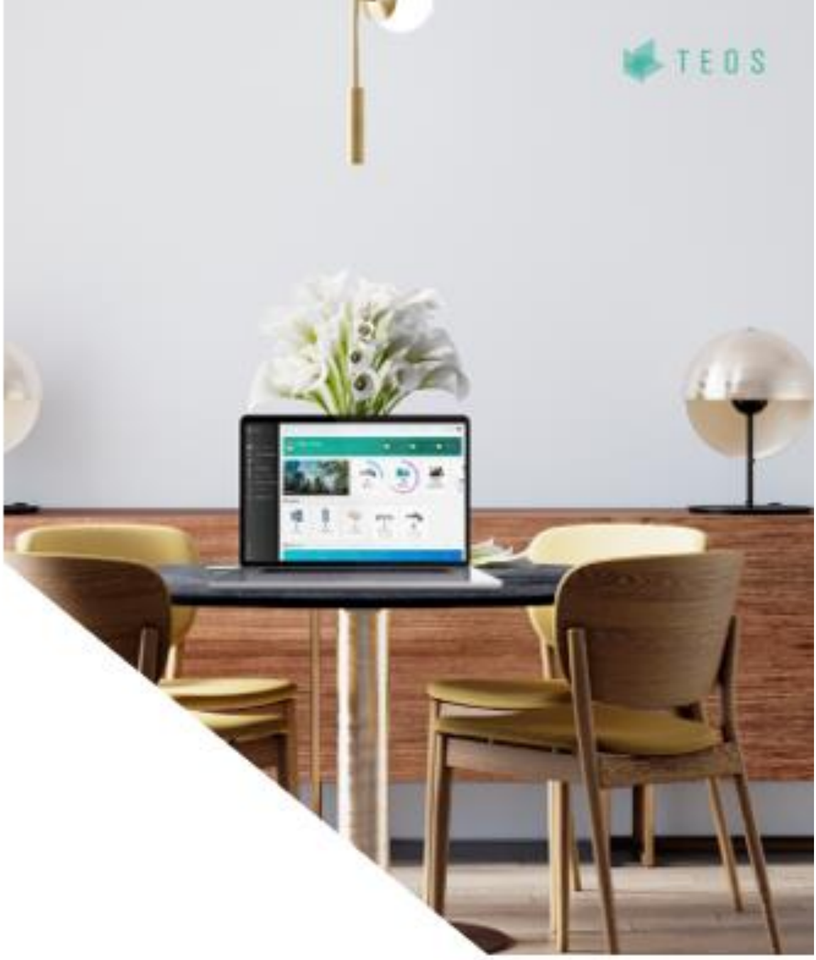
SONY



How to setup Azure AD

Document revision 1.5

Description

Following the standards of IT, TEOS can synchronize with Azure AD (Cloud version of Microsoft Active Directory) and at the same time use the App authentication (GraphAPI) to be able to add room resource without service accounts.

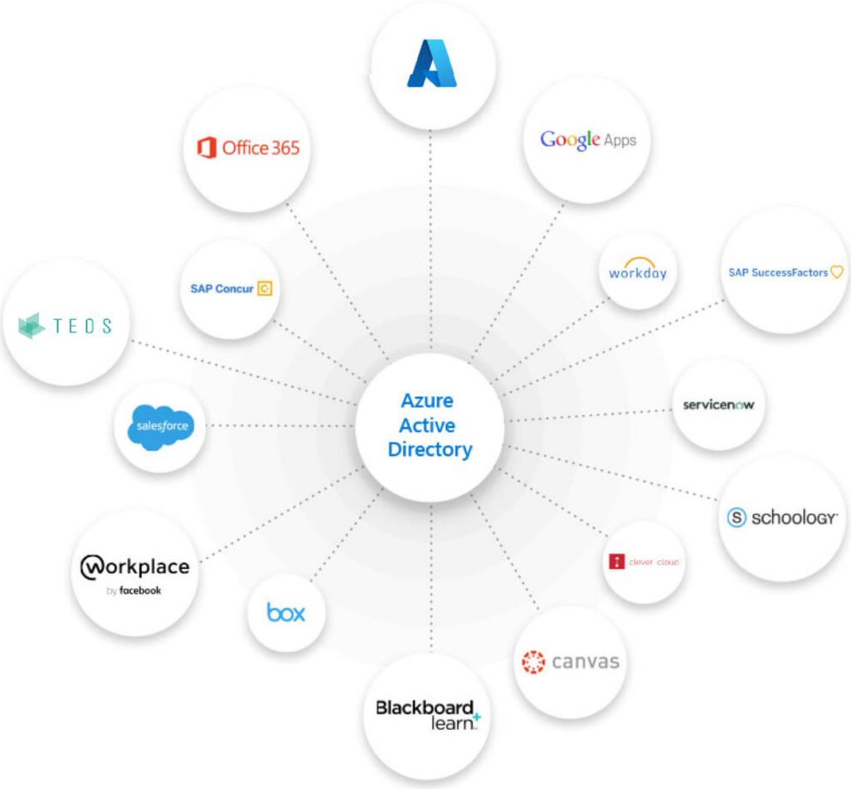
Requirements

- Manage for TEOS server installed (from Version 3.2 at least)
- Manage for TEOS need to access Azure AD
- For MFA support make sure MFA is configured on user level within Azure
- Access to the Manage for TEOS webpage interface with admin rights.
- Domain name of the server cannot be different.

Contents

1. Why synching TEOS with Azure AD

The Azure Active Directory (Azure AD) enterprise identity service provides single sign-on and multi-factor authentication to help protect your users from 99.9 percent of cybersecurity attacks. This platform can be used also for systems synchronizations (such as TEOS) to get the user verification for this single point which is Azure AD. Developer tools make it easy to integrate identity into your apps and services.



What is Azure AD?

Azure Active Directory is Microsoft's multi-tenant, cloud-based identity and access management service. It's the digital infrastructure that allows your employees to sign in and access external resources held in Office 365 and an ever-growing list of other SaaS applications, as well as those held on a corporate network or intranet. Azure AD's strength lies in the flexibility afforded to it by being entirely cloud-based. This means that it can either act as an organisation's only directory, or it can sync with an on-premises directory via Azure AD Connect.

Either way, it enables both on-premises and cloud-based users to access the same apps and resources, simultaneously benefitting from features such as single sign-on (SSO), multi-factor authentication (MFA), conditional access and more.

More importantly, it provides a single place from which to manage your identity, security and compliance controls across your entire IT estate.

What does Azure AD do?

Azure AD provides different benefits depending on what you're using it for.

For IT admins, it allows complete control over access to applications and resources utilising security controls like MFA and conditional access. They can also use Azure AD's built-in governance controls to apply automated lifecycle management and privileged access limitations.

In addition to this, Azure AD also provides admins with the ability to automate provisioning between Windows Server Active Directory and cloud apps like Office 365.

For developers, Azure AD can be used as a standards-based approach to enabling features like SSO and for personalising the app experiences using existing organisation data through APIs.

If you're a user or employee, Azure AD means quick and easy access to work resources, on a multitude of devices, from almost anywhere on the planet.

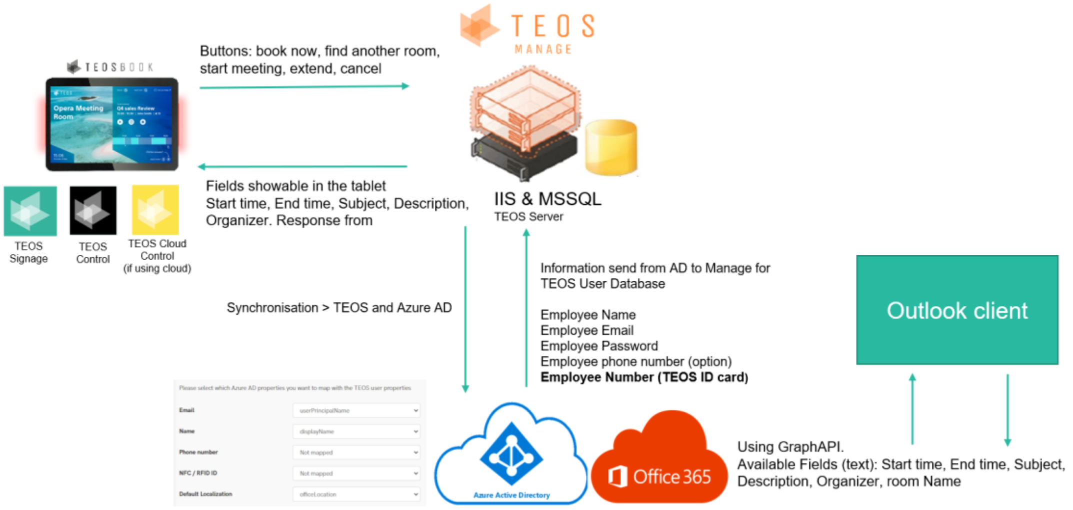
How does it work?

Azure AD, as the name suggests, is a directory – a container for your usernames, credentials and access rights (typically to information-based resources).

Cloud-only or hybrid

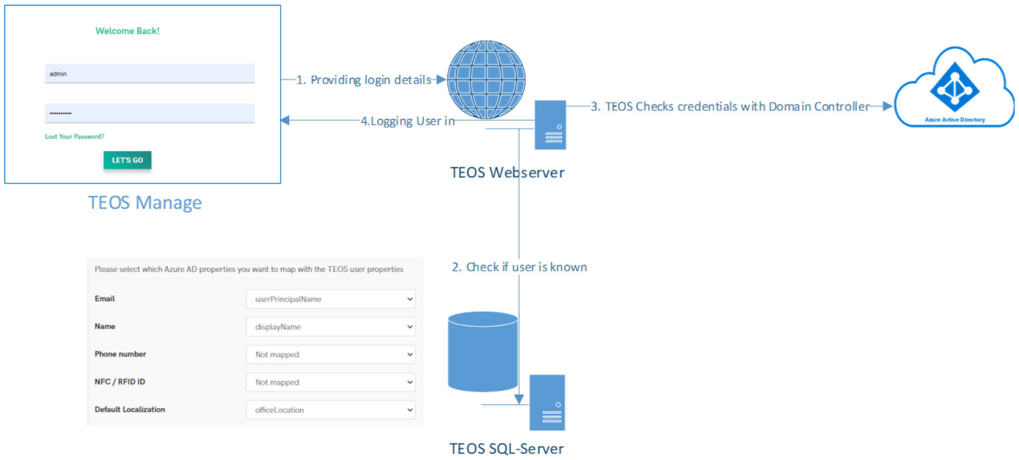
Azure AD can be operated in 'cloud-only' mode, allowing your users to sign into their Windows PCs using the cloud directory service. Alternatively, if you, like many organisations, are still tied to on-premise legacy infrastructure, Azure AD can use your local Active Directory as a master for account data and operate in a variety of hybrid modes.

Azure AD has been designed to enable easy integration with many of today's popular SaaS applications, enabling users to either single sign-on to applications directly or discover and launch them from a portal, such as Office 365 or the Azure AD access panel.


TEOS MANAGE
TEOSBOOK
Opera Meeting Room
Q4 sales Review
Buttons: book now, find another room, start meeting, extend, cancel
Fields showable in the tablet
Start time, End time, Subject, Description, Organizer. Response from
IIS & MSSQL
TEOS Server
TEOS Signage
TEOS Control
TEOS Cloud Control (if using cloud)
Synchronisation > TEOS and Azure AD
Information send from AD to Manage for TEOS User Database
Employee Name
Employee Email
Employee Password
Employee phone number (option)
Employee Number (TEOS ID card)
Outlook client
Azure Active Directory
Office 365
Using GraphAPI.
Available Fields (text): Start time, End time, Subject, Description, Organizer, room Name

Please select which Azure AD properties you want to map with the TEOS user properties

Email	userPrincipalName
Name	displayName
Phone number	Not mapped
NFC / RFID ID	Not mapped
Default Localization	officeLocation



Please select which Azure AD properties you want to map with the TEOS user properties

Email	userPrincipalName
Name	displayName
Phone number	Not mapped
NFC / RFID ID	Not mapped
Default Localization	officeLocation

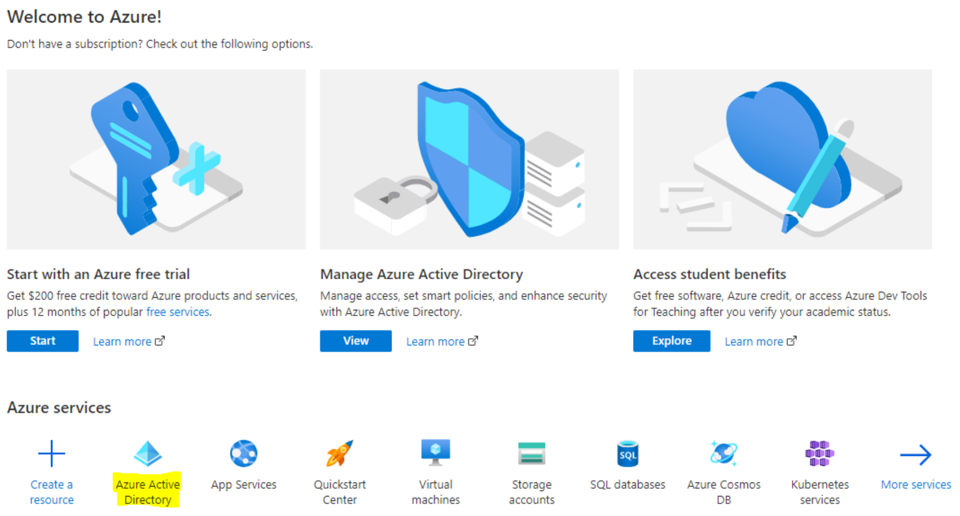
2. Azure AD (for TEOS Cloud or on-premises)

2.1 Configure your Azure Environment

You will need to go to https://portal.azure.com to start the configuration of the TEOS application in your Tenant.

Sign-in with admin rights to be able to create applications and be able to consent permissions.

1) When logged in into azure portal, go to Azure Active Directory



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Start | Learn more

Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

View | Learn more

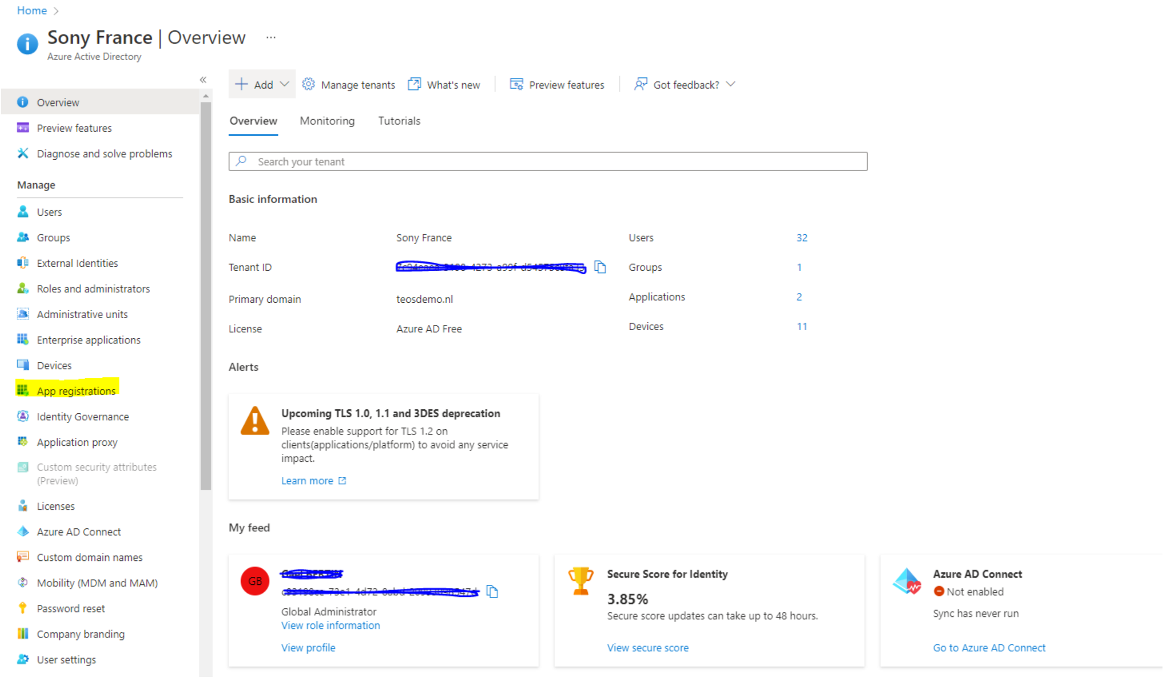
Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

Explore | Learn more

Azure services

2) Go to the left column and click on app registrations to be able to create you TEOS application



Home >

Sony France | Overview ···

Azure Active Directory

Basic information

Name	Sony France	Users	32
Tenant ID	[redacted]	Groups	1
Primary domain	teosdemo.nl	Applications	2
License	Azure AD Free	Devices	11

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation

Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

Learn more

My feed

GB [redacted]

Global Administrator

View role information

View profile

Secure Score for Identity

3.85%

Secure score updates can take up to 48 hours.

View secure score

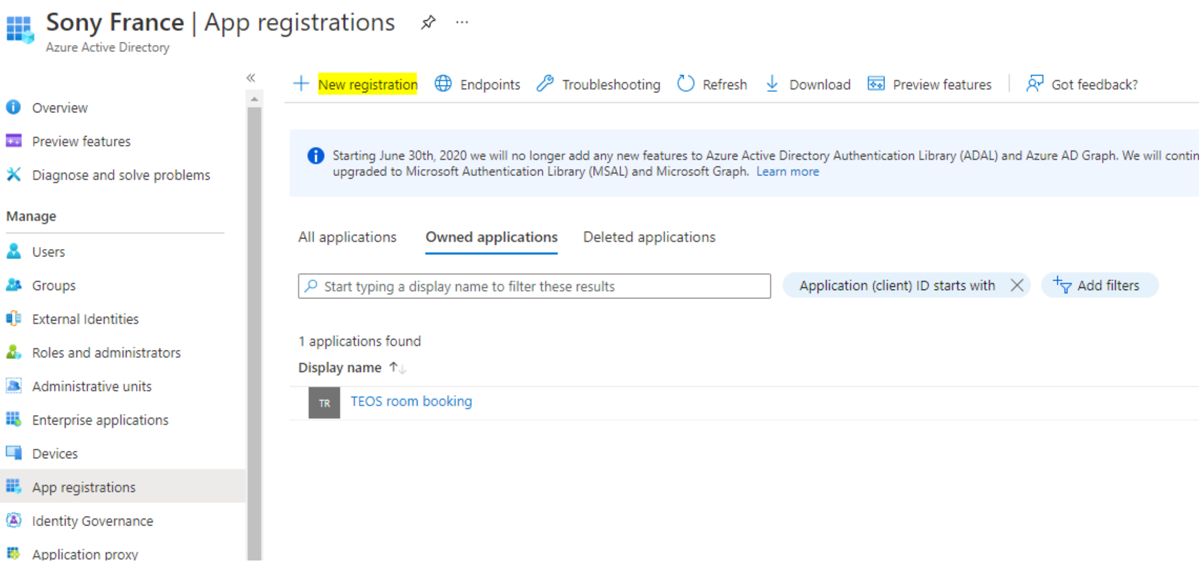
Azure AD Connect

Not enabled

Sync has never run

Go to Azure AD Connect

3) Under app registrations press “New registration” and define a name for the App.



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 contin upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

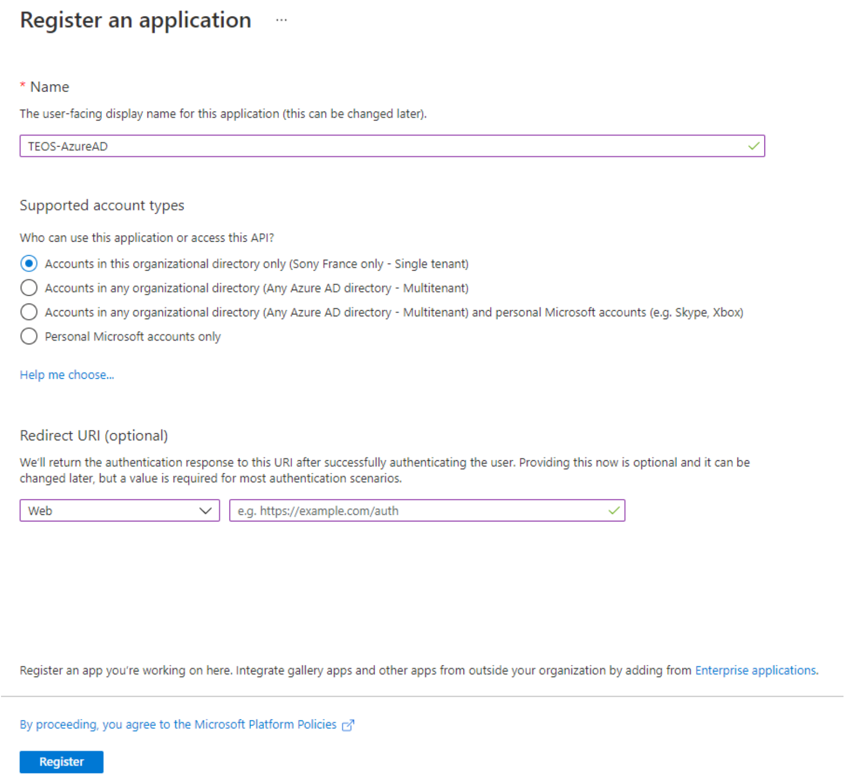
Start typing a display name to filter these results

Application (client) ID starts with

1 applications found

TEOS room booking

4) Define a name that you can easily recognize for a region or a country or where you will use the rooms/users. For Azure AD synchronization only, no need to add a redirect URI, the redirect URI is used mainly for Office365 rooms management and for our TEOS Employee App and Mobile App



* Name

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

TEOS-AzureAD

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Sony France 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)

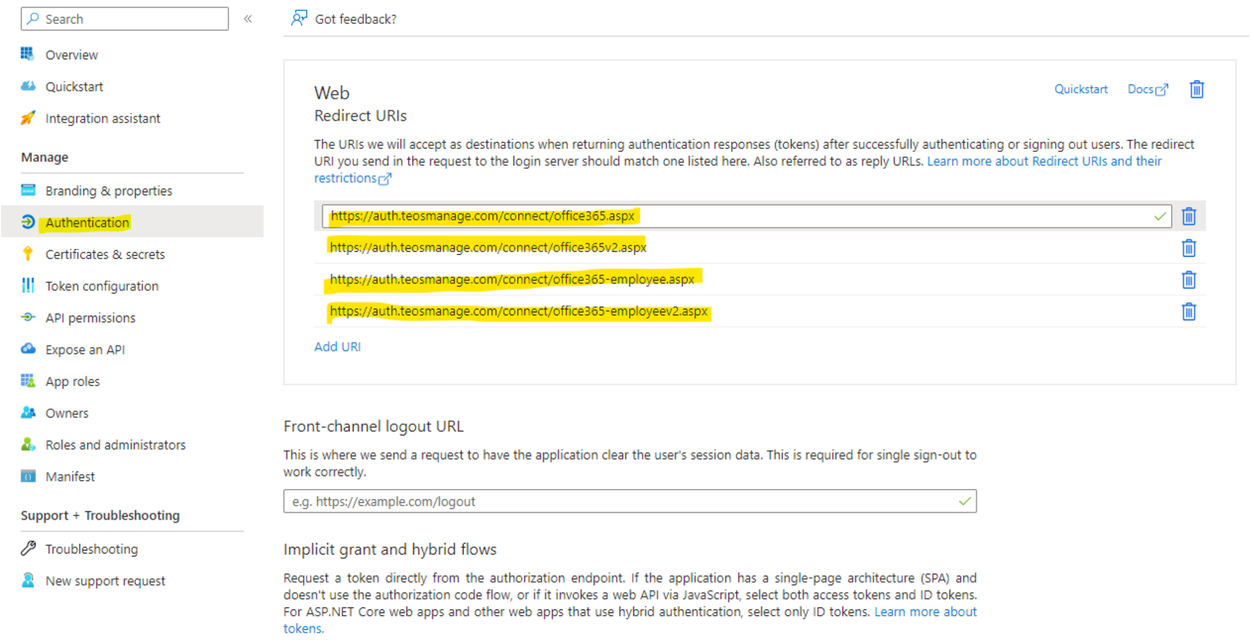
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

URL redirect for TEOS Manage (room booking): https://auth.teosmanage.com/connect/office365.aspx
URL redirect for Employee App: https://auth.teosmanage.com/connect/office365-employee.aspx
URL redirect for TEOS Manage (room booking): https://auth.teosmanage.com/connect/office365v2.aspx
URL redirect for Employee App: https://auth.teosmanage.com/connect/office365-employeev2.aspx
You can go to authentication menu under the left column to review the redirect URIs



Web

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://auth.teosmanage.com/connect/office365.aspx

https://auth.teosmanage.com/connect/office365v2.aspx

https://auth.teosmanage.com/connect/office365-employee.aspx

https://auth.teosmanage.com/connect/office365-employeev2.aspx

Front-channel logout URL

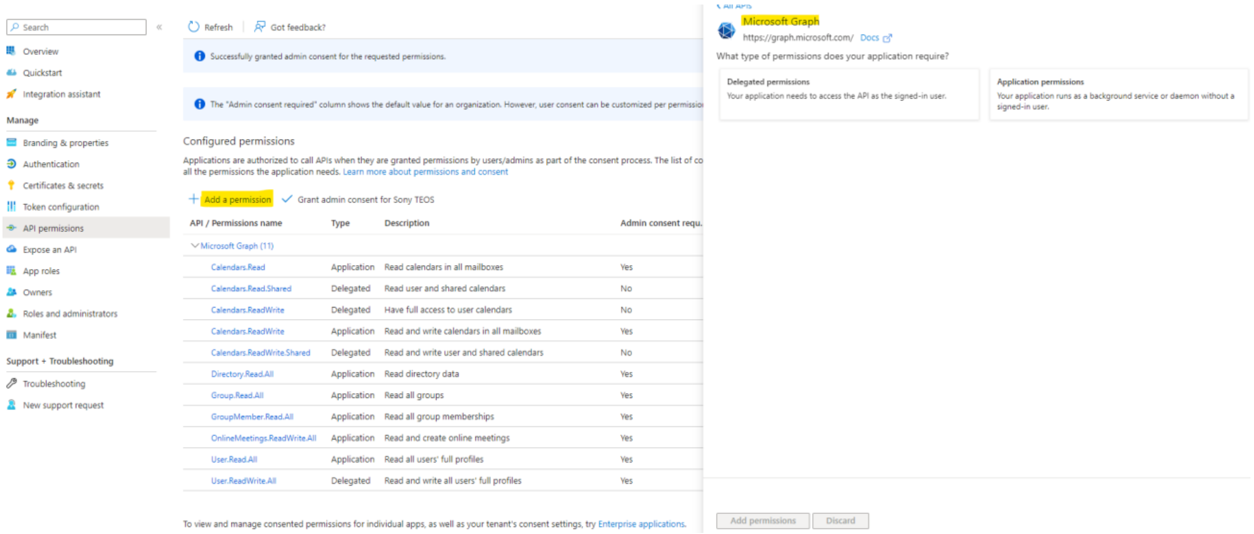
This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

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.

5) When you pressed to register, go then to API permissions, and start to add permissions by pressing “add a permission” and select Microsoft graph



Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permissio

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 co all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ.
Microsoft Graph (11)			
Calendars.Read	Application	Read calendars in all mailboxes	Yes
Calendars.Read.Shared	Delegated	Read user and shared calendars	No
Calendars.ReadWrite	Delegated	Have full access to user calendars	No
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes
Calendars.ReadWrite.Shared	Delegated	Read and write user and shared calendars	No
Directory.Read.All	Application	Read directory data	Yes
Group.Read.All	Application	Read all groups	Yes
GroupMember.Read.All	Application	Read all group memberships	Yes
OnlineMeetings.ReadWrite.All	Application	Read and create online meetings	Yes
User.Read.All	Application	Read all users' full profiles	Yes
User.ReadWrite.All	Delegated	Read and write all users' full profiles	Yes

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Microsoft Graph

https://graph.microsoft.com/

What type of permissions does your application require?

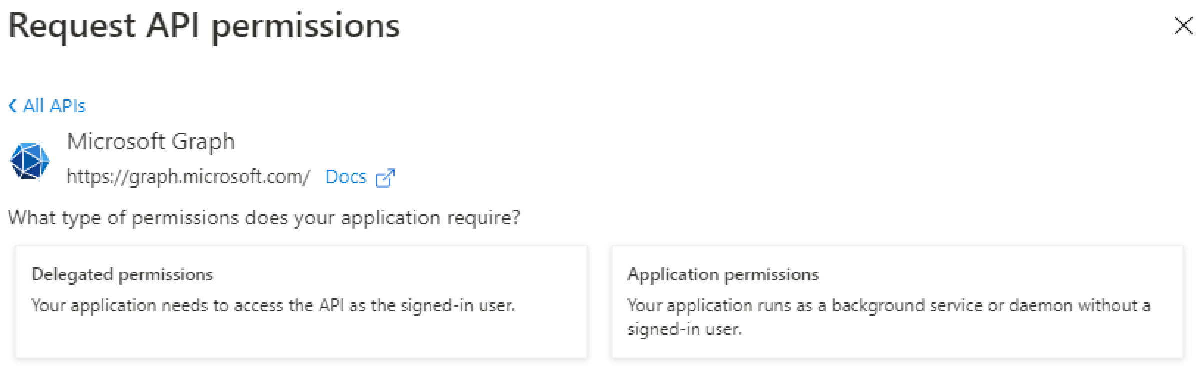
Delegated permissions

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.

Select if your permission is an application type permission or a delegated permission (in Azure AD it is only Application permissions)



Request API permissions

Microsoft Graph

https://graph.microsoft.com/

What type of permissions does your application require?

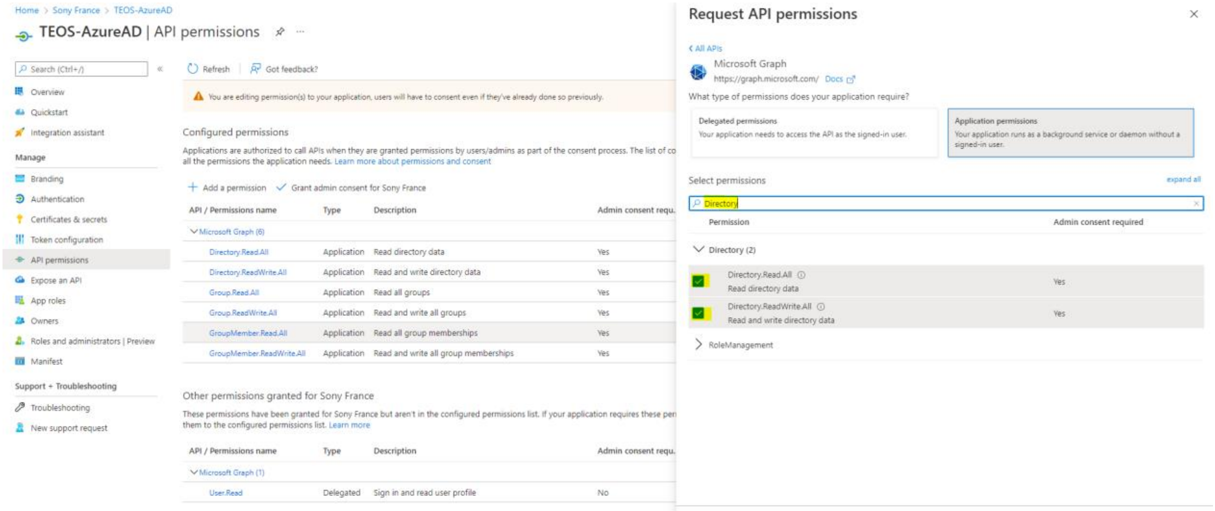
Delegated permissions

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.

You can then search by the name of the requested permission and select the checkbox to add it



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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 co all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ.
Microsoft Graph (6)			
Directory.Read.All	Application	Read directory data	Yes
Directory.ReadWrite.All	Application	Read and write directory data	Yes
Group.Read.All	Application	Read all groups	Yes
Group.ReadWrite.All	Application	Read and write all groups	Yes
GroupMember.Read.All	Application	Read all group memberships	Yes
GroupMember.ReadWrite.All	Application	Read and write all group memberships	Yes

Other permissions granted for Sony France

These permissions have been granted for Sony France but aren't in the configured permissions list. If your application requires these per them to the configured permissions list. Learn more

API / Permissions name	Type	Description	Admin consent requ.
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

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.

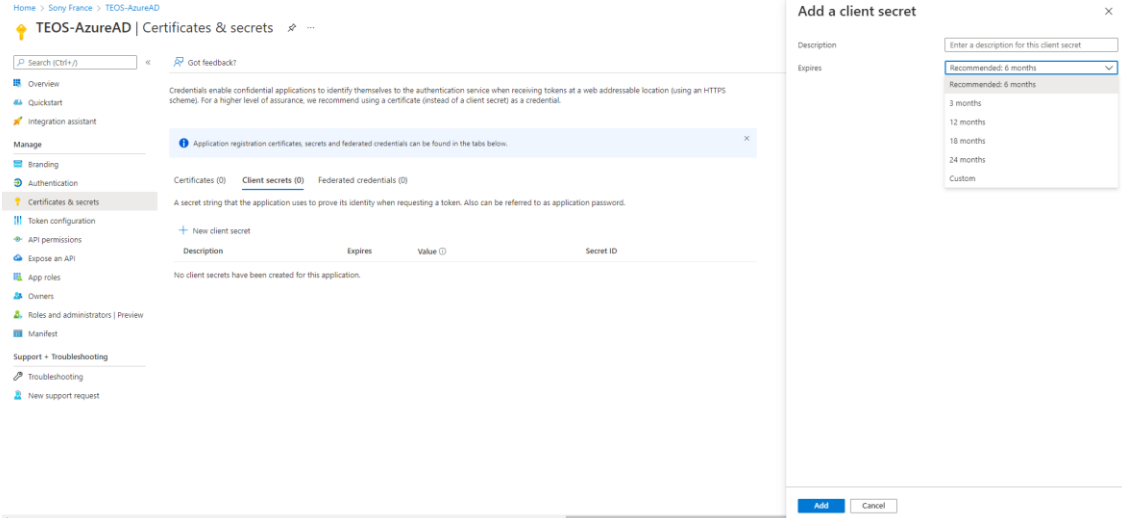
Select permissions — expand all

Directory

	Permission	Admin consent required
	Directory (2)	
☑	Directory.Read.All Read directory data	Yes
☑	Directory.ReadWrite.All Read and write directory data	Yes
	RoleManagement	

You can refer to section 2.2 and 2.3 to check what are the permissions needed.

6) After adding all the permission, you need to get a Client Secret that we will used by TEOS together with the Tenant ID and Client ID to be able to get the data. For that go to “Certificates & secrets” which on the left column. You can define under this section the expiration tie for the Client Secret (maximum 2 years). Copy then the value generated.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

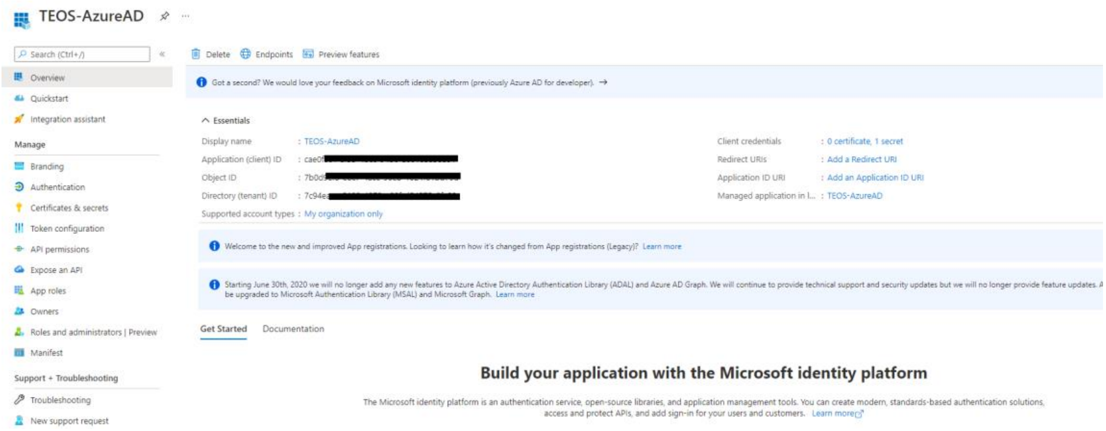
Add a client secret

Description: Enter a description for this client secret

Expires: Recommended: 6 months

- Recommended: 6 months
- 3 months
- 12 months
- 18 months
- 24 months
- Custom

7) You can you then to your overview the find again the Client ID, Tenant ID on top of the Client Secret (value).



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: TEOS-AzureAD	Client credentials	: 0 certificate, 1 secret
Application (client) ID	: cae0[redacted]	Redirect URIs	: Add a Redirect URI
Object ID	: 7b0d[redacted]	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 7c94e[redacted]	Managed application in l...	: TEOS-AzureAD
Supported account types	: My organization only		

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

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. A be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

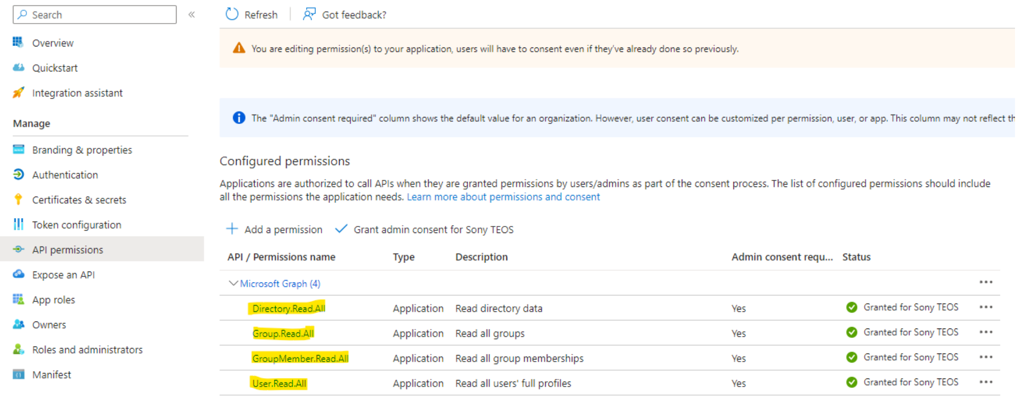
Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

2.2 Permissions needed for Azure Active Directory

To get TEOS working with Azure AD you will need the following permissions:

Permission name	Type	Description
Directory.Read.All	Application	Allows the app to read data in your organization's directory.
Group.Read.All	Application	Allows the app to list groups, and to read their properties and all group memberships on your behalf. Also allows the app to read calendar, conversations, files, and other group content for all groups you can access.
GroupMember.Read.All	Application	Allows the app to list groups, read basic group properties and read membership of all your groups.
User.read.All	Application	Sign in and read user profile



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect th

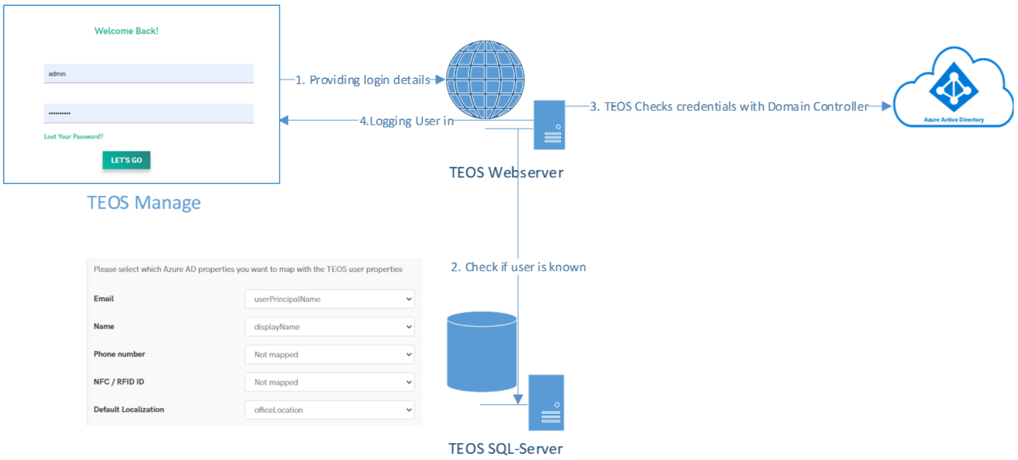
Configured permissions

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 Sony TEOS

API / Permissions name	Type	Description	Admin consent requ...	Status	
∨ Microsoft Graph (4)					···
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Sony TEOS	···
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Sony TEOS	···
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for Sony TEOS	···
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Sony TEOS	···

With those permissions, TEOS (when configured) will be able to get the user emails and names as minimum from user accounts and will be able when password verification is needed to verify against Azure AD if the user exists and if his password or Card ID is correct.



Please select which Azure AD properties you want to map with the TEOS user properties

Email	userPrincipalName
Name	displayName
Phone number	Not mapped
NFC / RFID ID	Not mapped
Default Localization	officeLocation

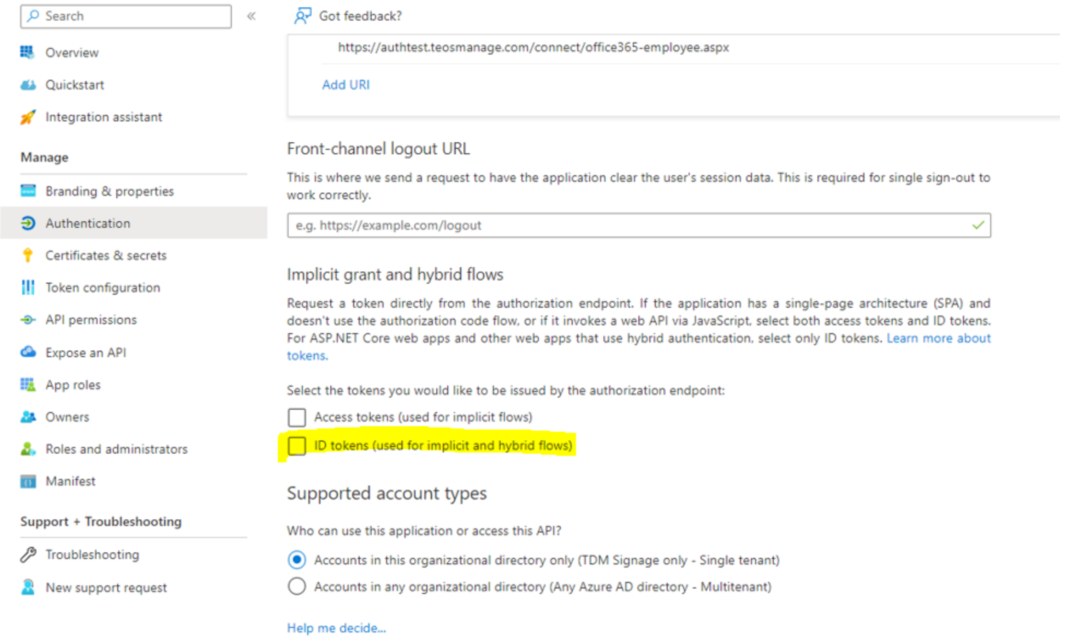
2.3 Configuration for MFA support with TEOS

For a user to login not only with Azure AD account but also using MFA, a configuration need to be done in Azure and points need to be verified:

1) Make sure the configuration of the application with the permissions requested in point 2.2 are applied

2) Under authentication, add a new redirect URL with https://tenantname.teoscloud.com/Account/LoginOpenId (make sure you put your tenant name for CLOUD and on premise just replace the tenantname.teoscloud.com by your server name).

3) On top of the redirect URL to add under authentication, enable the option “ID tokens (used for implicit and hybrid flows)”



https://authtest.teosmanage.com/connect/office365-employee.aspx

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)

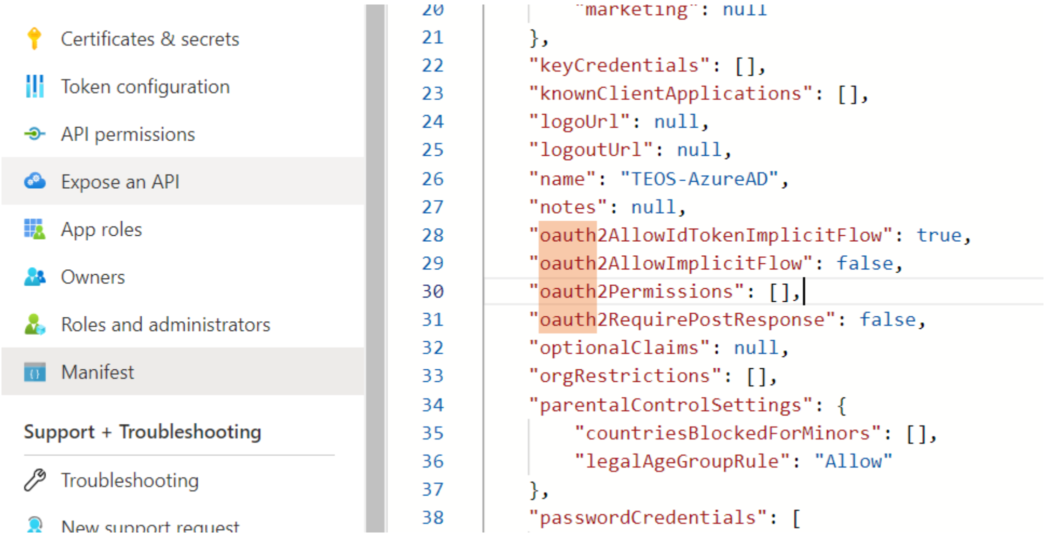
Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (TDM Signage only - Single tenant)

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

4) Under the application manifest tab, please ensure that oauth2 configuration is as configured below:



```
    "marketing": null
},
"keyCredentials": [],
"knownClientApplications": [],
"logoUrl": null,
"logoutUrl": null,
"name": "TEOS-AzureAD",
"notes": null,
"oauth2AllowIdTokenImplicitFlow": true,
"oauth2AllowImplicitFlow": false,
"oauth2Permissions": [],
"oauth2RequirePostResponse": false,
"optionalClaims": null,
"orgRestrictions": [],
"parentalControlSettings": {
    "countriesBlockedForMinors": [],
    "legalAgeGroupRule": "Allow"
},
"passwordCredentials": [
```

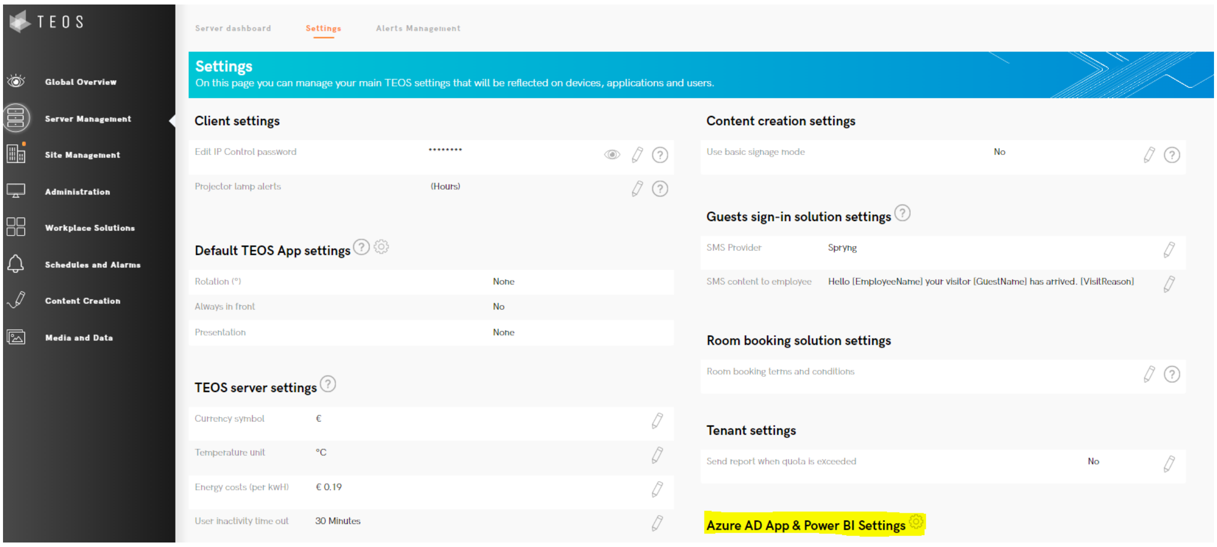
2.4 Sync TEOS with Azure AD User and App

Make sure TEOS Manage server can reach the following URLs in internet (port 443):

- Portal.azure.com
- outlook.office365.com
- login.microsoftonline.com
- Auth.teosmanage.com
- Graph.microsoft.com

You can do a telnet to the following URL to make sure they are accessible and open from the firewall.

Go to server management > settings and Azure AD App & Power BI



Settings

On this page you can manage your main TEOS settings that will be reflected on devices, applications and users.

Client settings

Edit IP Control password ********

Projector lamp alerts (Hours)

Default TEOS App settings

Rotation (°) None

Always in front No

Presentation None

TEOS server settings

Currency symbol €

Temperature unit °C

Energy costs (per kwH) € 0.19

User inactivity time out 30 Minutes

Content creation settings

Use basic signage mode No

Guests sign-in solution settings

SMS Provider Spryng

SMS content to employee Hello [EmployeeName] your visitor [GuestName] has arrived. [VisitReason]

Room booking solution settings

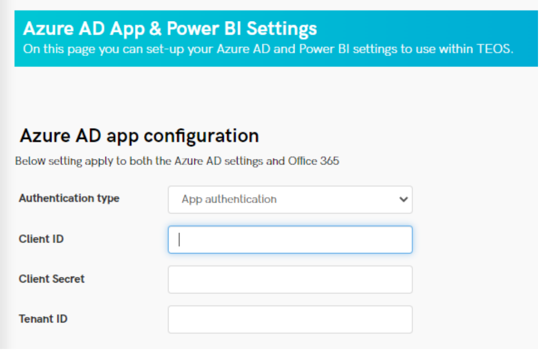
Room booking terms and conditions

Tenant settings

Send report when quota is exceeded No

Azure AD App & Power BI Settings

For the app usage, select under authentication “App Authentication”. Insert then the Client ID, Tenant ID and secret code value of the third-party account you created for TEOS.



Azure AD App & Power BI Settings

On this page you can set-up your Azure AD and Power BI settings to use within TEOS.

Azure AD app configuration

Below setting apply to both the Azure AD settings and Office 365

Authentication type: App authentication

Client ID

Client Secret

Tenant ID

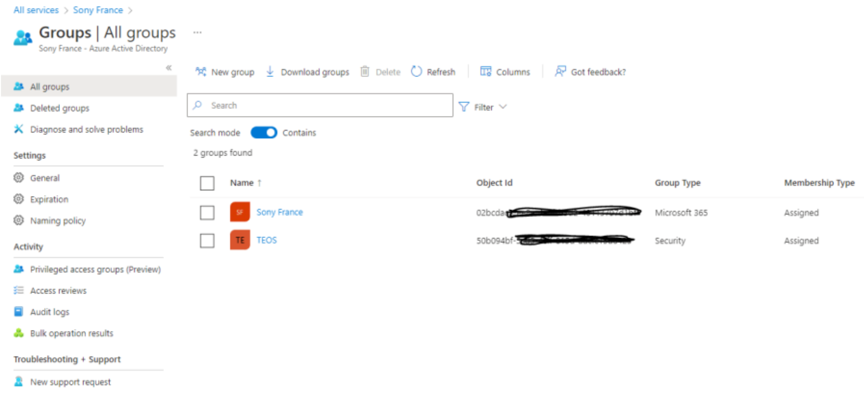
If you get an error in the synchronization, please go to your folders C:\\TEOS Manage > www > Backbone > web.config and make sure you have the correct url.

```
<add key="AllowSocialMediaDomain" value="https://auth.teosmanage.com" />
```

2.5 Add users from Azure AD to TEOS

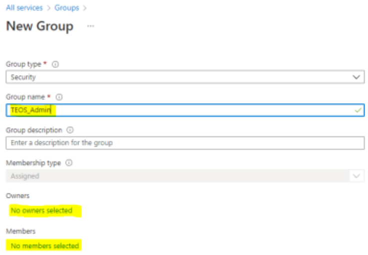
2.5.1 Configuration in Azure AD

Go to Azure AD and Groups, you can create a new group which will get the role defined in TEOS (for example a group which will be administrator, another one which can be dedicated for content creation or even for resources right accesses)



2 groups found

Name ↑	Object Id	Group Type	Membership Type
Sony France	02bcda[redacted]	Microsoft 365	Assigned
TEOS	50b094bf-[redacted]	Security	Assigned



Group type * : Security

Group name * : TEOS_Admin

Group description : Enter a description for the group

Membership type : Assigned

Owners : No owners selected

Members : No members selected

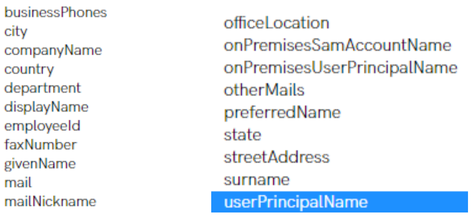
When the group is created click on “no members selected” for you to be able to add users to the group

2.5.2 Configuration in TEOS

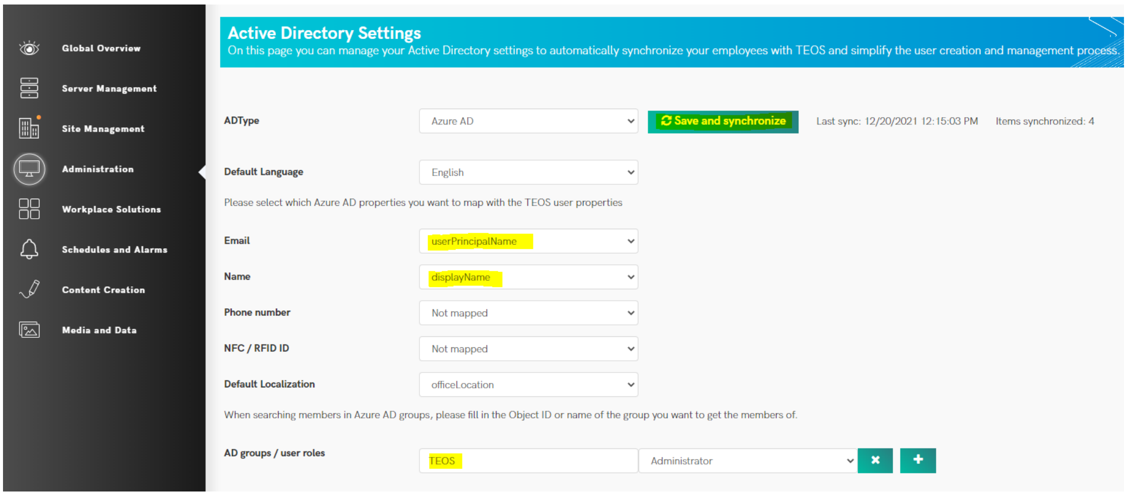
Go to Administration > Active Directory Settings

Select the AD Type to Azure AD. Select then the default language. You can then select the field that TEOS will be able to save in his database from user profiles.

The required ones are Email and name, the other properties are optional depending on your usage (phone number, NFC/RFID ID, Default Localization). You can map the following properties to the TEOS user properties.


businessPhones
city
companyName
country
department
displayName
employeeId
faxNumber
givenName
mail
mailNickname
officeLocation
onPremisesSamAccountName
onPremisesUserPrincipalName
otherMails
preferredName
state
streetAddress
surname
userPrincipalName

You can finalize by linking the user group with TEOS to define the different roles, click save and synchronize to get the configuration done.



Active Directory Settings

On this page you can manage your Active Directory settings to automatically synchronize your employees with TEOS and simplify the user creation and management process.

ADType: Azure AD

Last sync: 12/20/2021 12:15:03 PM Items synchronized: 4

Default Language: English

Please select which Azure AD properties you want to map with the TEOS user properties

Email: userPrincipalName

Name: displayName

Phone number: Not mapped

NFC / RFID ID: Not mapped

Default Localization: officeLocation

When searching members in Azure AD groups, please fill in the Object ID or name of the group you want to get the members of.

AD groups / user roles: TEOS Administrator ✖ ✚

You can go then go to Administration > Users and you will see your synchronized users.

2.6 Recap of all premissions which can be required for TEOS

Permission name (Graph API)	Type	Description
Calendars.Read	Application	For Booking panels: read/display the booking into the booking panel
Calendars.ReadWrite	Application	For Booking panels: allow the booking from the booking panel on the room resource calendar
User.read.all	Application	For Booking panels: Required to localize the email address of the room calendar resources into TEOS
Calendars.ReadWrite	Delegated	For the user booking App: In order to be able from the web application/ mobile application of TEOS, user will need to login with his O365 calendar account in the web application and mobile in order to see his spaces booking done in outlook into the applications. This application is focusing into the space using together with O365 booking style
Calendars.ReadWrite.Shared	Delegated	For the user booking Application and web portal, the application needs to be able to get room calendars information's in order to filter accordingly the availabilities to the user application
User.readwrite.all	Delegated	For the user booking Application and web application, this permission will allow the user to login within the application only and allow him also to write on his O365 calendar using his user name. No other usage is done with this permission
Directory.read.all	Application	Tool User management: For the possibility to synchronize users with the tool and reading the Group ID/ Group name identified in the tool. This to automatically define the groups of users who will use the tool and to use the Azure AD authentication
Group.read.all	Application	Tool User management: For the possibility to synchronize users with the tool and reading the Group ID/ Group name identified in the tool. This to automatically define the groups of users who will use the tool and to use the Azure AD authentication
GroupMember.read.all	Application	Tool User management: For the possibility to synchronize users with the tool and reading the Group ID/ Group name identified in the tool. This to automatically define the groups of users who will use the tool and to use the Azure AD authentication
User.read.all	Application	Tool User management: For the possibility to synchronize users with the tool and reading the Group ID/ Group name identified in the tool. This to automatically define the groups of users who will use the tool and to use the Azure AD authentication

Visit us on

https://teos.solutions