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

Palwinder Singh 5.18K 0

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

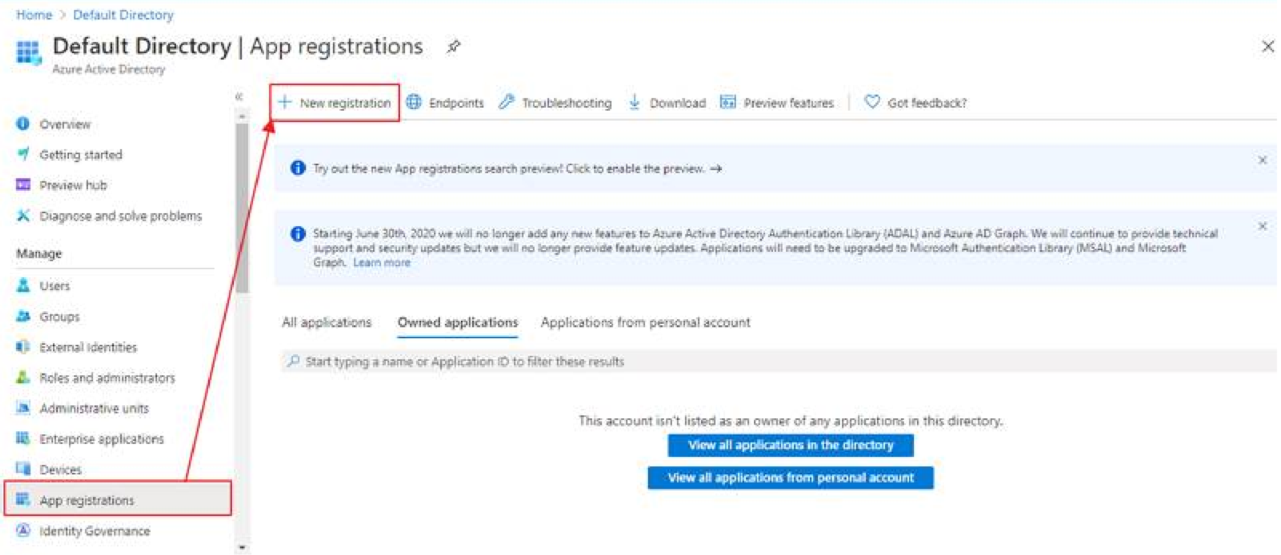
You need to be logged in to the admin control panel of PHPKB software with the Superuser account. Once you are logged in as a superuser, please follow the instructions given below,

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:



Try out the new App registrations search preview! Click to enable the preview. →

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

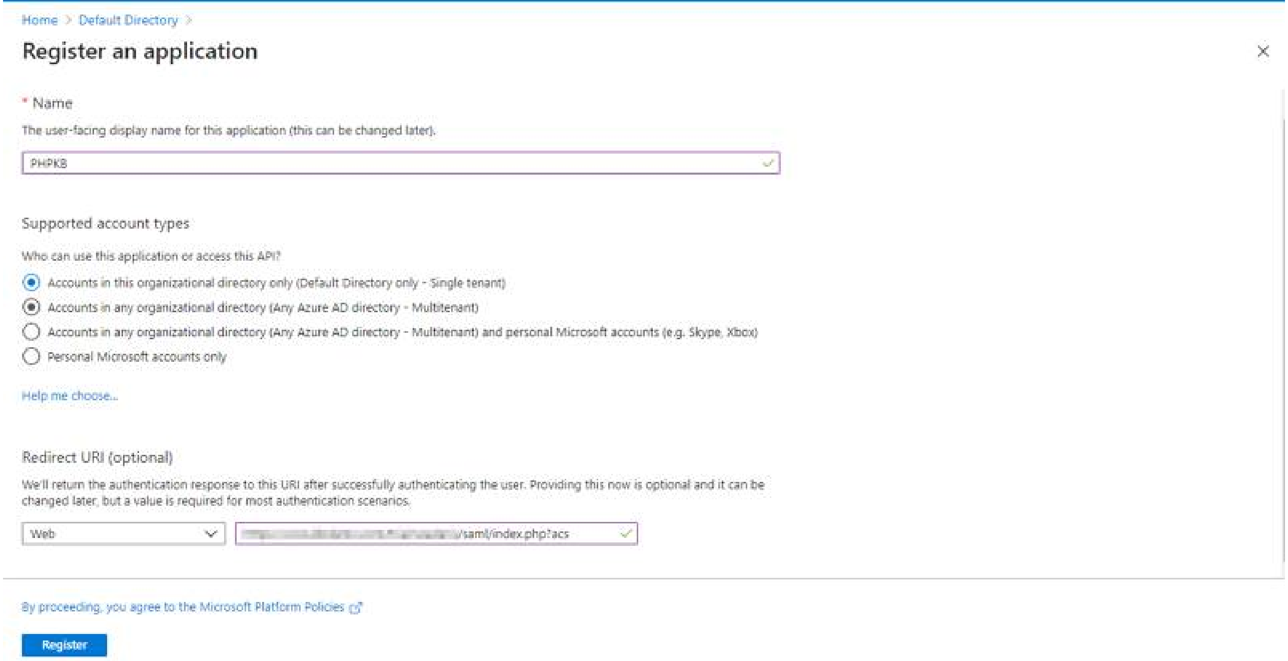
This account isn't listed as an owner of any applications in this directory.

   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:

Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.



Home > Default Directory >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

PHPKB

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant)

● Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

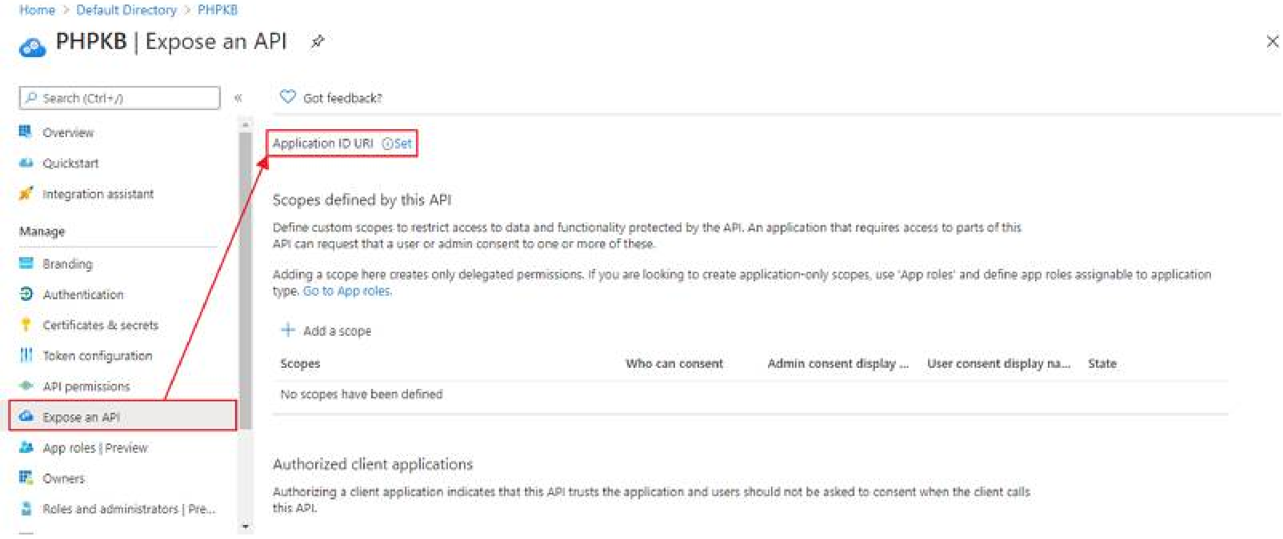
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | [redacted]/saml/index.php?acs

By proceeding, you agree to the Microsoft Platform Policies

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



Home > Default Directory > PHPKB

PHPKB | Expose an API

Application ID URI ⓘ Set

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
No scopes have been defined				

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

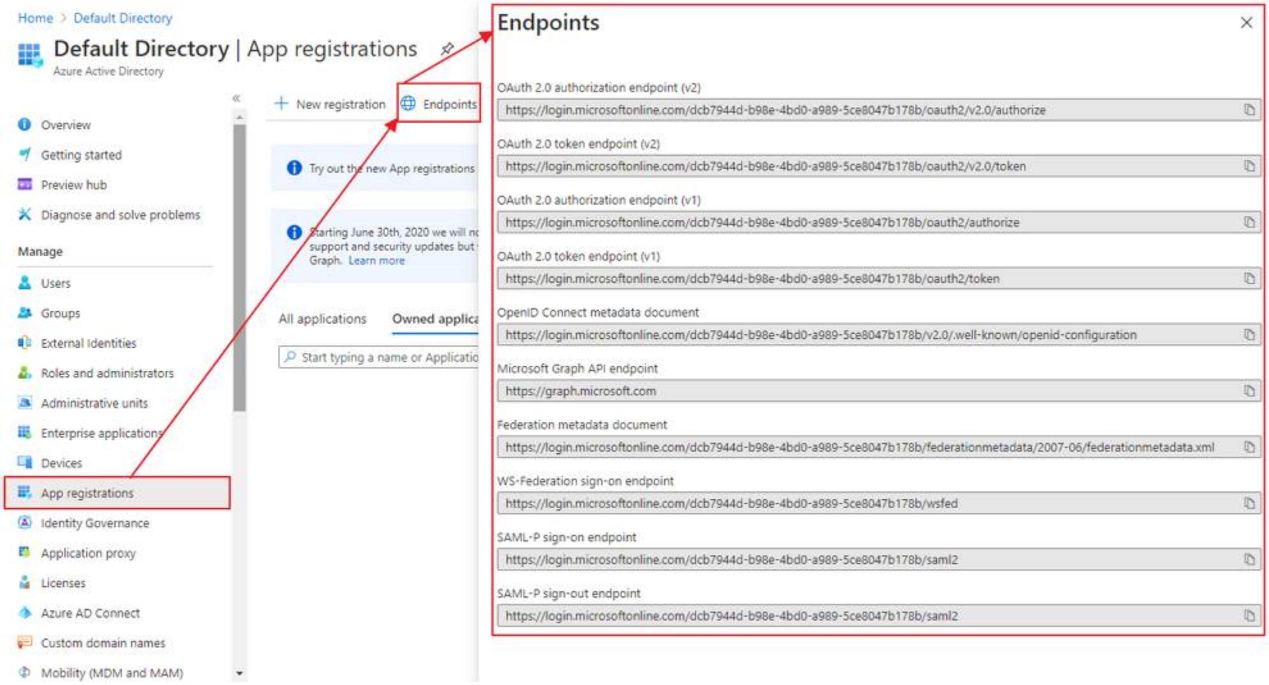
NOTE: Please ensure that the SP Entity ID value from the View Metadata of this SP does not have a trailing slash('/'). If SP Entity ID has a trailing slash then update it by removing the trailing slash from the SP EntityID / Issuer field under the Service Provider Metadata tab of the plugin, enter the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

Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.



Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/v2.0/.well-known/openid-configuration

Microsoft Graph API endpoint
https://graph.microsoft.com

Federation metadata document
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/federationmetadata/2007-06/federationmetadata.xml

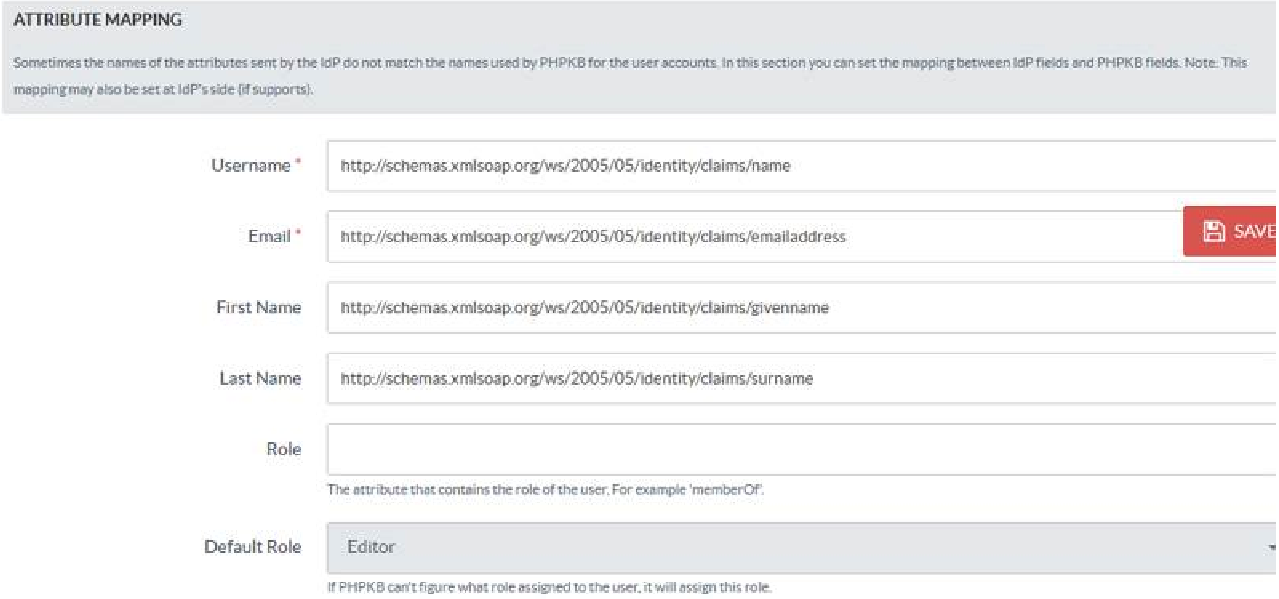
WS-Federation sign-on endpoint
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/wsfed

SAML-P sign-on endpoint
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/saml2

SAML-P sign-out endpoint
https://login.microsoftonline.com/dcb7944d-b98e-4bd0-a989-5ce8047b178b/saml2

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.



ATTRIBUTE MAPPING

Sometimes the names of the attributes sent by the IdP do not match the names used by PHPKB for the user accounts. In this section you can set the mapping between IdP fields and PHPKB fields. Note: This mapping may also be set at IdP's side (if supports).

Username * http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Email * http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

First Name http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Last Name http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Role

The attribute that contains the role of the user. For example 'memberOf'.

Default Role Editor

If PHPKB can't figure what role assigned to the user, it will assign this role.

- ## 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-

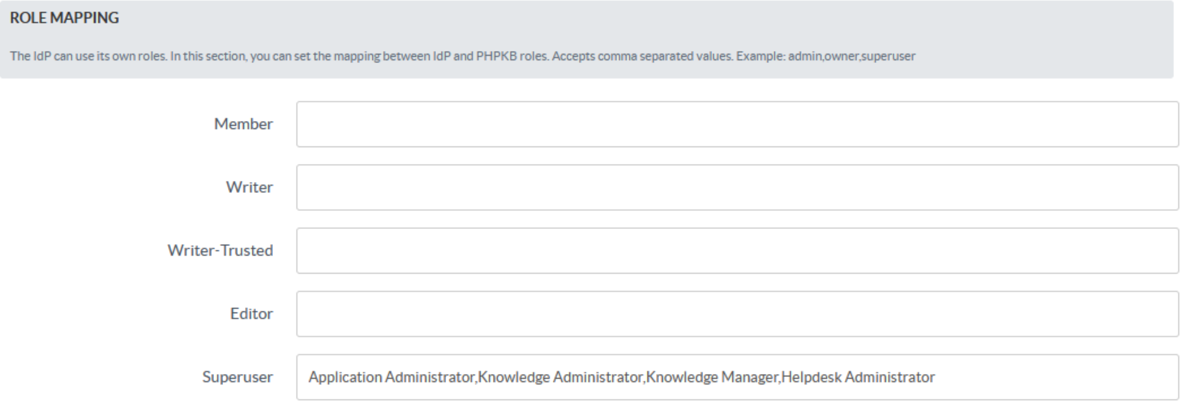
Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

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 comma-separated-values next to the "Superuser" field shown below. You may wish to refer to the default roles available in Azure AD.



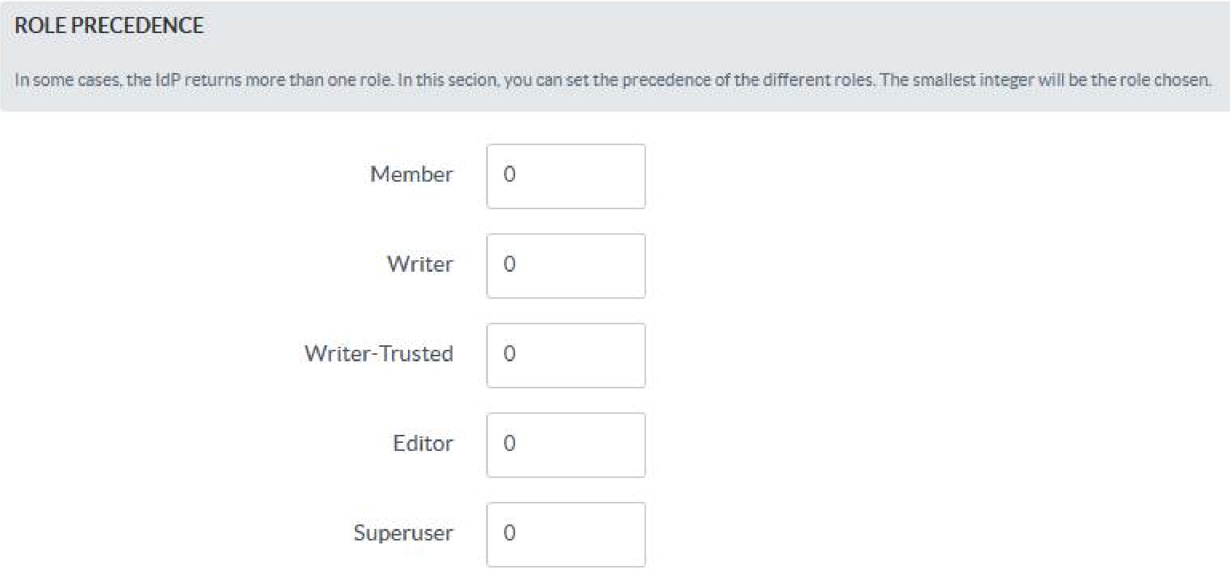
ROLE MAPPING

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.



ROLE PRECEDENCE

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

Member	0
Writer	0
Writer-Trusted	0
Editor	0
Superuser	0

- ## 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, Microsoft updates this certificate every 45 days, so the previous one will expire after this time, and you will have to update it manually.

Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

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

Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.