

# Omega 365 Cloud

18-Jun-2023 | Author N/A

---



## Omega 365 Cloud

Simple, Secure and Agile

### Simple

[Omega 365](#) is hosted online relieves your IT resources by requiring only an internet connection. Its API can help you customize the final integration with the existing systems step.

- Instant and continuous access without the risks, costs and administrative responsibilities associated with maintaining the required IT infrastructure.
- Ability to scale rapidly to meet growing business needs.
- Access to comprehensive security, backup and disaster recovery.
- Access to applications without the burden of maintaining a distributed computing environment.

### Secure

Omega 365 are ISO 27001 certified and a partner with the industry leader cloud provider Microsoft Azure to ensure privacy, security and compliance for the infrastructure and environment.

Microsoft is compliant across a diverse set of regulations. For more information about a specific compliance program, please see [Microsoft Azure Trust Center](#).

### Agile

Omega 365 is a SaaS platform designed to streamline project and asset management across various sectors, including Oil & Gas, Industrial, Construction, Mining, and Infrastructure. Offering complete integration capabilities, Omega 365 caters to organizational requirements for planning, execution, control, and effective management of projects and assets, irrespective of their size. Leverage the power of seamless process integration and enable your teams to drive performance, by embracing and implementing your organization's proven best practices.

### Broad Global Reach

Available to be hosted within any of the [Microsoft Azure public cloud regions](#).

# Omega 365 Cloud

Setup - Authentication - OpenID Connect - Configuring Azure AD Tenant.....	3
Setup - Authentication - Azure AD Tenant Users Sync Service.....	10
Setup - Authentication - SAML 2.0 - Configuring Azure AD Tenant.....	13
Setup - Authentication - SAML 2.0 - Configuring Keycloak.....	16
Setup - Authentication - SAML 2.0 - Configuring Okta.....	19

# OpenID Connect - Configuring Azure AD Tenant

22-Dec-2023 | Andriejus Koleinikovas

## OpenID Connect with Azure AD

This authentication method uses application in Microsoft 365 / Office 365 / Azure AD tenant to authenticate Omega 365 / Pims solutions users with their organisation's account.

### Setup Options

## Single tenant

Only users from single Azure Active Directory tenant can authenticate against the solution using this authentication method.

## Multitenant

Users from any Azure Active Directory tenant can authenticate against the solution using this authentication method.

### Application Setup

Log on to Azure Portal (<https://portal.azure.com>) and navigate to the Azure Active Directory resource.

Under the *Manage* section, find *App registrations* and begin registration of a new application.

- Give the application a name (for example Pims or Omega 365).
- Choose either the single tenant or multitenant option under *Supported account types*.
- Add the solution's redirect URI. The redirect URI is the solution's root URL with /login path. For example, <https://demo.omega365.com/login>.

**Register an application** ...

\* Name

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

Omega 365 Demo ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Omega 365 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 ✓  ✓

## Setup - Authentication - OpenID Connect - Configuring Azure AD Tenant

The next configuration steps are a different for Pims and Omega 365 authentication setup. Please see the section for your product.

### Application Setup for Omega 365

Navigate to Authentication tab and check *ID tokens (used for implicit and hybrid flows)* checkbox under Implicit grant and hybrid flows.

Next, choose single tenant or multitenant access mode under *Supported account types*.

Omega 365 Demo | Authentication

Search (Ctrl+/) Save Discard Got feedback?

Overview Quickstart Integration assistant Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators | Preview Manifest Support + Troubleshooting Troubleshooting New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web Quickstart Docs Add URI

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions.](#)

https://demo.omega365.com/login

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Omega 365 only - Single tenant)

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

Switch to *API permission* tab and add additional required Microsoft Graph permissions.

Manage

Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles

Configured permissions


Applications are authorized to call APIs when they are granted permissions by users/admins. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Omega 365

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

## Request API permissions

[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

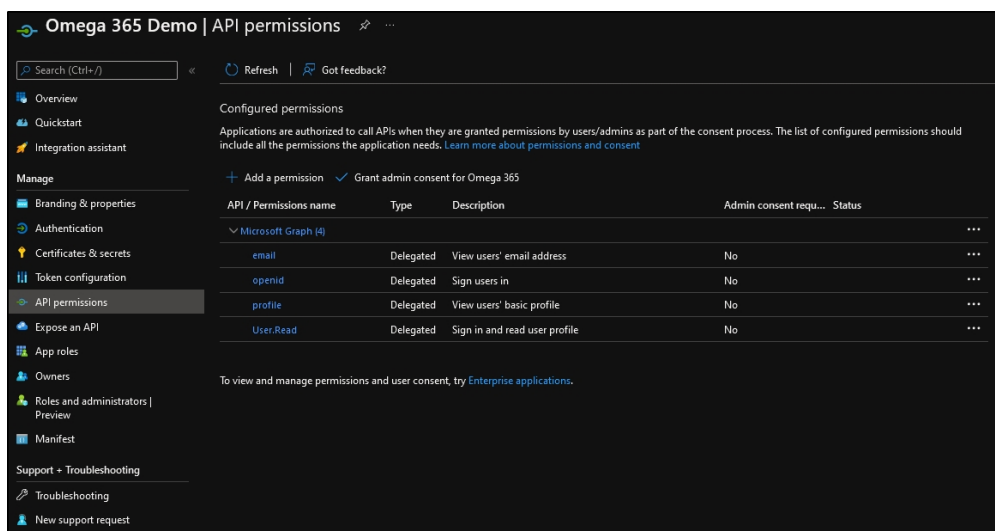
Application permissions

Your application runs as a background service or daemon without a signed-in user.

- Microsoft Graph - Delegated permissions - openid
- Microsoft Graph - Delegated permissions - email
- Microsoft Graph - Delegated permissions - profile

When delegated permissions are used, users logging in to the application will be presented with a standard permission consent dialog. To ease the login process, tenant's global administrator can consent for the whole organisation by clicking *Grant admin consent for <ORGANISATION>* button. Doing this will bypass permission consent dialog for all users.

The final API permissions setup should contain permissions displayed in the screenshot below.



**Omega 365 Demo | API permissions**

Search (Ctrl+F) Refresh Got feedback?

Overview Quickstart Integration assistant Manage Branding & properties Authentication Certificates & secrets Token configuration **API permissions** Expose an API App roles Owners Roles and administrators | Preview Manifest Support + Troubleshooting Troubleshooting New support request

Configured permissions

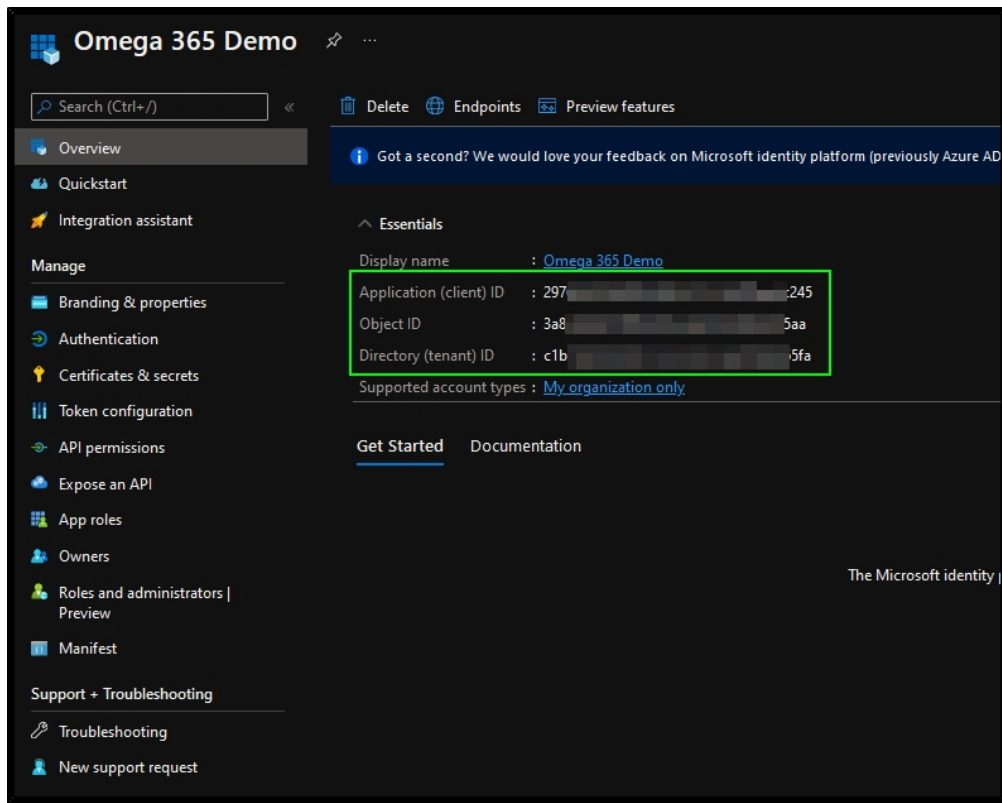
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Omega 365

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				...
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage permissions and user consent, try [Enterprise applications](#).

Finally, return to the *Overview* tab and note down *Application (client) ID* and *Directory (tenant) ID* values.



Once done, provide following to Omega 365:

- Directory (tenant) ID
- Application (client) ID
- Application access mode (single tenant or multitenant)

## Application Setup for Pims

Navigate to *Authentication* tab and check *ID tokens (used for implicit and hybrid flows)* checkbox under *Implicit grant and hybrid flows*.

Next, choose single tenant or multitenant access mode under *Supported account types*.

# Setup - Authentication - OpenID Connect - Configuring Azure AD Tenant

The screenshot shows the 'Authentication' configuration page in the Azure AD portal for an application named 'Omega 365 Demo'. The left-hand navigation pane includes sections for Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators | Preview, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area is titled 'Platform configurations' and contains several sections: 'Web' (with a 'Redirect URIs' list containing 'https://demo.omega365.com/login'), 'Front-channel logout URL' (with a text input field containing 'e.g. https://example.com/logout'), 'Implicit grant and hybrid flows' (with a note about token requests and two checkboxes: 'Access tokens (used for implicit flows)' which is unchecked, and 'ID tokens (used for implicit and hybrid flows)' which is checked), and 'Supported account types' (with a note 'Who can use this application or access this API?' and two radio buttons: 'Accounts in this organizational directory only (Omega 365 only - Single tenant)' which is selected, and 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)' which is unselected).

Switch to *API permission tab* and add additional required Microsoft Graph permissions.

- Microsoft Graph - Delegated permissions - openid
- Microsoft Graph - Delegated permissions - email

When delegated permissions are used, users logging in to the application will be presented with a standard permission consent dialog. To ease the login process, tenant's global administrator can consent for the whole organisation by clicking *Grant admin consent for <ORGANISATION>* button. Doing this will bypass permission consent dialog for all users.

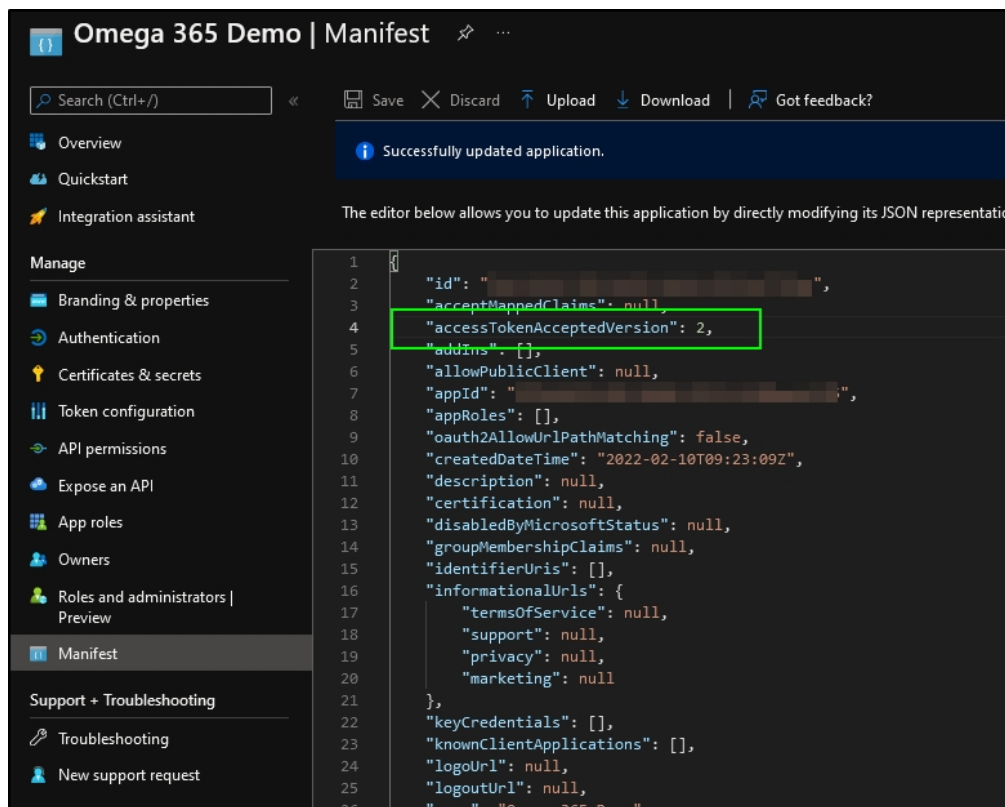
The final API permissions setup should contain permissions displayed in the screenshot below.

The screenshot shows the 'API permissions' configuration page in the Azure AD portal for the same application. The left-hand navigation pane is identical to the previous screenshot, but the 'API permissions' item is now selected. The main content area is titled 'Configured permissions' and includes a note about applications being authorized to call APIs. Below this is a '+ Add a permission' button and a link 'Grant admin consent for Omega 365'. A table lists the configured permissions:

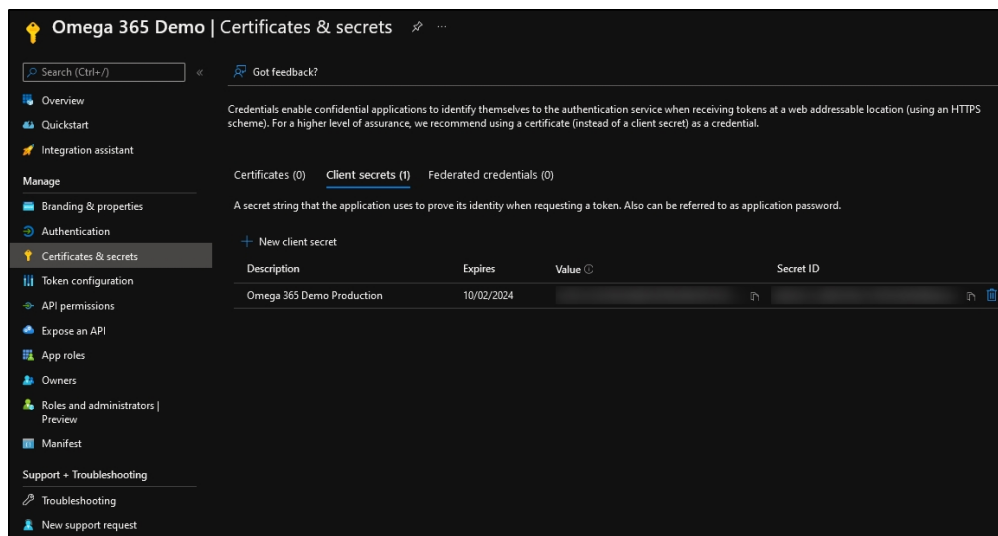
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	...
User.Read	Delegated	Sign in and read user profile	No	...

Below the table, there is a note: 'To view and manage permissions and user consent, try Enterprise applications.'

Set `accessTokenAcceptedVersion` value to `2` the application manifest in *Manifest* tab (default is `null`).

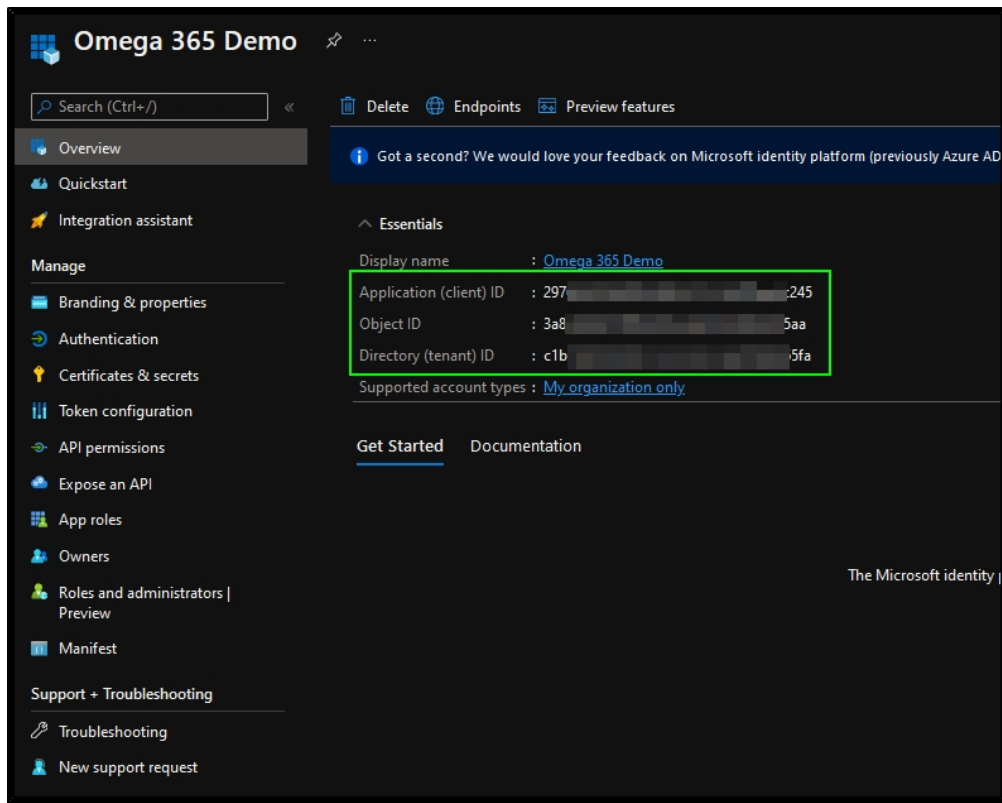


Navigate to *Certificates & secrets* and generate a new secret. Note down the secret value and its expiration. Secret value has to be provided to Omega 365 and the secret has to be renewed after its expiration date.



Finally, return to the *Overview* tab and note down *Application (client) ID* and *Directory (tenant) ID* values.





Once done, provide following to Omega 365:

- Directory (tenant) ID
- Application (client) ID
- Application secret value and its expiration date
- Application access mode (single tenant or multitenant)

# Azure AD Tenant Users Sync Service

21-Mar-2022 | Erikas Seselskis

## Azure AD Users Sync setup

To enable Azure AD users synchronization, following must be done on client's Azure AD Tenant:

- Go to the App registrations tab and click new registration.
- Give the application a name, like Pims Sync. Choose if single tenant

[Home](#) > [Omega AS](#) >

### Register an application

\* Name

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

Pims Mats synd ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Omega AS 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 e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- Go to Api permissions, and click "Add a permission"

# Setup - Authentication - Azure AD Tenant Users Sync Service

Home > Omega AS > Pims Mats sync

Pims Mats sync | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview  
Quickstart  
Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Omega AS

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	-	...


- On the select an api tab, choose "Microsoft Graph"


## Request API permissions


Select an API


Microsoft APIs APIs my organization uses My APIs


Commonly used Microsoft APIs


**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.


**Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios

**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server

**Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

- Choose "application permissions"

## Request API permissions

< All APIs

 Microsoft Graph  
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Your application runs as a background service or daemon without a signed-in user.

- Add the permissions "GroupMember.Read.All" and "User.Read.All", then click add permissions.

## Request API permissions

# SAML 2.0 - Configuring Azure AD Tenant

15-Mar-2022 | Erikas Seselskis

## Configuring SAML 2.0 on Azure AD Tenant

This authentication method uses application in Azure AD tenant to authenticate Omega 365 / Pims solutions users with their organisation's account.


### To register Pims in Azure Active Directory:

Log in to <https://portal.azure.com> and navigate to your Azure Active Directory resource.

- Under "Enterprise applications" section click "New application"
- Then click "Create your own application"
- Type in the name of the application, e.g. Pims, choose "Integrate any other application you don't find in the gallery (Non-gallery)" and click Create:

### 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?

Pims 

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 Azure AD (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

- Click on the Enterprise Application you just created
- Under "Single sign-on" choose "SAML" sign-on method
- Under section "Basic SAML Configuration" click edit button and in the field "Identifier (Entity ID)" provide URL of solution, i.e. <https://pims.pimshosting.com/> ("/" at the end is important), in the field "Reply URL (Assertion Consumer Service URL)" enter URL of solution, appended with "/api/saml2/sp/acs" at the end, i.e. <https://pims.pimshosting.com/api/saml2/sp/acs> and click Save:




## Basic SAML Configuration

 Save |  Got feedback?

Identifier (Entity ID) \* ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default



  ⓘ 

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) \* ⓘ


The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

  ⓘ 

[Add reply URL](#)

Sign on URL (Optional) ⓘ




Relay State (Optional) ⓘ

Logout Url (Optional) ⓘ



- Under "User Attributes & Claims" section click Edit button and change value of "Unique User Identifier (Name ID)" claim to user.mail

### Attributes & Claims ...

[+ Add new claim](#) [+ Add a group claim](#) [≡ Columns](#) |  Got feedback?

Required claim

Claim name	Value	
Unique User Identifier (Name ID)	<div><div>user.mail [nameid-format:emailAddress]</div></div>	...

- Under "SAML Signing Certificate" section download files "Certificate (Base64)" and "Federation Metadata XML". Provide these files to Omega.

## Setup - Authentication - SAML 2.0 - Configuring Azure AD Tenant

- Under section "Users and groups" add users/groups which should have permissions to access Pims.

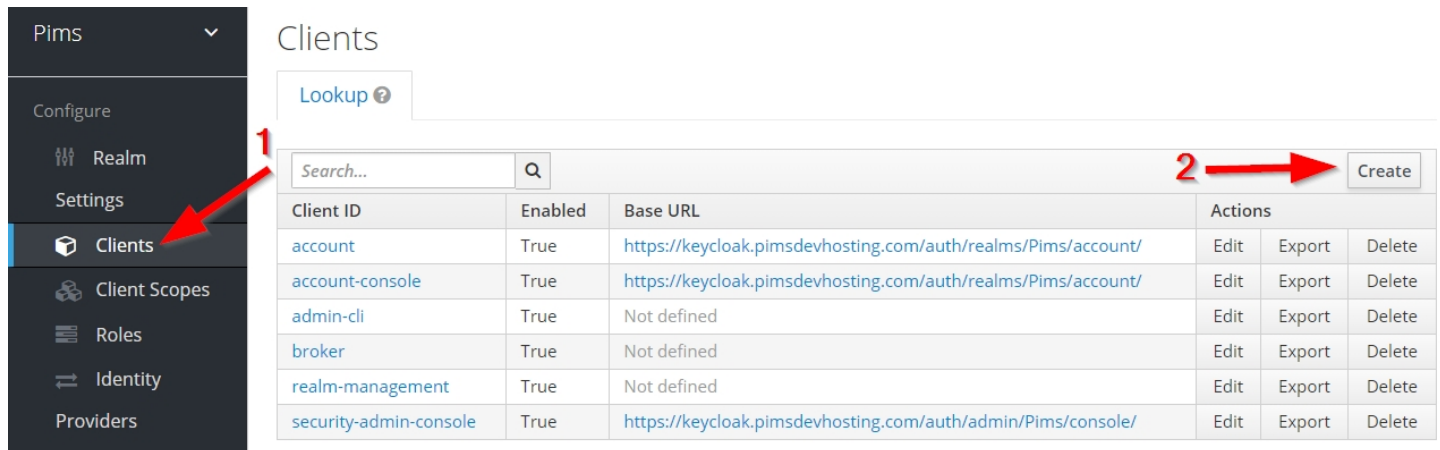
# SAML 2.0 - Configuring Keycloak

19-May-2021 | Erikas Seselskis

## SAML authentication setup with Identity Provider Keycloak

If your organization uses Keycloak Identity Provider (IdP) for user authentication, you can configure Pims to allow your users to log in using their IdP credentials.

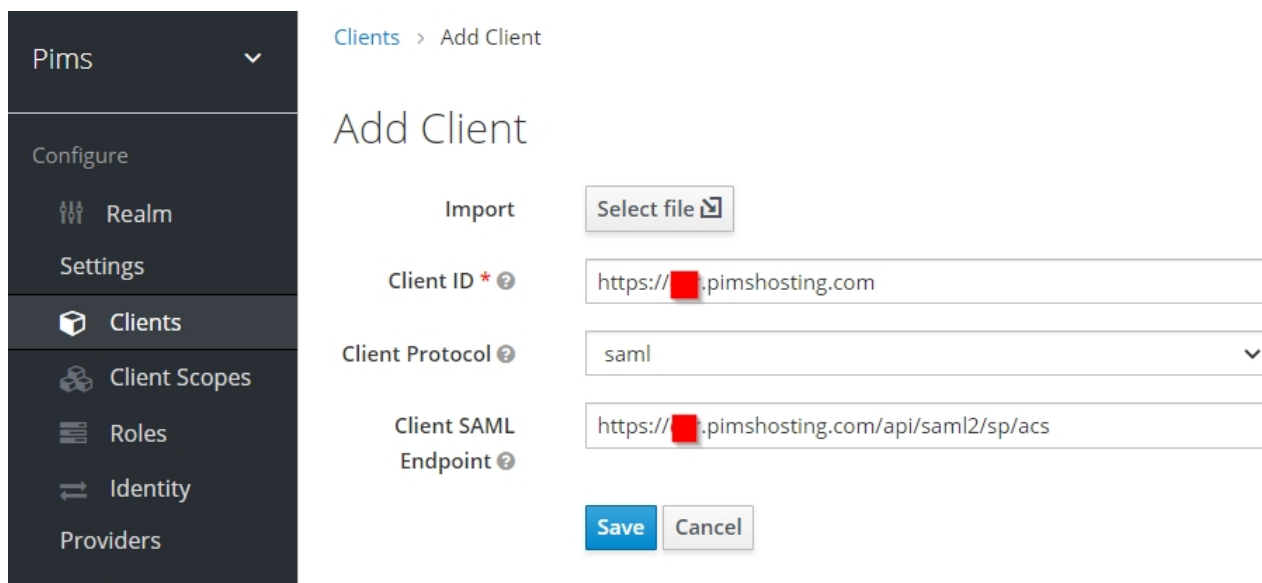
1. Open your Keycloak administration console, choose Realm on which you want to register Pims (by default Master) and click Clients and then "Create":



The screenshot shows the Keycloak administration console. On the left sidebar, the 'Clients' menu item is highlighted with a red arrow labeled '1'. The main area displays the 'Clients' tab with a table of existing clients. A red arrow labeled '2' points to the 'Create' button in the top right corner of the table.

Client ID	Enabled	Base URL	Actions		
account	True	https://keycloak.pimsdevhosting.com/auth/realms/Pims/account/	Edit	Export	Delete
account-console	True	https://keycloak.pimsdevhosting.com/auth/realms/Pims/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	https://keycloak.pimsdevhosting.com/auth/admin/Pims/console/	Edit	Export	Delete

2. In field "Client ID" provide URL of your Pims solution https://<client>.pimshosting.com, under "Client Protocol" choose SAML and in field "Client SAML Endpoint" provide https://<client>.pimshosting.com/api/saml2/sp/acs and click "Save" button:



The screenshot shows the 'Add Client' form in the Keycloak administration console. The 'Client ID' field is filled with 'https://[redacted].pimshosting.com', the 'Client Protocol' is set to 'saml', and the 'Client SAML Endpoint' is filled with 'https://[redacted].pimshosting.com/api/saml2/sp/acs'. The 'Save' button is highlighted.

3. Open created client and set "Sign Assertions" to On, "Client Signature Required" to Off, "Force Name ID Format" to On, "Name ID Format" to "email", "https://<client>.pimshosting.com/api/saml2/sp/acs" as "Valid Redirect URIs" and save it:



## Setup - Authentication - SAML 2.0 - Configuring Keycloak

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

Settings

Roles

Client Scopes ?

Mappers ?

Scope ?

Sessions ?

Offline Access ?

Cluster

Client ID ?

https://[REDACTED].pimshosting.com

Name ?

Description ?

Enabled ?

ON

Always Display in Console ?

OFF

Consent Required ?

OFF

Login Theme ?

Client Protocol ?

saml

Include AuthnStatement ?

ON

Include OneTimeUse Condition ?

OFF

Force Artifact Binding ?

OFF

Sign Documents ?

ON

Optimize REDIRECT signing key lookup ?

OFF

Sign Assertions ?

ON

Signature Algorithm ?

RSA\_SHA256

SAML Signature Key Name ?

KEY\_ID

Canonicalization Method ?

EXCLUSIVE

Encrypt Assertions ?

OFF

Client Signature Required ?

OFF

Force POST Binding ?

ON

Front Channel Logout ?

ON

Force Name ID Format ?

ON

Name ID Format ?

email

Root URL ?

Valid Redirect URIs ?

https://[REDACTED].pimshosting.com/api/saml2/sp/acs

Base URL ?

Master SAML Processing URL ?

https://[REDACTED].pimshosting.com/api/saml2/sp/acs

IDP Initiated SSO URL Name ?

IDP Initiated SSO Relay State ?

4. Copy IdP Metada file and provide it to Omega. IdP Metadata file, can founded by clicking on "Realm Settings" and then on "SAML 2.0 identity Provided Metadata":

## Setup - Authentication - SAML 2.0 - Configuring Keycloak

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity

Providers

User Federation

Authentication

Manage

Groups

Users

General

Login

Keys

Email

Themes

Localization

Cache

Tokens

\* Name

Pims

Display name

HTML Display name

Frontend URL ?

Enabled ?

ON

User-Managed Access ?

OFF

Endpoints ?

OpenID Endpoint Configuration

SAML 2.0 Identity Provider Metadata

Save

Cancel

# SAML 2.0 - Configuring Okta

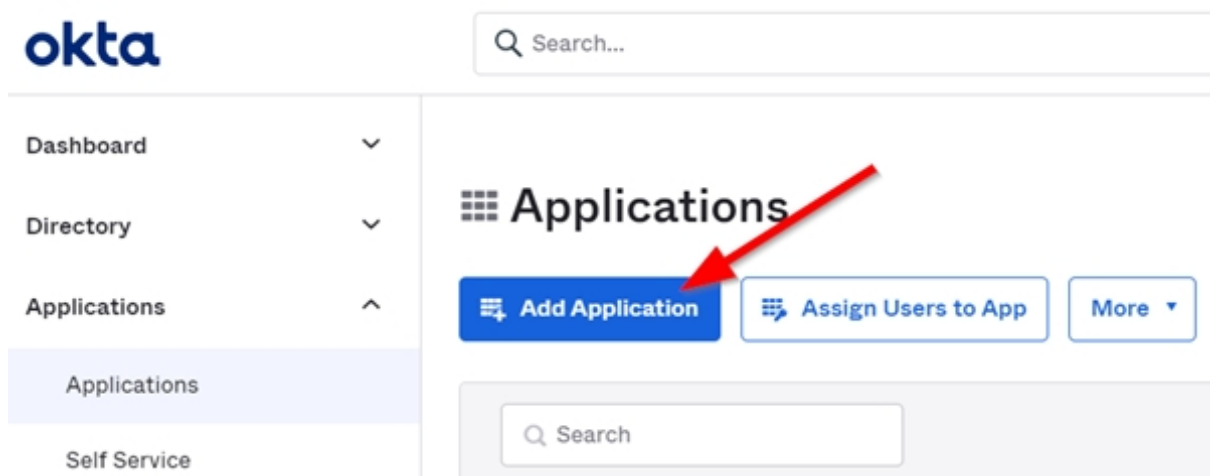
21-Mar-2024 | Author N/A

## SAML authentication setup with Identity Provider Okta

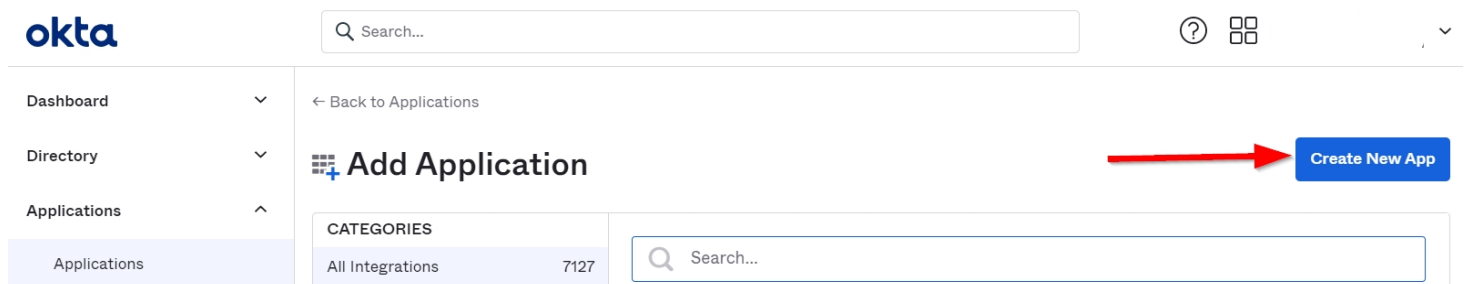
To enable Okta as SAML Identity Provider for Pims, in Okta portal you should add and configure Pims application.

Registering Pims in Okta

Navigate to Applications->Applications and click "Add Application":



Then on the right side click "Create New App":



In popup window choose "Web" as platform and "SAML 2.0" as sign on method and click "Create":

## Create a New Application Integration

Platform

Web

Sign on method



Secure Web Authentication (SWA)

Uses credentials to sign in. This integration works with most apps.



SAML 2.0

Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.



OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.





Create

Cancel

In step "General Settings" of "Create SAML Integration" provide name for the App (i.e. Pims) and click "Next":

## Create SAML Integration

1 General Settings	2 Configure SAML
<div><div>1 General Settings</div><div><div>App name</div><div>Pims</div></div><div><div>App logo (optional) ?</div><div><div></div><div><div></div><div>Browse</div></div><div>Upload Logo</div></div></div><div><div>Requirements</div><ul style="list-style-type: none"><li>• Must be PNG, JPG or GIF</li><li>• Less than 1MB</li></ul><div><b>For Best Results, use a PNG image with</b><ul style="list-style-type: none"><li>• Minimum 420px by 120px to prevent upscaling</li><li>• Landscape orientation</li><li>• Transparent background</li></ul></div></div><div><div>App visibility</div><div><div><input type="checkbox"/> Do not display application icon to users</div><div><input type="checkbox"/> Do not display application icon in the Okta Mobile app</div></div></div><div><div>Cancel</div><div> <div>Next</div></div></div></div>	

In step "Configure SAML" of "Create SAML Integration" provide:

- Single sign on URL: "https://<client>.pimshosting.com/api/saml2/sp/acs"
- Audience URI (SP Entity ID): https://<client>.pimshosting.com
- Name ID format: "EmailAddress"
- Application username: "Email"

Leave default advanced settings and click "Next":

1 General Settings	2 Configure SAML
--------------------	------------------

**A SAML Settings**

**General**

Single sign on URL ?

https://[REDACTED].pimshosting.com/api/saml2/sp/acs

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

https://[REDACTED].pimshosting.com

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

EmailAddress

Application username ?

Email

Update application username on

Create and update

[Show Advanced Settings](#)

In "Feedback step" of "Create SAML Integration" choose "I'm an Okta customer adding an internal app" and click "Finish":


**3 Help Okta Support understand how you configured this application**

Are you a customer or partner?

☒ I'm an Okta customer adding an internal app


☐ I'm a software vendor. I'd like to integrate my app with Okta


Now open "Sign On" tab and click "View Setup Instructions":



# Pims

Active ▾

 View Logs

 Monitor Imports

General

**Sign On**

Import

Assignments

## Settings Edit


### Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ SAML 2.0

Default Relay State





**SAML 2.0** is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.


From the opened window download certificate, copy content of field IDP metadata and provide them to Omega.

To allow users to authenticate against Pims you should add them under Assignments by clicking Assign->Assign to People/Groups:




# CPR

Active ▾

 View Logs ▾

General Sign On Import **Assignments**

Assign ▾

 Convert Assignments

Assign to People

Assign to Groups

Groups