Profile Data

Required field attributes are (case-sensitive) for your SAML user token:

email

firstname

lastname

phone (optional)

language_code (optional) - ISO 639-1 code. Refer here:

https://en.wikipedia.org/wiki/List_of_ISO_639-1_codes -

Assertion Consumer Service URL:

[https://saml.amplifi.io/saml/module.php/saml/sp/saml2-accs.php/\[companyname\]](https://saml.amplifi.io/saml/module.php/saml/sp/saml2-accs.php/[companyname])

Where "**companyname**" is the name/alias of the Organization

The customer's Amplifi.io DAM instance url is <https://companyname.amplifi.io>

Entity ID:

companyname (where "**companyname**" is the name/alias of the organization)

Redirects to SAML Single Sign-on URL are HTTPS POST

Hashing algorithm (ADFS): Amplifi.io can use either SHA-1 or SHA-2 (SHA-256) algorithm when using Active Directory Federation Services (ADFS)

Integration with Active Directory Federation Services (ADFS)

Currently, we only support Forms Based Authentication for ADFS. Integrated Windows Authentication is not supported.

SAMPLE: MICROSOFT AZURE AD SETUP

Amplifi.io and Microsoft Azure AD SSO Set-up

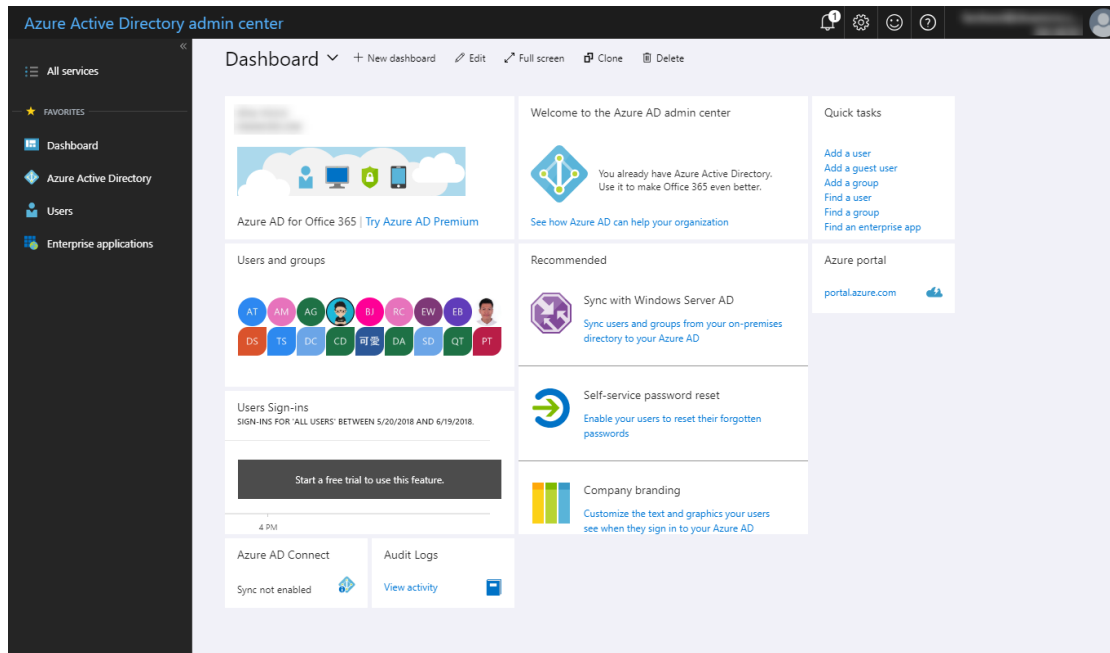
Please note that the information on these screens are generic names and your organization will need to obtain Amplifi.io specific items from the support or onboarding team managing your account.

Specifically:

- **Entity ID**
- **Reply URL** (your full amplifi.io subdomain with no trailing slash)
- **SAML Token Attributes** (outlined above in the **Required Profile Data** section)

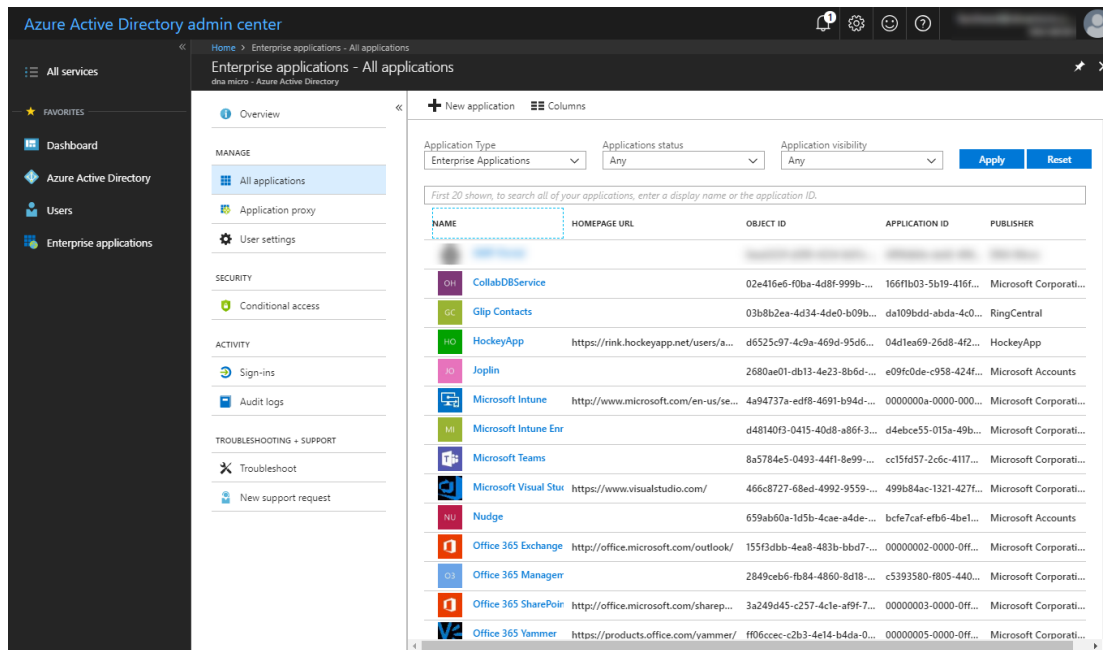
Once the setup is complete the Amplifi team needs to obtain the Metadata XML generated in order to fully activate the SSO service for your company.

1) Log in to your Azure AD admin center

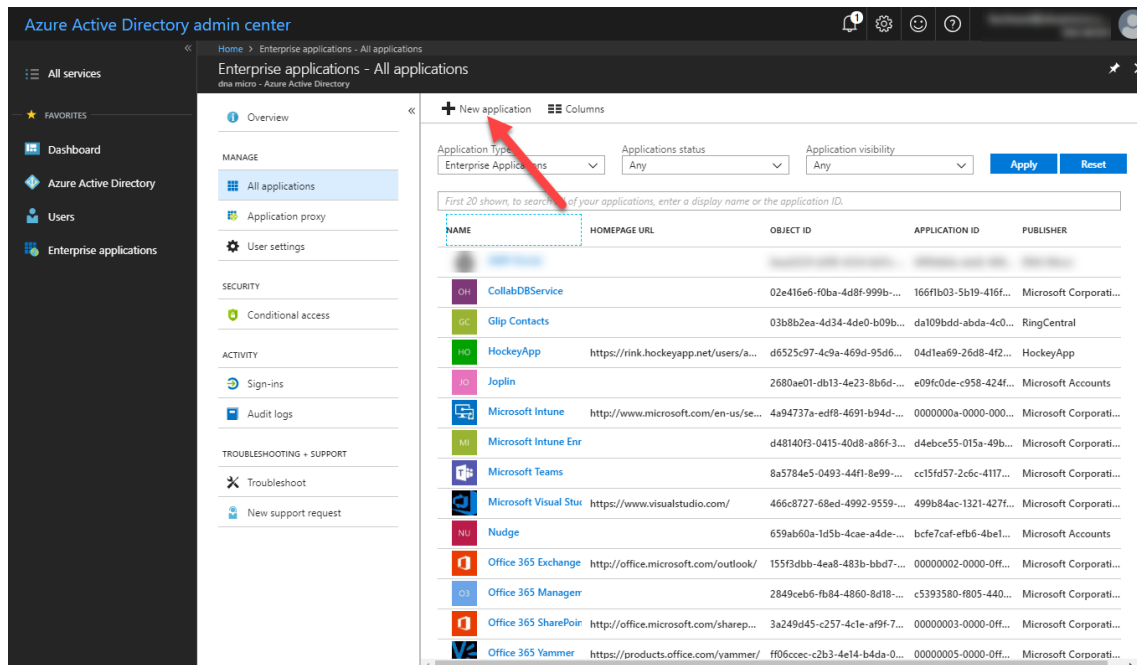


The screenshot displays the Azure Active Directory admin center dashboard. The interface includes a top navigation bar with the title "Azure Active Directory admin center" and a "Dashboard" dropdown menu. A left-hand sidebar lists "All services" and "FAVORITES" including "Dashboard", "Azure Active Directory", "Users", and "Enterprise applications". The main content area is divided into several sections: a "Welcome to the Azure AD admin center" message, a "Quick tasks" panel with links like "Add a user" and "Add a guest user", a "Users and groups" section showing a grid of user icons, a "Recommended" section with "Sync with Windows Server AD", "Self-service password reset", and "Company branding" options, and a "Users Sign-ins" section with a "Start a free trial to use this feature" button. At the bottom, there are "Azure AD Connect" and "Audit Logs" status indicators.

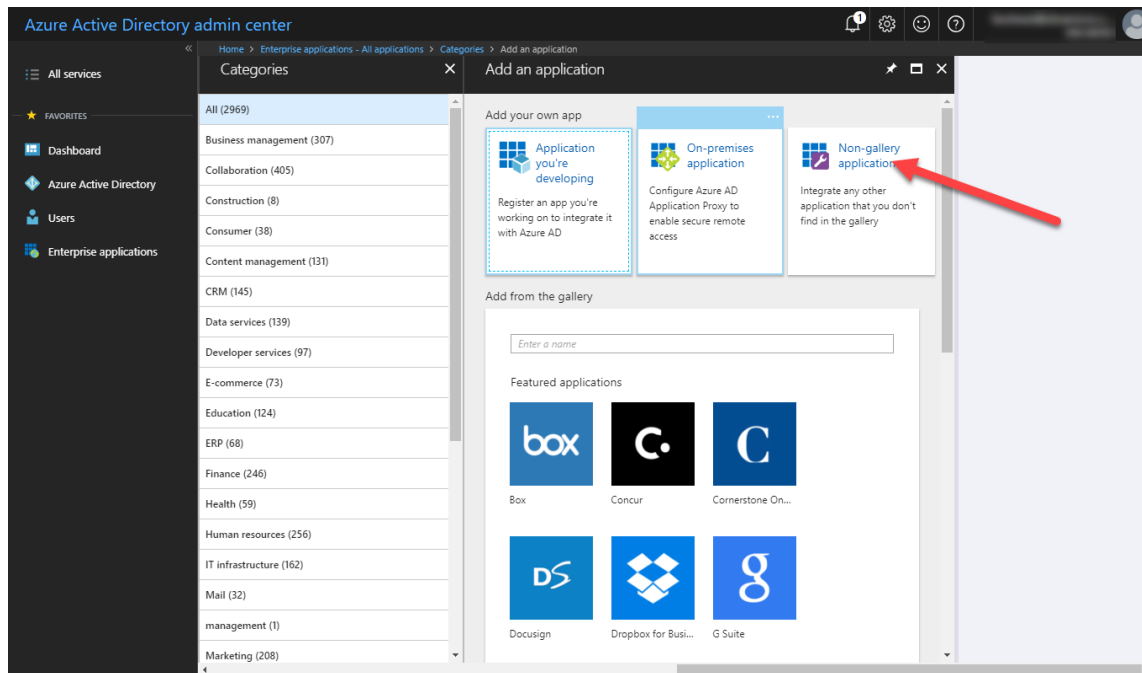
2) Go to Enterprise Applications



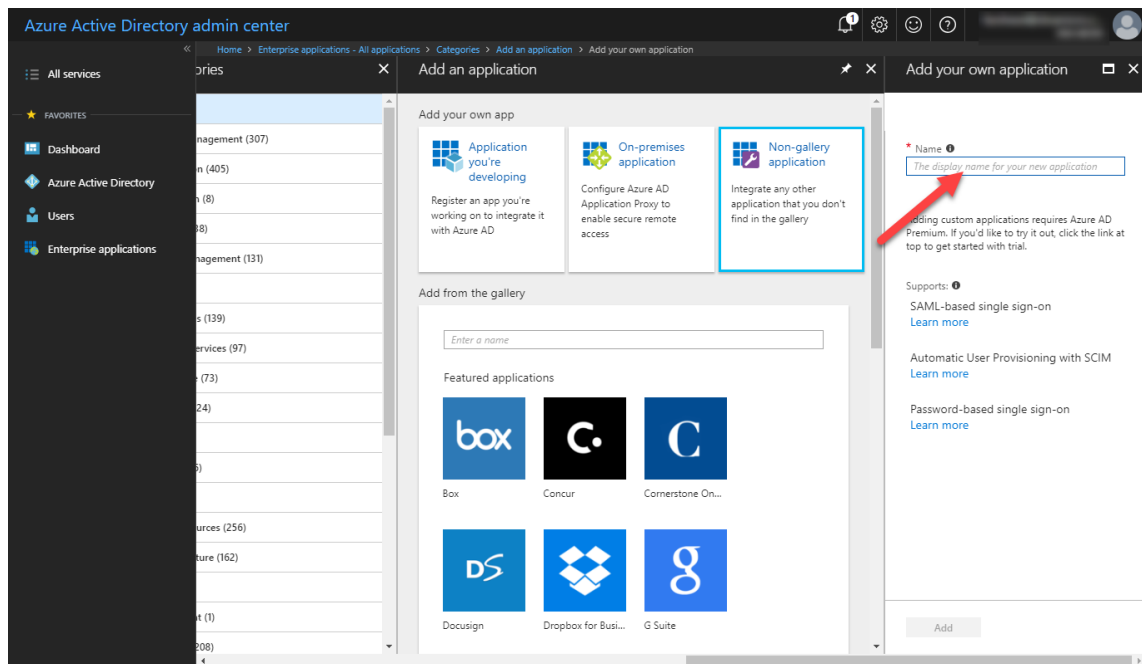
3) Click on + New application



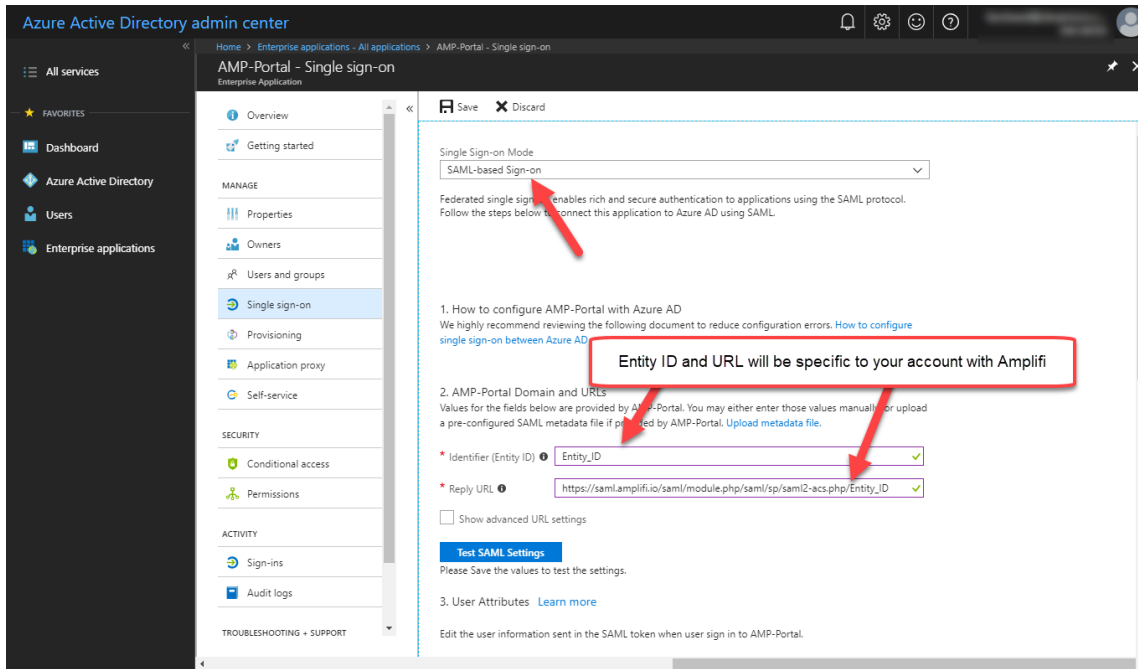
4) Click on 'Non-gallery' application



5) Specify a name such as 'Amplifi.io'



6) Select SAML and Entity ID as Provided by Amplifi.io



Azure Active Directory admin center

Home > Enterprise applications > All applications > AMP-Portal - Single sign-on

AMP-Portal - Single sign-on

Enterprise Application

Save Discard

Single Sign-on Mode
SAML-based Sign-on

Federated single sign-on enables rich and secure authentication to applications using the SAML protocol. Follow the steps below to connect this application to Azure AD using SAML.

1. How to configure AMP-Portal with Azure AD
We highly recommend reviewing the following document to reduce configuration errors: [How to configure single sign-on between Azure AD](#)

2. AMP-Portal Domain and URLs
Values for the fields below are provided by AMP-Portal. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by AMP-Portal. [Upload metadata file](#).

* Identifier (Entity ID) ✓

* Reply URL ✓

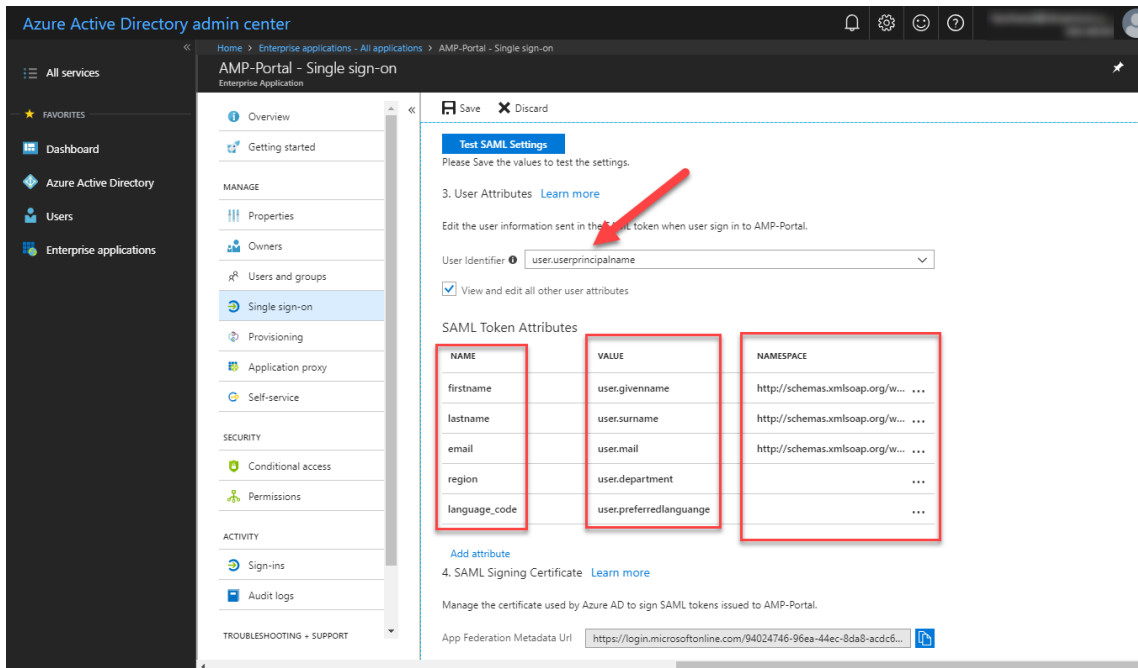
Show advanced URL settings

[Test SAML Settings](#)
Please Save the values to test the settings.

3. User Attributes [Learn more](#)

Edit the user information sent in the SAML token when user sign in to AMP-Portal.

7) Define SAML Tokens (As Applicable)



Azure Active Directory admin center

Home > Enterprise applications > All applications > AMP-Portal - Single sign-on

AMP-Portal - Single sign-on

Enterprise Application

Save Discard

[Test SAML Settings](#)
Please Save the values to test the settings.

3. User Attributes [Learn more](#)

Edit the user information sent in the SAML token when user sign in to AMP-Portal.

User Identifier

View and edit all other user attributes

SAML Token Attributes

NAME	VALUE	NAMESPACE
firstname	user.givenname	http://schemas.xmlsoap.org/w... ..
lastname	user.surname	http://schemas.xmlsoap.org/w... ..
email	user.mail	http://schemas.xmlsoap.org/w... ..
region	user.department	...
language_code	user.preferredlanguage	...

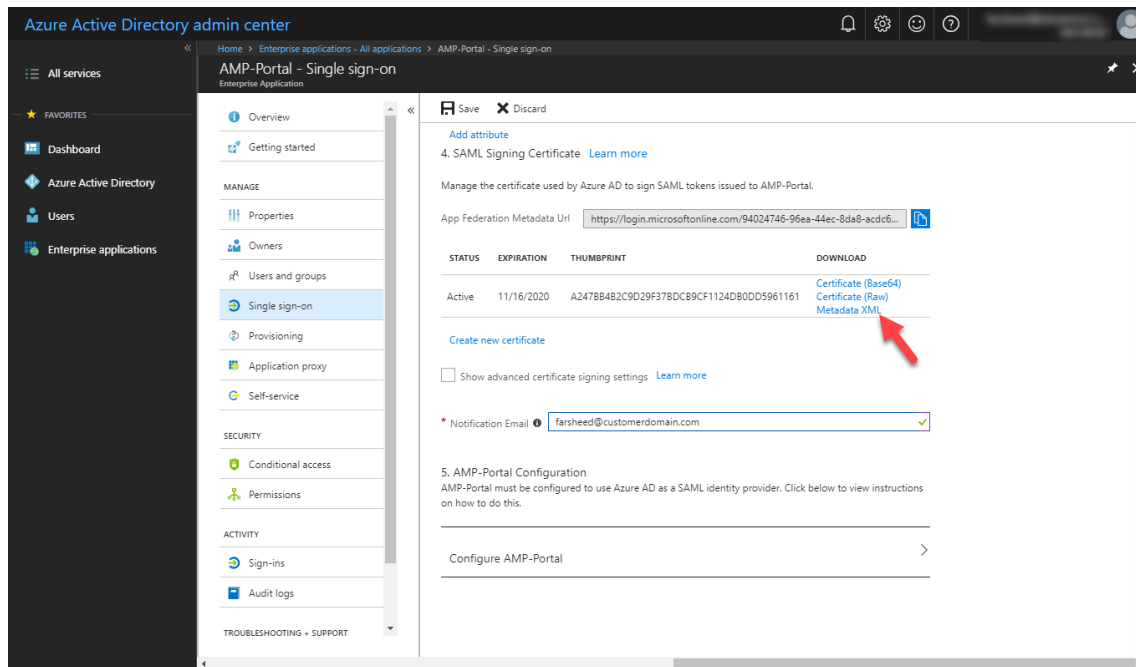
[Add attribute](#)

4. SAML Signing Certificate [Learn more](#)

Manage the certificate used by Azure AD to sign SAML tokens issued to AMP-Portal.

App Federation Metadata Url <https://login.microsoftonline.com/94024746-96ea-44ec-8da8-acdc6...>

8) Download Meta XML and Send to Amplifi Team



Azure Active Directory admin center

Home > Enterprise applications > All applications > AMP-Portal > Single sign-on

AMP-Portal - Single sign-on

Overview

4. SAML Signing Certificate [Learn more](#)

Manage the certificate used by Azure AD to sign SAML tokens issued to AMP-Portal.

App Federation Metadata Url <https://login.microsoftonline.com/94024746-96ea-44ec-8da8-acd6...>

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	11/16/2020	A2478B482C9D29F378DC89CF1124D80DD5961161	Certificate (Base64) Certificate (Raw) Metadata XML

[Create new certificate](#)

Show advanced certificate signing settings [Learn more](#)

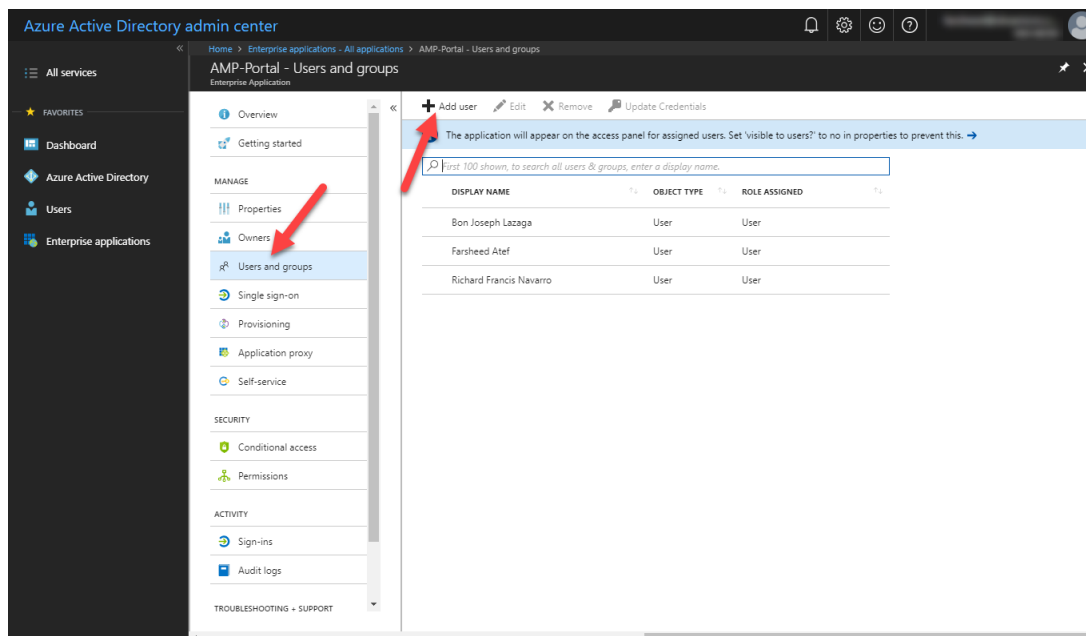
* Notification Email

5. AMP-Portal Configuration

AMP-Portal must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.

[Configure AMP-Portal](#)

9) Provide Access to Your Users



Azure Active Directory admin center

Home > Enterprise applications > All applications > AMP-Portal > Users and groups

AMP-Portal - Users and groups

[Add user](#) [Edit](#) [Remove](#) [Update Credentials](#)

The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
Bon Joseph Lazaga	User	User
Farsheed Atef	User	User
Richard Francis Navarro	User	User