# Configuring Azure AD with PHPKB SAML Single Sign-On (SSO) Plugin

274 Q Palwinder Singh H June 10, 2022 Documentation



In this article, we will guide you with steps on **how to configure Azure AD** with the SAML Single Sign-On (SSO) Plugin of PHPKB knowledge base software.

## Configuring Azure AD with SAML SSO Plugin

You need to be logged in to the admin control panel of PHPKB software with the Superuser account. Once you are logged in as a superuser, please follow the instructions given below,

### 1. Configure Azure AD as Identity Provider (IdP)

- a. In Tools > Manage Settings > SAML tab, click View Metadata of this SP button. Here, you can find the SP metadata such as SP Entity ID and ACS (AssertionConsumerService) URL which are required to configure the Identity Provider.
- b. Log in to Azure AD Portal
- c. Select Azure Active Directory > App registrations and click on the New registration option:

Default Directory	App registrations 🛷	×
0 Overview	+ New registration 🕀 Endpoints 🤌 Troubleshooting 🛓 Download 🐻 Preview features   🛇 Got feedback?	
of Getting started	1 Try out the new App registrations search preview. Click to enable the preview. →	×
Preview hub		
Manage	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more	×
L Users		
A Groups	All applications Owned applications Applications from personal account	
External Identities	A Start typing a name or Application ID to filter these results	
Roles and administrators		
Administrative units	This account isn't listed as an owner of any applications in this directory.	
Reference applications	View all applications in the directory	
Devices	View all applications from personal account	
R App registrations		
All second and second		

d. Assign a **Name** and choose the account type. In the Redirect URI field, provide the ACS URL provided in the **View Metadata of this SP** and click on the **Register** button:



- Register
- e. Navigate to Expose an API menu option and click the Set button and replace the APPLICATION ID URI with the Service Provider Entity ID (provided in the View Metadata of this SP). Alternatively, you can set this value (start Powered by PHPKB (Knowledge Base Software)

copying after "//" (double slash), for example: b23eaba2-5499-40d3-80fa-7cf5f432cefb) in **Manage Settings** > **SAML** tab > **Service Provider Entity ID** (SP Entity ID) field:

×



**NOTE**: Please ensure that the SP Entity ID value from the View Metadata of this SP does not have a trailing slash('/'). If SP Entity ID has a trailing slash then update it by removing the trailing slash from the SP EntityID / Issuer field under the Service Provider Metadata tab of the plugin, enter the updated value at Azure and click on the Save button.

f. Go back to Azure Active Directory > App Registrations window and click on the Endpoints option:

Home > Default Directory		Endpoints	×
Default Directory	App registrations		
and a state of the	«	OAuth 2.0 authorization endpoint (v2)	
Ovaniew	<ul> <li>+ New registration</li> <li>Endpoints</li> </ul>	https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/oauth2/v2.0/authorize	D
Overview		OAuth 2.0 token endpoint (v2)	
Getting started	Try out the new App registrations	https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/oauth2/v2.0/token	D
Preview hub		(or 1000 provide a sector of the sector of t	
X Diagnose and solve problems		Https://lopin.microsoftonline.com/dcb7944d-b98e-dbd0-a989-5ce8047b178b/nauth2/authorize	Ph
Manage	Atarting June 30th, 2020 we will no support and security updates but	Dauth 3.0 folkers and point 4:01	
& Users	Graph. Learn more	https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/oauth2/token	D
A Groups	All applications Owned applics	OpenID Connect metadata document	
External Identities	An applications Owned applica	https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/v2.0/.well-known/openid-configuration	0
& Roles and administrators	Start typing a name or Application	Microsoft Graph API endpoint	
Administrative units		https://graph.microsoft.com	Ð
Enternice analications		Federation metadata document	
The second secon		https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/federationmetadata/2007-06/federationmetadata.xml	0
Devices		WS-Federation sign-on endpoint	
App registrations		https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/wsfed	Ð
Identity Governance		SAML-P sign-on endpoint	
Application proxy		https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/saml2	0
Licenses		SAML-P sign-out endpoint	
Azure AD Connect		https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/saml2	Ð
🔁 Custom domaín names			_
A Mabile APAL and MARA			

## 2. Configuring PHPKB as Service Provider (SP)

Login to PHPKB Admin Panel with the superuser credentials.

Go to **Tools** > **SAML Authentication** tab and configure **PHPKB** as **Service Provider** (SP). Provide the required settings (i.e. IdP Entity ID or Issuer, SSO Service URL, or Login URL) as provided by your Identity Provider.

Attribute Mapping: The Attribute Mapping feature allows you to map the user attributes sent by the IdP during SSO to the user attributes at PHPKB. In the **Tools > SAML Authentication** tab, go to the **Attribute Mapping** section, and fill up the following fields in the **Attribute Mapping** section.

e IdP do not match the names used by PHPKB for the user accounts. In this section you can set the mapping between Id	P fields and PHPKB fields. Note: This
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	🖺 SAVE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	
The attribute that contains the role of the user. For example 'memberOf'.	
Editor	
	e kdP do not match the names used by PHPKB for the user accounts. In this section you can set the mapping between ld http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname Ittp://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname Ittp://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname Ittp://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname Ittp://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname Ittp://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname Ittp://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

#### **Role Mapping**

This feature allows you to assign and manage the roles of the users when they perform SSO because IdP can use its own roles.

From the **Role Mapping** section of the SAML tab, provide a mapping for the field named Writer, Editor, etc. This attribute will contain the role-related information sent by the IdP and will be used for Role Mapping.

Navigate to the role mapping section and provide the mappings for the highlighted roles as comma-separated-values (CSV) of their IdP roles.

**Example**: If you wish to assign the PHPKB user-level "**Superuser**" to the Azure AD "Application Administrator", "Knowledge Administrator", "Knowledge Manager", and "Helpdesk Administrator" roles, then put them as commaseparated-values next to the "Superuser" field shown below. You may wish to refer to the default roles available in Azure AD.

ROLE MAPPING					
The IdP can use its own roles. In this section, you can set the mapping between IdP and PHPKB roles. Accepts comma separated values. Example: admin,owner,superuser					
Member					
Writer					
Writer-Trusted					
Editor					
Superuser	Application Administrator, Knowledge Administrator, Knowledge Manager, Helpdesk Administrator				

#### **Role Precedence**

In some cases, the IdP returns more than one role. In this section, you can set the precedence of the different roles. The smallest integer will be the role chosen.

#### **Advanced Settings**

Handle some other parameters related to customizations and security issues. If signing/encryption is enabled, then x509 cert and private key for the SP must be provided. You can also enable the Debug Mode to get errors/warnings that happen during the SAML workflow.

**Note:** In the **federationmetadata.xml** file from Azure AD, there are four **X509** certificates, and you can use the **second one** in the list, located under EntityDescriptor/RoleDescriptor/KeyDescriptor[2]/KeyInfo/X509DataX509Certificate.

**Caution:** Kindly be aware that, by default, <u>Microsoft updates this certificate every 45 days</u>, so the previous one will expire after this time, and you will have to update it manually.

#### **Custom Fields**

**Applicable To:** Enterprise Edition (MySQL), Enterprise Multi-Language Edition (MySQL), Enterprise Edition (SQL Server), Enterprise Multi-Language Edition (SQL Server)

Online URL: https://www.phpkb.com/kb/article/configuring-azure-ad-with-phpkb-saml-single-sign-on-sso-plugin-274.html