WP ENGINE SAML SSO - AZURE AD

WordPress Site Configuration

WP Engine-hosted WordPress sites can be configured to use SAML authentication for users based on their presence in an Azure AD tenant. This is accomplished using the WordPress OneLogin SAML SSO plugin. Most of the plugin's features can be ignored, but the others have very specific values that must be precise. Azure tenants must also be provisioned by a Texas A&M Azure administrator.

Make An Appointment With Identity Management

Schedule a "Integrate an Application with NetID" appointment for the creation of a new SAML SSO integration with Azure AD and include a list of the websites you want to set up. Know that each website takes time to integrate from both you and Identity Management so time constraints will be considered. An Azure Enterprise Application must be created for each website (but not for the development environment of a live website) by an Azure administrator. Only after that is done should a site's plugin be configured to authenticate a user within an Azure Active Directory tenant.

Before The Appointment

Before the appointment, install but do not activate the OneLogin SAML SSO plugin on each website you would like to authenticate with.

During The Appointment

Log in to your website, https://portal.azure.com/, and open this document for reference. You will be configuring settings for both the SSO plugin and your new Enterprise Application in Azure Active Directory.

Configure the OneLogin SAML SSO Plugin Settings

Identity Provider Settings

In your WordPress plugin's settings page under Identity Provider Settings, copy the following values from your Azure Enterprise Application's "Single sign-on" page.

(Azure field) => (WordPress field)

1. Azure AD Identifier => IdP Entity ID
2. Login URL => Single Sign On Service URL
3. Login URL => Single Log Out Service URL
4. SAML Signing Certificate => X.509 Certificate
    a. Click “Edit” in the “SAML Signing Certificate” box
    b. In the new SAML Signing Certificate overlay panel click the three dots next to the active certification’s thumbprint value.
    c. This will show a drop down - you then select "PEM certificate download".
    d. Copy the file contents from there and paste them into the SAML Signing Certificate field in WordPress
5. Service Provider Entity ID (urn:subdomain.domain.com)

Options

1. Set “Alternative ACS Endpoint” to Enabled
2. Set “Match WordPress account by” to Username

Other options are available but are less-often used. Ones that might be used are listed below. Others you may see have either been added since this document was created or are not likely to be used.

1. Create user if not exists
   “Auto-provisioning. If user not exists, WordPress will create a new user with the data provided by the IdP.”
2. Update user data
   “Auto-update. WordPress will update the account of the user with the data provided by the IdP.”
3. Force SAML login
   “Protect WordPress and force the user to authenticate at the IdP in order to access when any WordPress page is loaded and no active session.”
   This is useful if you have an internal-facing application, a testing environment, or a website with some other purpose that needs to ensure users are in the Active Directory tenant.
4. Keep Local login
   Only enable this while debugging. This plugin enhances security, so keeping the local login negates that effort.
5. Trigger wp_login hook
   “When enabled, the wp_login hook will be triggered.”

Enable this if you have a third party plugin conflict that needs this action hook to trigger.

Attribute Mapping

Under Attribute Mapping enter the following values:

1. **Username**: username
2. **E-mail**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
3. **First Name**: givenname
4. **Last Name**: surname

Advanced Settings (Service Provider Entity Id)

Under Advanced Settings, set Service Provider Entity Id to the value found in the plugin's XML metadata. This typically looks like "urn:subdomain.domain.com" and can be found by clicking the link at the top right of the plugin's settings page or at this URL: subdomain.domain.com/wp-login.php?saml_metadata

Configure the Azure Enterprise Application Settings

Basic SAML Configuration

First open your website's OneLogin plugin XML metadata page (see "Advanced Settings (Service Provider Entity Id)" above for instructions). We will use this in a moment. In your website's Azure Enterprise Application, under "Single sign-on", look at the "Basic SAML Configuration" section and click "Edit". Update the following fields in the overlay panel. You will find the "OneLogin Alternate Endpoint" in the XML metadata as the "Location" value of the "AssertionConsumerService" element. It probably looks something like this: https://subdomain.domain.com/wp-content/plugins/onelogin-saml-sso/alternative_acs.php

1. Identifier (Entity ID) => urn:subdomain.domain.com
2. Reply URL (Assertion Consumer Service URL) => OneLogin Alternate Endpoint

User Attributes & Claims

Due to how Azure Active Directory interprets TAMU NetID information, our current understanding is that a user's NetID username is most accurately obtained from the Azure "user.userprincipalname" meta. However, "user.userprincipalname" is equivalent to "netid@tamu.edu" and WordPress does not natively allow special characters in usernames. Therefore a "username" claim must be configured with a Source value of "Transformation"

to allow us to trim the trailing “@tamu.edu” from the “user.userprincipalname” value. The final list of claims should show in Azure as follows:

1. name - user.userprincipalname
2. emailaddress - user.userprincipalname
3. givenname - user.givenname
4. surname - user.surname
5. username - Trim (user.userprincipalname)
6. Unique User Identifier - user.userprincipalname

Multisite or Development Server

You can manage Active Directory authentication for multiple websites using the same Azure Enterprise Application. You might want to do this if you have a website with a production server and a staging server, or if you have a multisite network. To add more sites, install and configure the SSO plugin on those additional sites and then follow these steps:

1. On the Single sign-on page, look at the Basic SAML Configuration section and click the Edit link
2. In the panel overlay, under Identifier (Entity ID), add each site's Entity ID (example: urn:subdomain.domain.com)
3. Under Reply URL, add each site’s alternative login URL which is found in each site’s SSO plugin settings page’s metadata XML page link (example: https://subdomain.domain.com/subdirectory/wp-content/plugins/onelogin-saml-sso/alternative_acs.php)