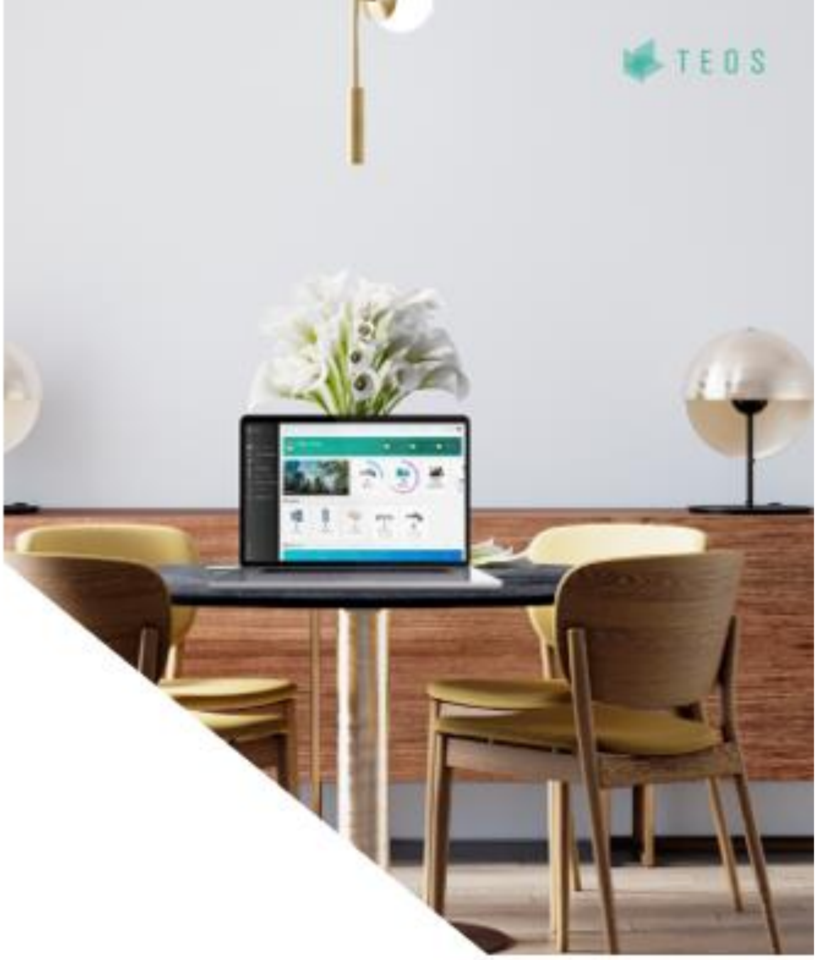


How to setup Single Sign On (SSO)

Document revision 1.2

Description

Following the standards of IT, TEOS support the Single Sign On SSO configuration using OpenID using OIDC, to be able to have Single Sign On using a lot of Identity platform such as Microsoft Entra ID.

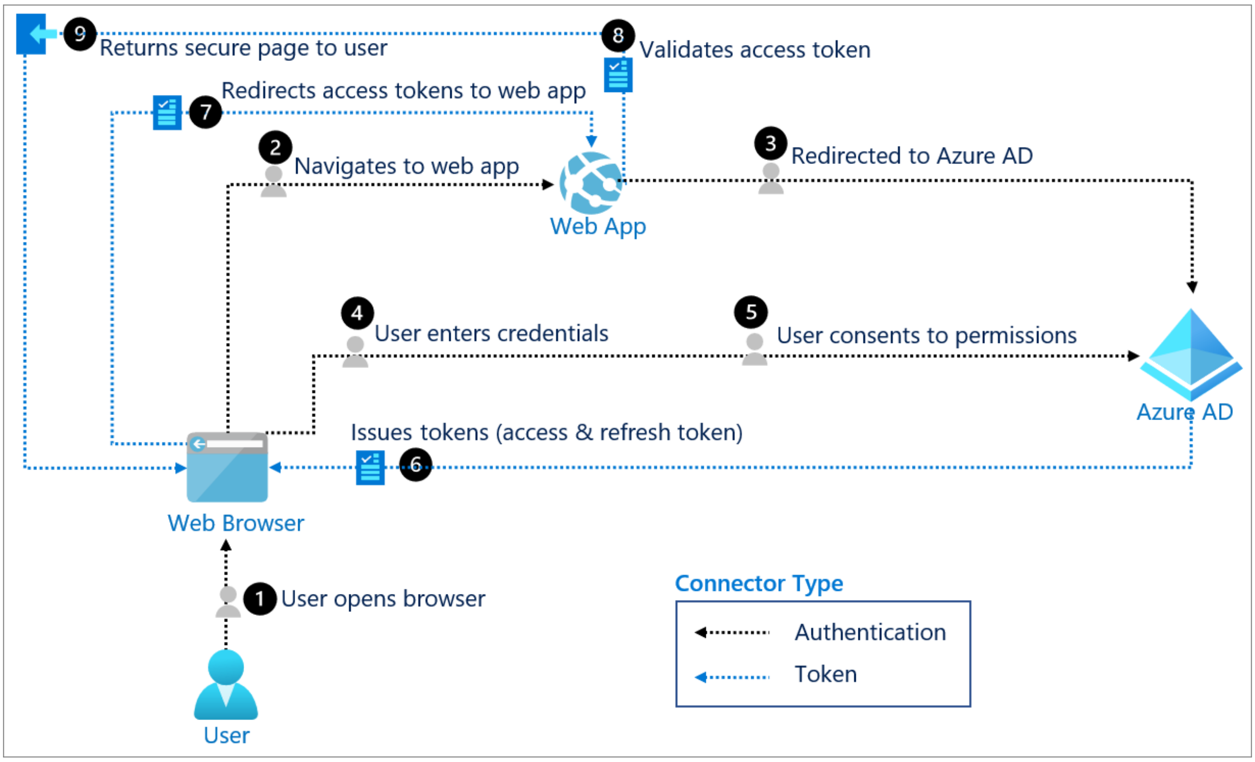
Requirements

- Manage for TEOS server installed (from Version 3.3 at least)
- Manage for TEOS need to access Azure AD
- Access to the Manage for TEOS webpage interface with admin rights.
- A default URL access to skip SSO has been created to use the Admin/support access: https://tenantname.teoscloud.com/Account/SkipSsoLogin (only for the admin panel access not for the employee app)
- Make sure TEOS Manage server can reach the needed URLs in internet (port 443)

Contents

1. What is OpenID Connect SSO

OpenID connect is a protocol designed for user authentication. OpenID connect is a standard added on the top of Oauth 2.0 (Authorization Protocol) framework which adds ID Token to the access token in OAuth 2.0. OAuth and OpenID both act as Single Sign-On (SSO) standards. OpenID Connect must be in JWT(JSON) data format. One of the Key factors about OpenID Connect is the ability to exchange and make use of information.


9 Returns secure page to user
8 Validates access token
7 Redirects access tokens to web app
2 Navigates to web app
3 Redirected to Azure AD
Web App
4 User enters credentials
5 User consents to permissions
Azure AD
Issues tokens (access & refresh token) 6
Web Browser
1 User opens browser
User
Connector Type
Authentication
Token

Why OpenID Connect?

As we know that Open ID connect is an identity layer for authentication purpose above OAUTH2.0 framework, which is used for authorization, but back in the day OAUTH 2.0 was misused for pseudo authentication and as a result Open ID Connect entered the picture.

How OpenID Connect SSO Works?

OpenId connect is the Identity layer over the Base OAuth 2.0 Protocol. Identity is nothing but the Set of Attributes related to the Users. OpenID connect Identify the users with Specific Attributes sent by IdPs like Email. This Information is passed through the ID token and Signed with IETF JSON Web Signature. Another case of OpenID SSO is Azure acting as an IdP, to login into the OpenID connect application like native mobile applications running on Android and iOS, webapps OpenID Connect will redirect a user to an identity provider (IdP) to check the user's identity, either by looking for an active session i.e Single Sign-On (SSO) or by asking the user to authenticate. Once the IdP authenticates the user with SSO Session or valid Credentials and authorizes them to access a specific application, the IdP redirects back to that application. This redirection also passes information about the user back to the app confirming the user's identity and that it can use to.

Applications of OpenID Connect

Identity Providers like Google, Twitter, Facebook use this so that users can login in to the Identity Provider, and then access other apps and websites without having to sign in or share their login information. Native Single Sign-On is enabled by OpenID Connect. As the popularity of native applications grows due to their ease of use and distribution, there is a greater demand for default OAuth 2.0 in native environments.

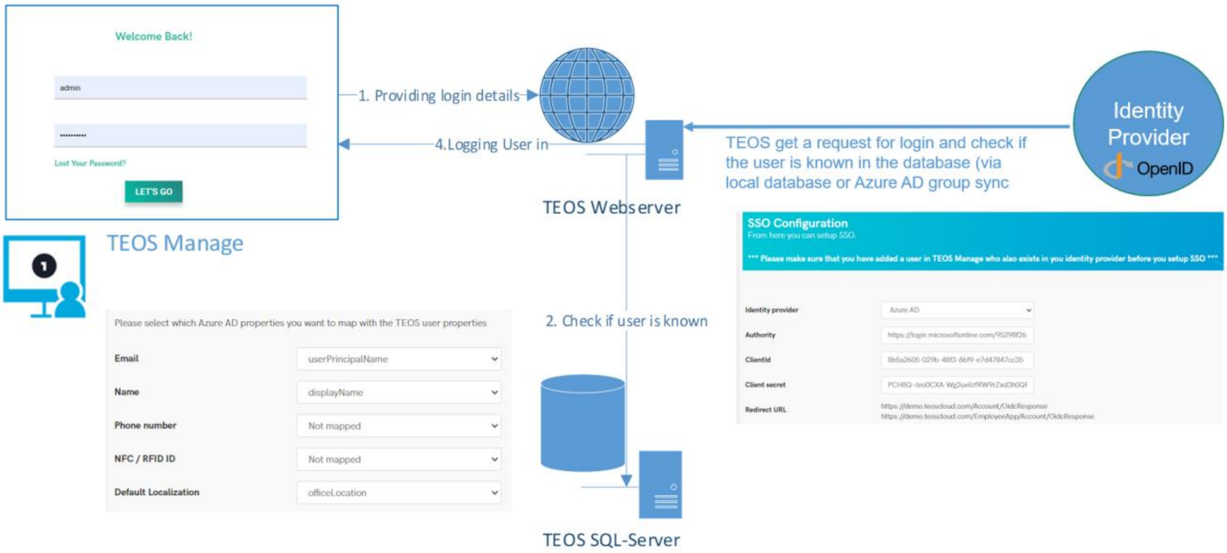
However, the burden of managing authentication across a sea of different native apps falls on the end user, who must know which login is for which app and which must be re-authenticated.

How does it work for TEOS?

Single Sign On with TEOS will allow user to login directly with his user rights access without having to login into the platform but login into his Windows Session or into the Identity Provider which will trust the authentication for TEOS using OIDC protocol and OpenID.

The user email address must be at least identified in TEOS Server having is field manually or using Azure AD. Azure AD, as the name suggests, is a directory – a container for your usernames, credentials, and access rights (typically to information-based resources).

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.


Welcome Back!
Lost Your Password?
LET'S GO
1. Providing login details
4.Logging User in
TEOS Webserver
Identity Provider
OpenID
TEOS get a request for login and check if the user is known in the database (via local database or Azure AD group sync
TEOS Manage
2. Check if user is known
TEOS SQL-Server

admin

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

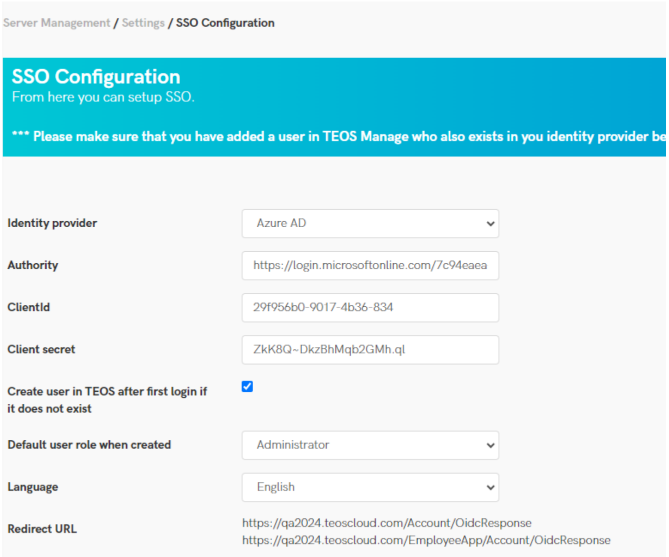
SSO Configuration
From here you can setup SSO.

*** Please make sure that you have added a user in TEOS Manage who also exists in you identity provider before you setup SSO ***

Identity provider	Azure AD
Authority	https://login.microsoftonline.com/95298f26
ClientId	8b6a2605-029b-48f3-86f9-e7d47847cc35
Client secret	PCH8Q~Ieo0CXA-Wg2uvilzfRW9rZxd3h0QF
Redirect URL	https://demo.teoscloud.com/Account/OidcResponse https://demo.teoscloud.com/EmployeeApp/Account/OidcResponse

2. Enable user auto-registration

When configuring SSO within TEOS within Server management > Settings > SSO Configuration, it is possible enable the option to automatically create a user with a default user role (which include a localization access) and a default language. This makes transparent the login and access for users for example using the employee application



Server Management / Settings / SSO Configuration

SSO Configuration
From here you can setup SSO.

*** Please make sure that you have added a user in TEOS Manage who also exists in you identity provider be

Identity provider	Azure AD
Authority	https://login.microsoftonline.com/7c94eaea
ClientId	29f956b0-9017-4b36-834
Client secret	ZkK8Q~DkzBhMqb2GMh.ql
Create user in TEOS after first login if it does not exist	☑
Default user role when created	Administrator
Language	English
Redirect URL	https://qa2024.teoscloud.com/Account/OidcResponse https://qa2024.teoscloud.com/EmployeeApp/Account/OidcResponse

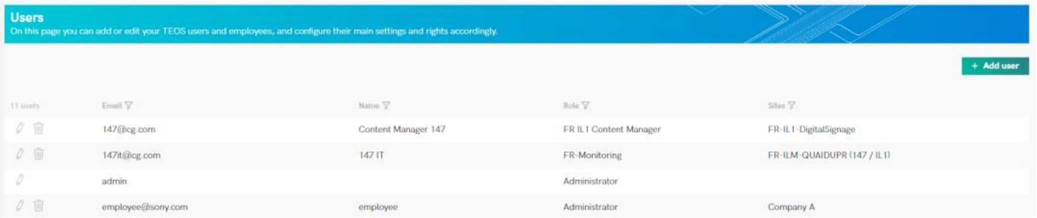
The setup is very simple for this feature, just enable the option “create user in TEOS after first login if it does not exist” and select the default user role to apply when created. You can also define a default user language which can be changed after by the user.

3. Create users and rights before synching SSO.

This section is used to manage your users. This consists of both creating the individual users, as well as assigning them to groups and permissions. These roles will be used to give view to part of the platform and uses as user rights capability within content management or device localization management or visibility of spaces in the Mobile App

Users

On the User Management page, you can create, delete or edit users.



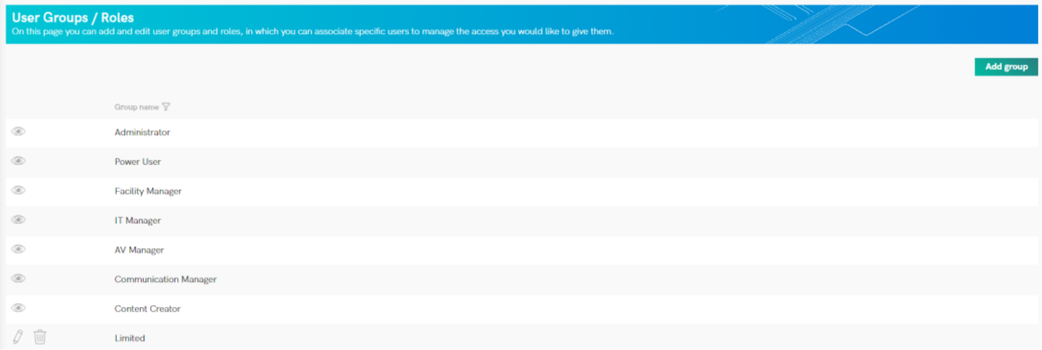
Users

On this page you can add or edit your TEOS users and employees, and configure their main settings and rights accordingly.

11 users	Email	Name	Role	Sites
	147@cg.com	Content Manager 147	FR IL1 Content Manager	FR-IL1-DigitalSignage
	147it@cg.com	147 IT	FR-Monitoring	FR-ILM-QUAIDUPR (147 / IL1)
	admin		Administrator	
	employee@sony.com	employee	Administrator	Company A

User groups / roles

In this section you will see the standard/pre-created roles at the top. These roles can’t be adjusted and only have a view option. You can also create your own groups.



User Groups / Roles

On this page you can add and edit user groups and roles, in which you can associate specific users to manage the access you would like to give them.

Group name
Administrator
Power User
Facility Manager
IT Manager
AV Manager
Communication Manager
Content Creator
Limited

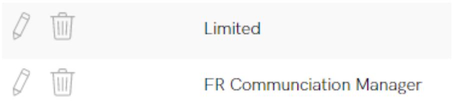
Standard roles

The rights for the standard roles can be seen when you click the 👁 icon in front of the role.

Created roles

In the USER GROUPS / ROLES section as an administrator you can use the ADD GROUP button to add new roles which you can assign to a user when you are creating or editing a user.
You can give this role a name and select the sections in Manage for TEOS where you want the created role to have access to.When you select a menu item (the items with a – symbol in front) automatically it will select all subsections of that item.
For example, if you select Schedules and Alarms it will also select Content schedules, Actions Schedule, Alarms, Meetings Schedule and Automation Scenarios.
If you select a subsection, it will automatically select the menu item.
For example, if you select Content schedule it will automatically activate Schedules and Alarms.
After saving this created role can be used when creating or editing a user.

After you have created a new role they will appear in the User group / role section from where you also have the options to edit or delete the create role.



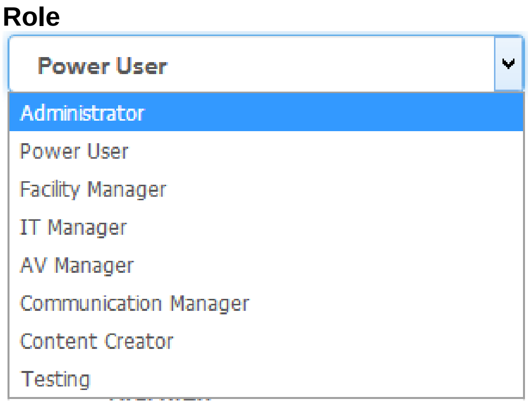
Limited

FR Communciation Manager

Creating / Editing a user

When creating or editing a user you will now have more options to use as role for a user.
When you are creating a user by clicking “Server Management” > “User Management” > “Add user” or editing a user by clicking the pencil icon in front of the username you also need to fill in the following details

- Name
- Email
- Phone number
- Language
- Tenant
- Role
- Password
- Confirm password
- Can create users in their group (to give the rights to create users for the users group)
- Disable access to Manage for TEOS platform
- Enable lockout (when a password is entered incorrect multiple times)
- Device group access*
- NFC ID



Role

Power User

Administrator
Power User
Facility Manager
IT Manager
AV Manager
Communication Manager
Content Creator
Testing

You can find the pre-configured roles here and after those you will see the created roles. In our example this created role Is "Testing".

Users can be imported using script based on an excel (please consult the https://teos.solutions resources). The other option to get users on top of the manual creation on the platform is by synchronizing Azure AD Groups and assigning to roles. TEOS will then automatically synchronize users.

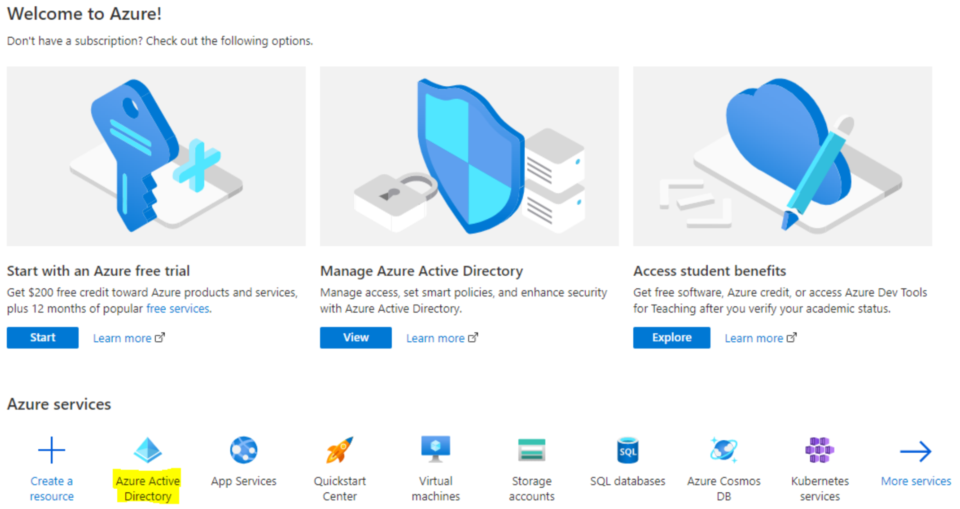
4. Azure AD user group synchronizations

4.1 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.

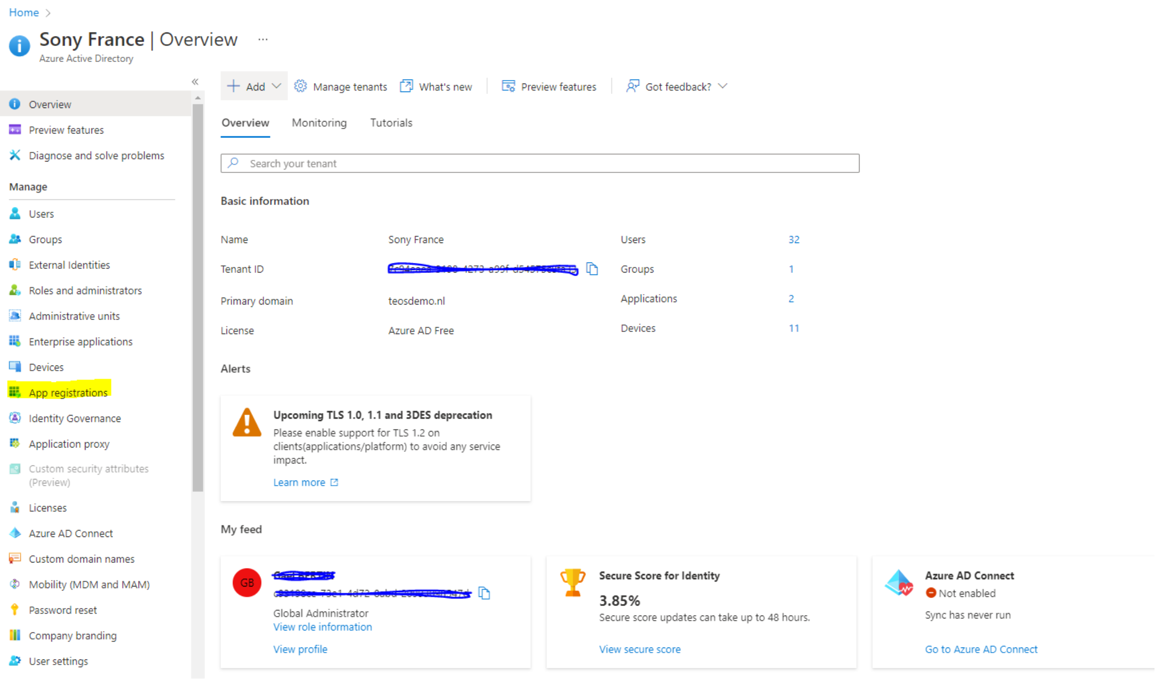
Manage Azure Active Directory

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

Access student benefits

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

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

[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

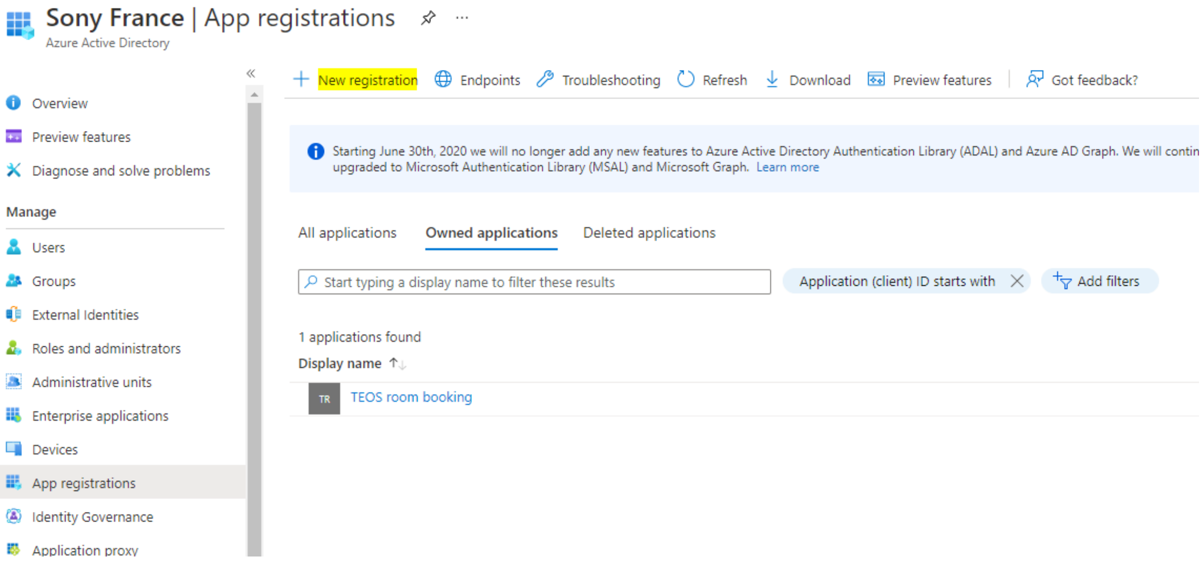
Azure AD Connect

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.



Sony France | App registrations

Azure Active Directory

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

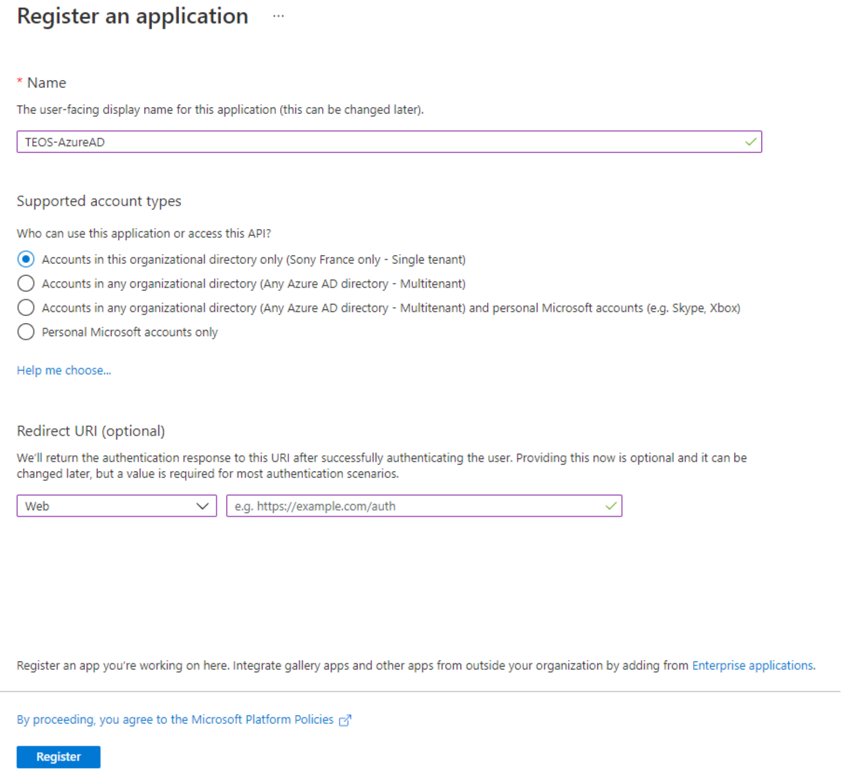
Application (client) ID starts with

1 applications found

Display name

TR 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



Register an application ···

* 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)

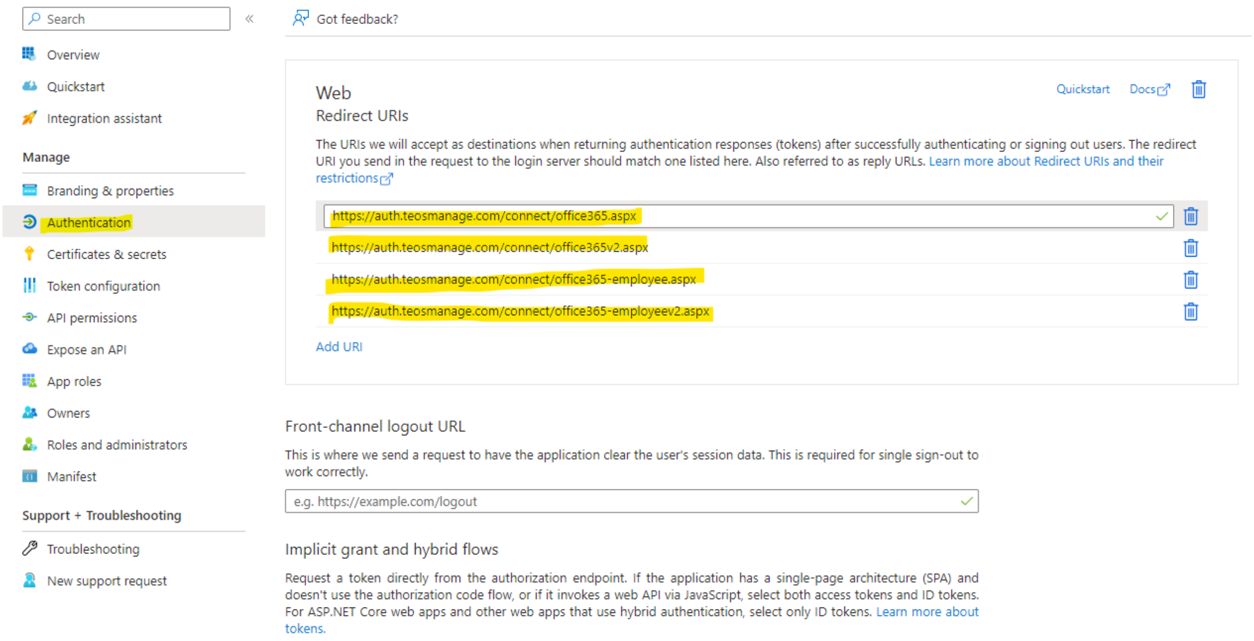
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

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

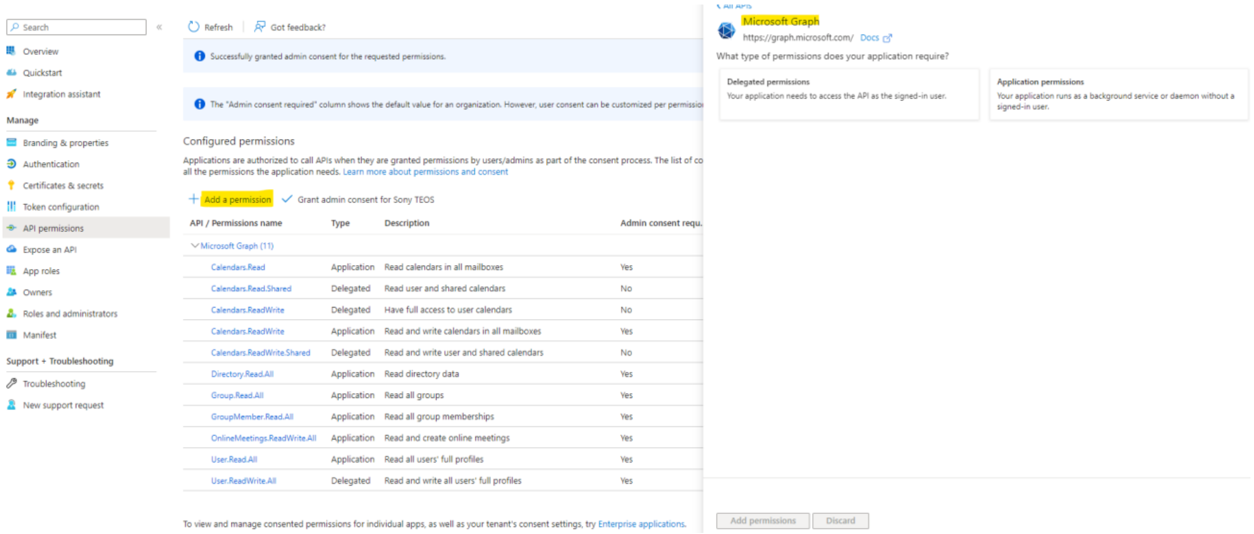
This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

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/ Docs

What type of permissions does your application require?

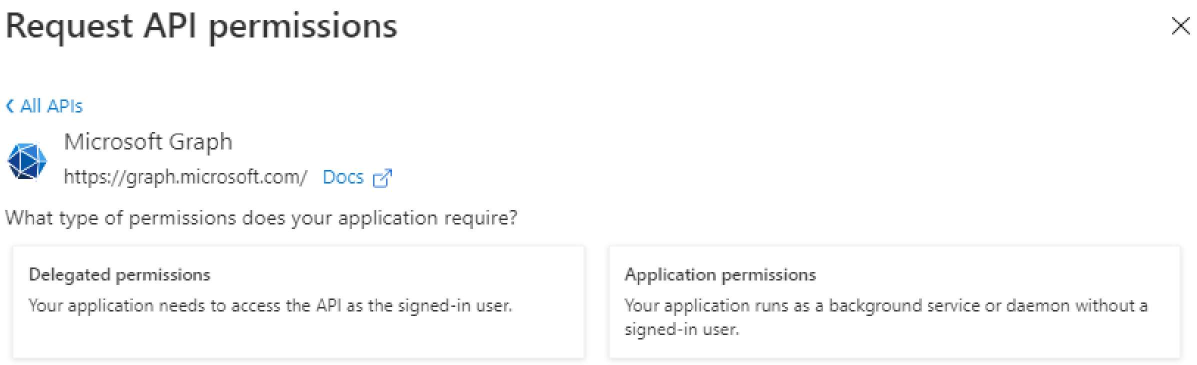
Delegated permissions

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 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?

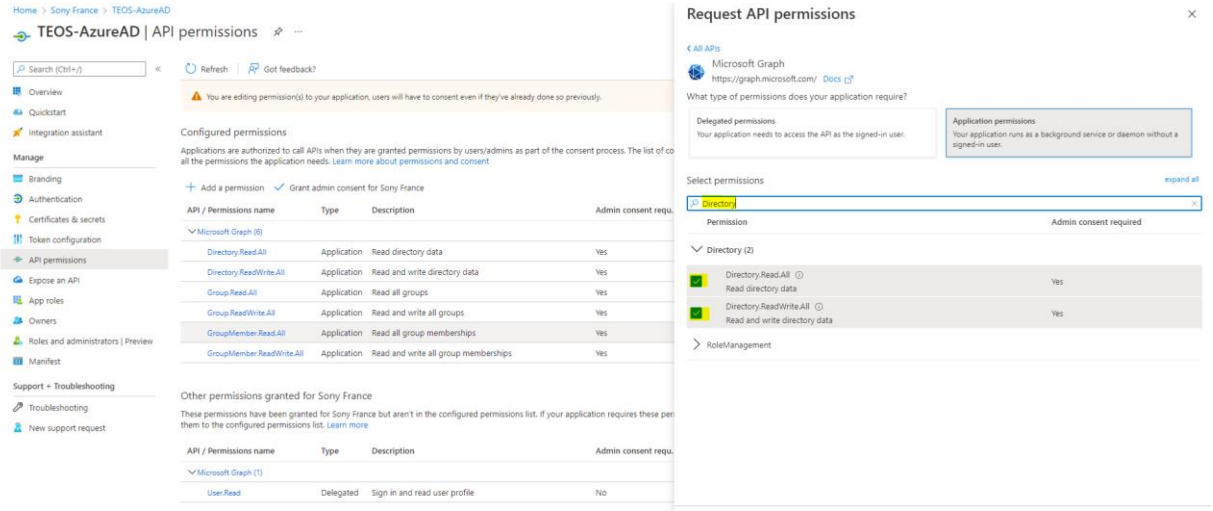
Delegated permissions

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

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.

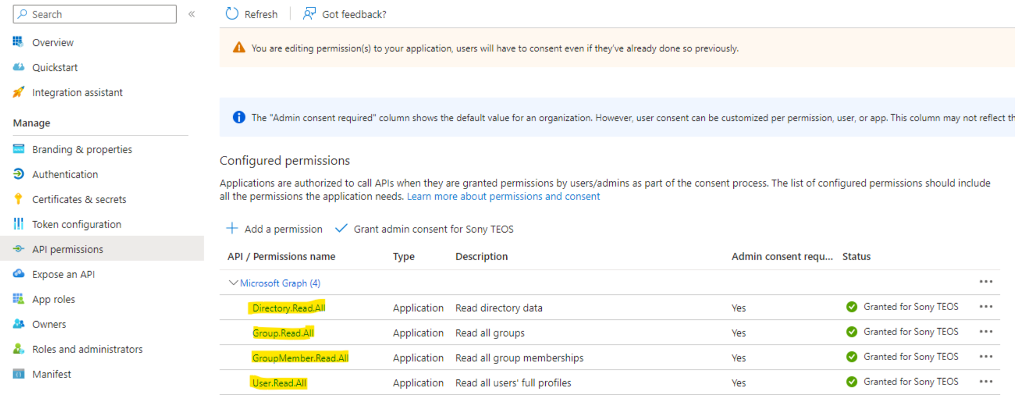
Select permissions

Directory

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

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

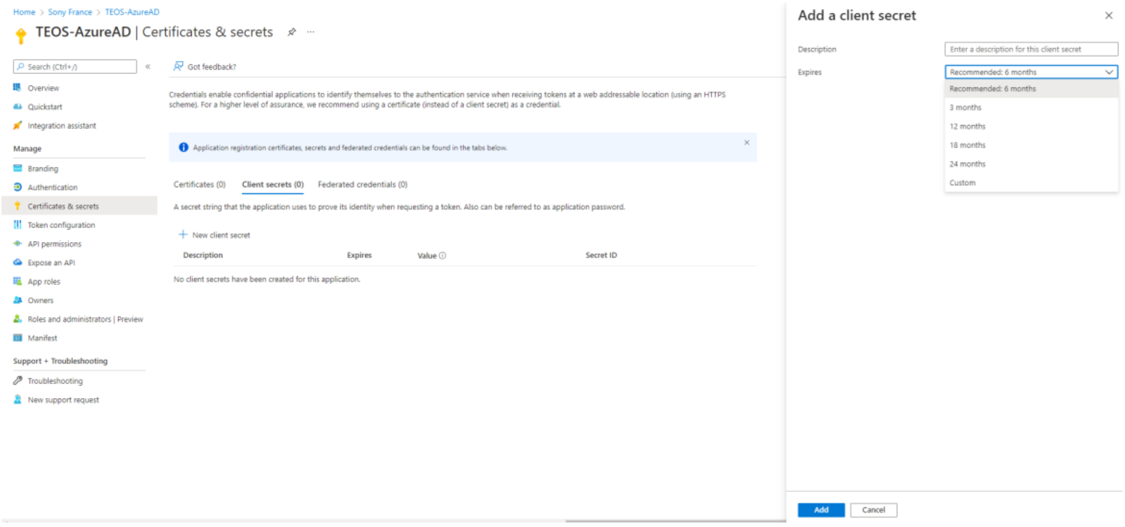
Configured permissions

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

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.

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.



Home > Sony France > TEOS-AzureAD

TEOS-AzureAD | Certificates & secrets

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.

Certificates (0) | Client secrets (0) | Federated credentials (0)

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

+ New client secret

Description	Expires	Value	Secret ID

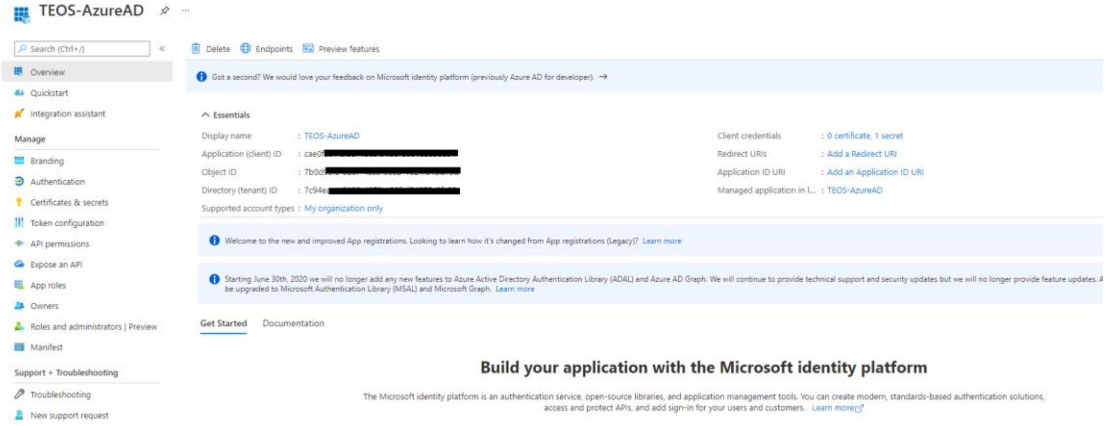
No client secrets have been created for this application.

Add a client secret

Description: Enter a description for this client secret

Expires: Recommended: 6 months

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



TEOS-AzureAD

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

Essentials

Display name : TEOS-AzureAD
Application (client) ID : cae0f[redacted]
Object ID : 7b0d[redacted]
Directory (tenant) ID : 7c94e[redacted]
Supported account types : My organization only

Client credentials : 0 certificate, 1 secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : TEOS-AzureAD

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

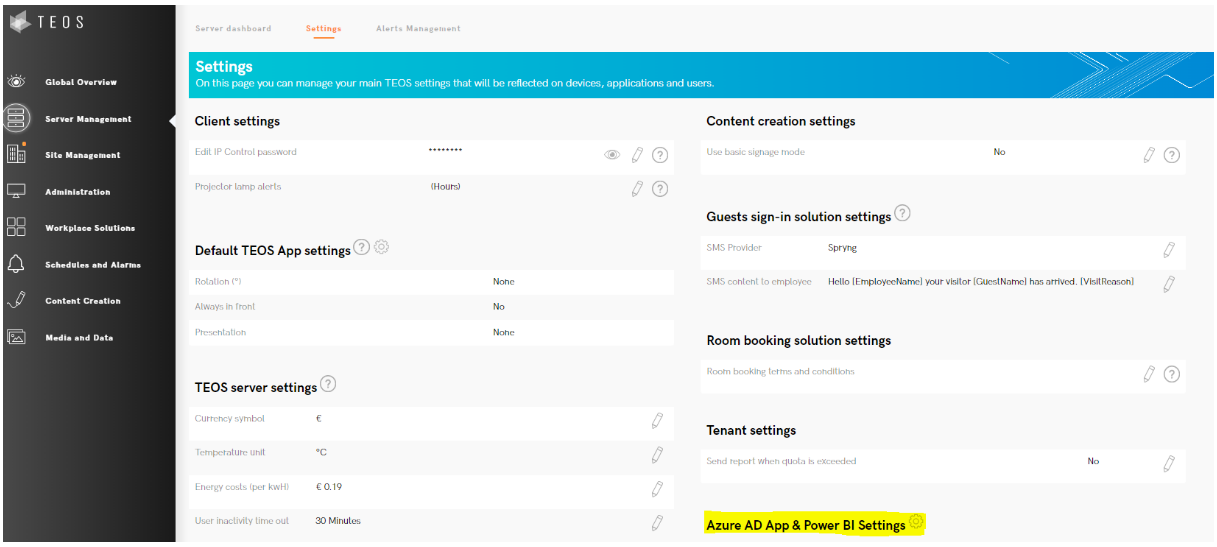
Get Started | Documentation

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

4.2 Sync TEOS with Azure AD User

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

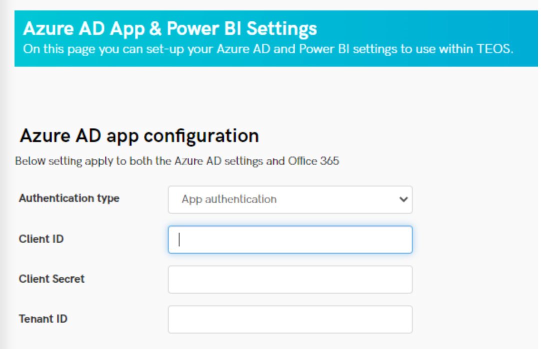
Room booking terms and conditions

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	

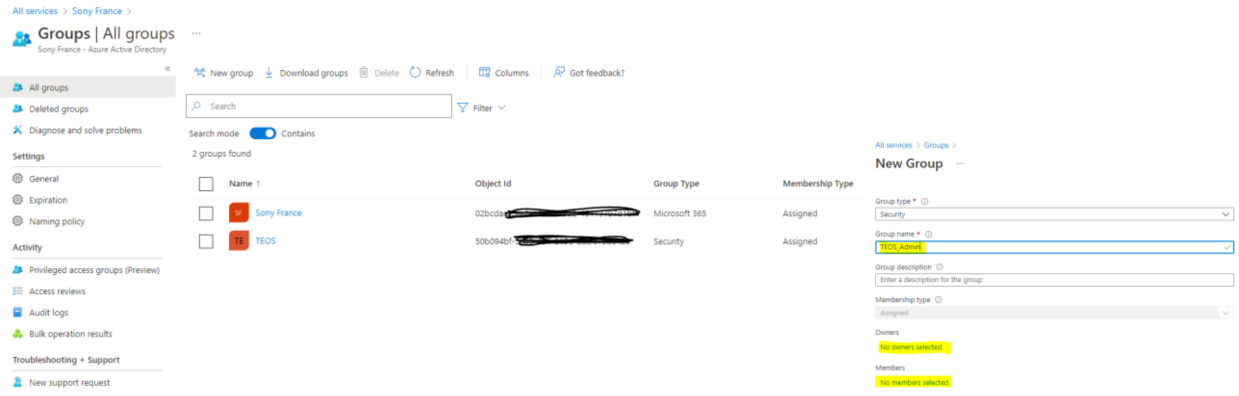
If you get an error in the synchronization, please go to your folders C:\\TEOS Manage > www > Backbone > web.config and make sure you have the correct url.

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

4.3 Add users from Azure AD to TEOS

4.3.1 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)



All services > Sony France >

Groups | All groups

Sony France - Azure Active Directory

Search mode: Contains

2 groups found

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

All services > Groups >

New Group

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

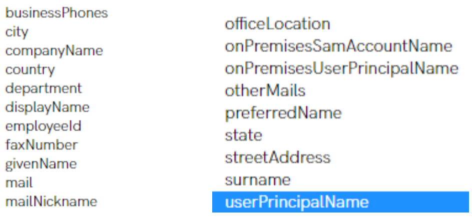
When the group is created click on “no members selected” for you to be able to add users to the group

4.3.2 Configuration in TEOS

Go to Administration > Active Directory Settings

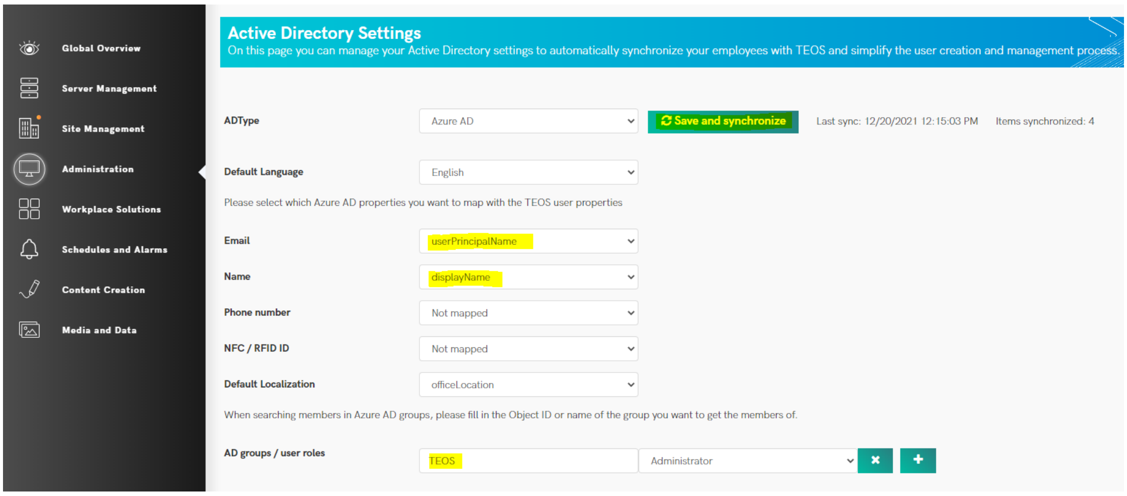
Select the AD Type to Azure AD. Select then the default language. You can then select the field that TEOS will be able to save in his database from user profiles.

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.

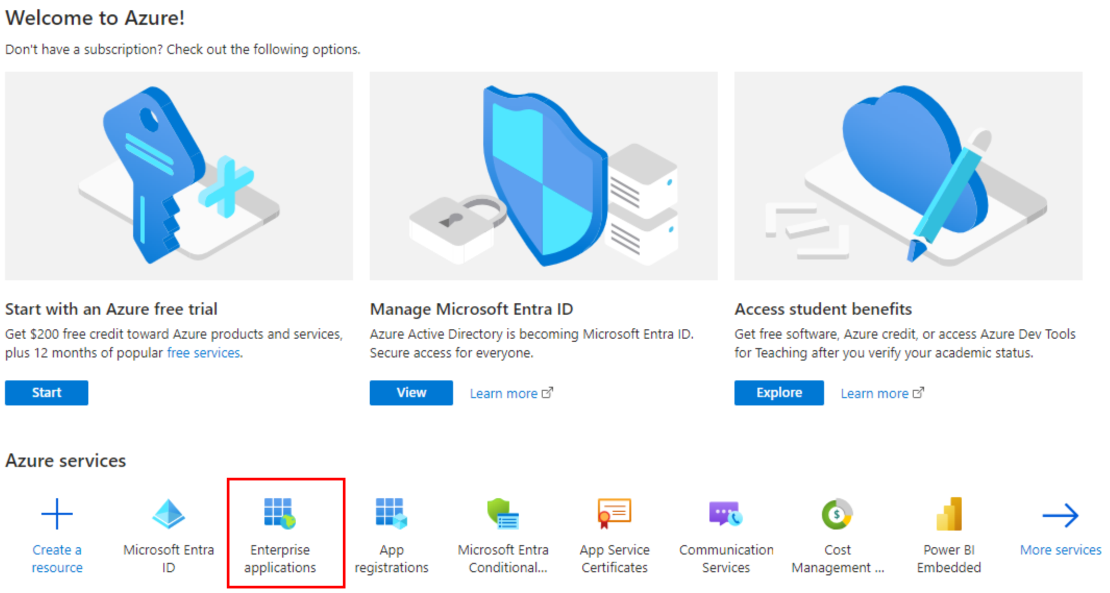
5. Configuration of Single Sign On (SSO) in Azure

5.1 Example of configuration in Azure

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

Manage Microsoft Entra ID

Azure Active Directory is becoming Microsoft Entra ID. Secure access for everyone.

View Learn more

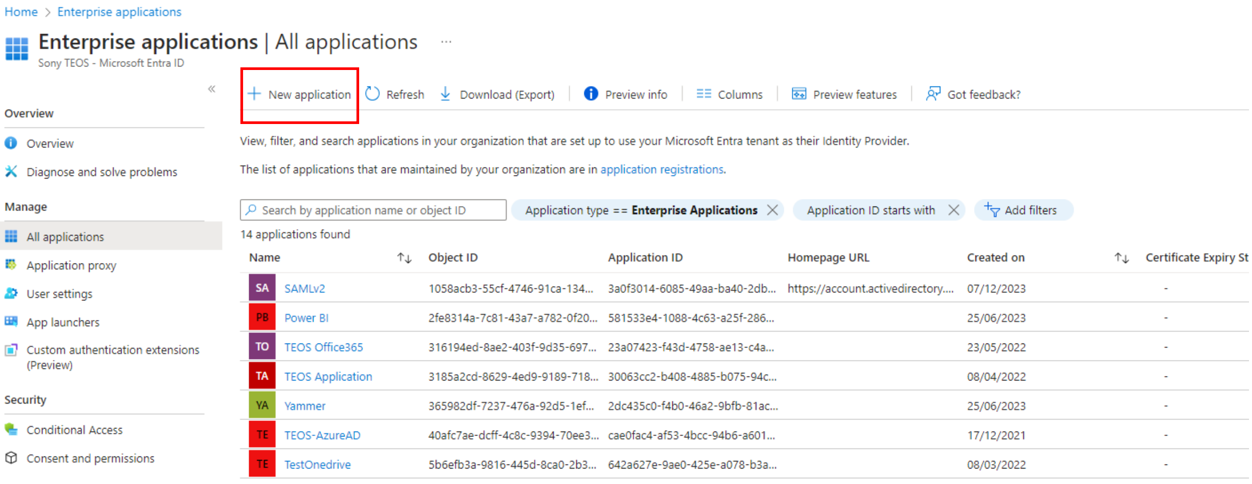
Access student benefits

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

Explore Learn more

Azure services

2) Click on new application (or if you have already a TEOS dedicated application you can select it)



View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

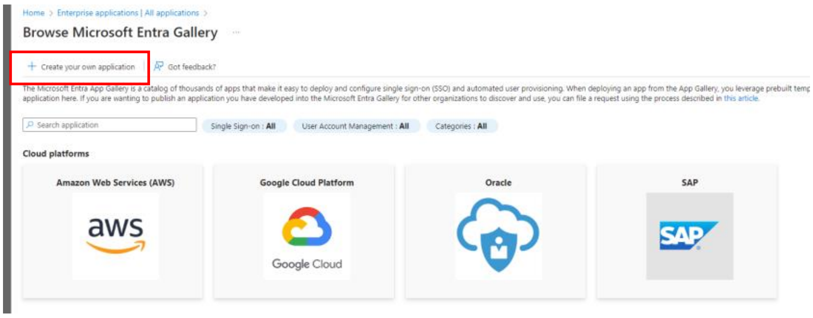
The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID | Application type == **Enterprise Applications** | Application ID starts with | Add filters

14 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry St
SA SAMLv2	1058acb3-55cf-4746-91ca-134...	3a0f3014-6085-49aa-ba40-2db...	https://account.activedirectory....	07/12/2023	-
PB Power BI	2fe8314a-7c81-43a7-a782-0f20...	581533e4-1088-4c63-a25f-286...		25/06/2023	-
TO TEOS Office365	316194ed-8ae2-403f-9d35-697...	23a07423-f43d-4758-ae13-c4a...		23/05/2022	-
TA TEOS Application	3185a2cd-8629-4ed9-9189-718...	30063cc2-b408-4885-b075-94c...		08/04/2022	-
YA Yammer	365982df-7237-476a-92d5-1ef...	2dc435c0-f4b0-46a2-9bfb-81ac...		25/06/2023	-
TE TEOS-AzureAD	40afc7ae-dcff-4c8c-9394-70ee3...	cae0fac4-af53-4bcc-94b6-a601...		17/12/2021	-
TE TestOnedrive	5b6efb3a-9816-445d-8ca0-2b3...	642a627e-9ae0-425e-a078-b3a...		08/03/2022	-

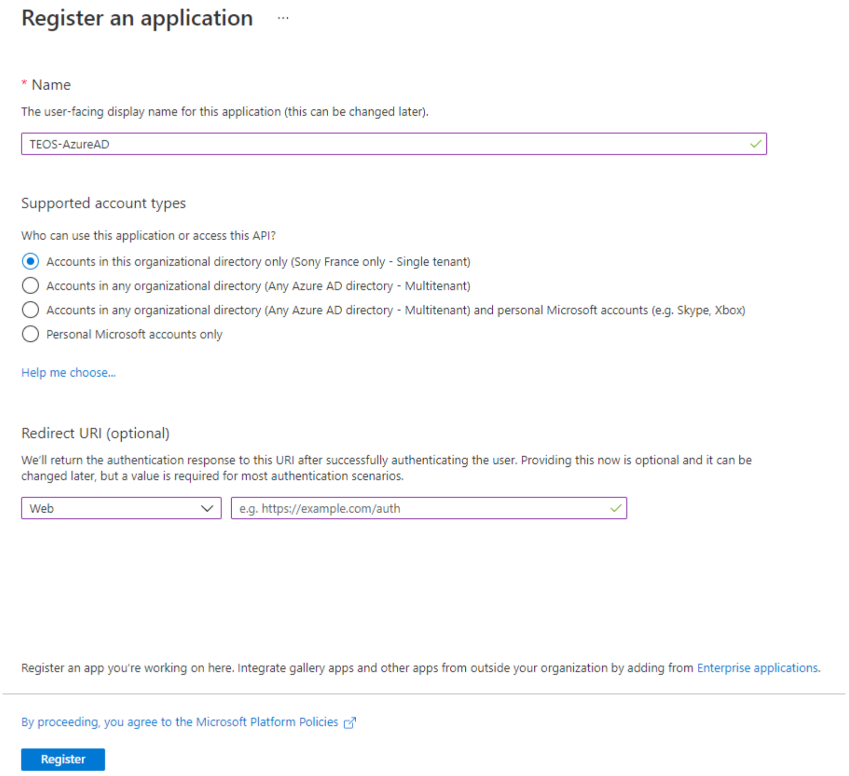
3) Under app registrations press “create your own application” and define a name for the App. Select “register an application to integrate with Microsoft Entra ID (app you’re developing)



Home > Enterprise applications | All applications >
Browse Microsoft Entra Gallery ...
Create your own application
Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt temp application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

4) Define a name that you can easily recognize for a region or a country or where you will use the rooms/users.



Register an application ···

* 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 ✓

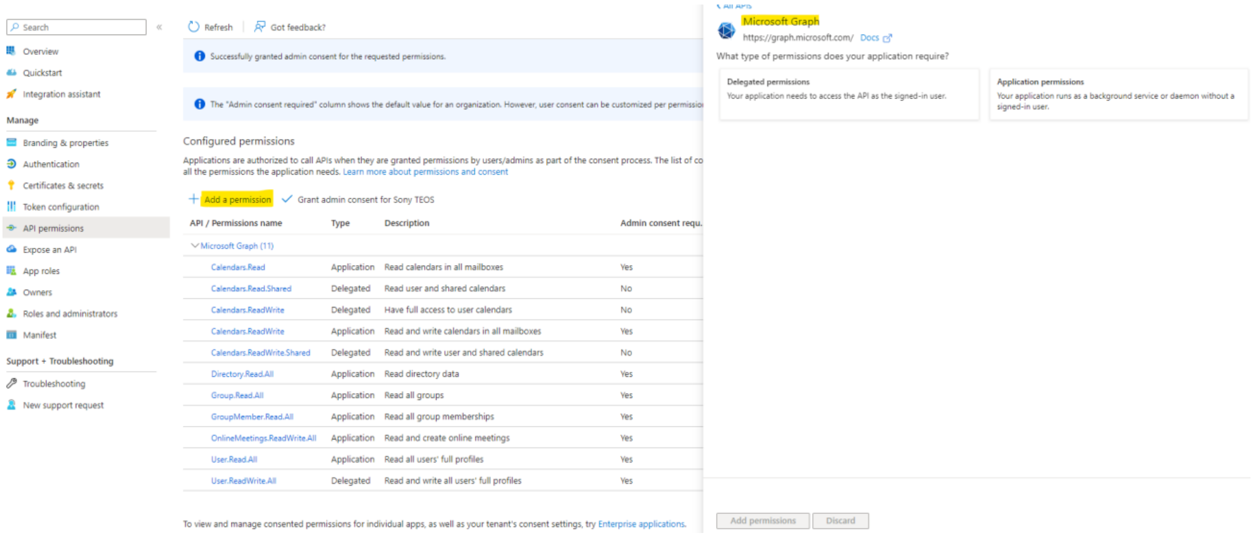
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Redirect URLs are shown in your TEOS tenant under server management > Settings > SSO Configuration, it is based directly on the tenant name.

URL redirect for TEOS Manage Page: https://yourteostenantname/Account/OidcResponse
(Example: https://demo.teoscloud.com/Account/OidcResponse)
URL redirect for Employee App: https://yourteostenantname/EmployeeApp/Account/OidcResponse
(Example: https://demo.teoscloud.com/EmployeeApp/Account/OidcResponse)

5) When you pressed to register, go then to 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

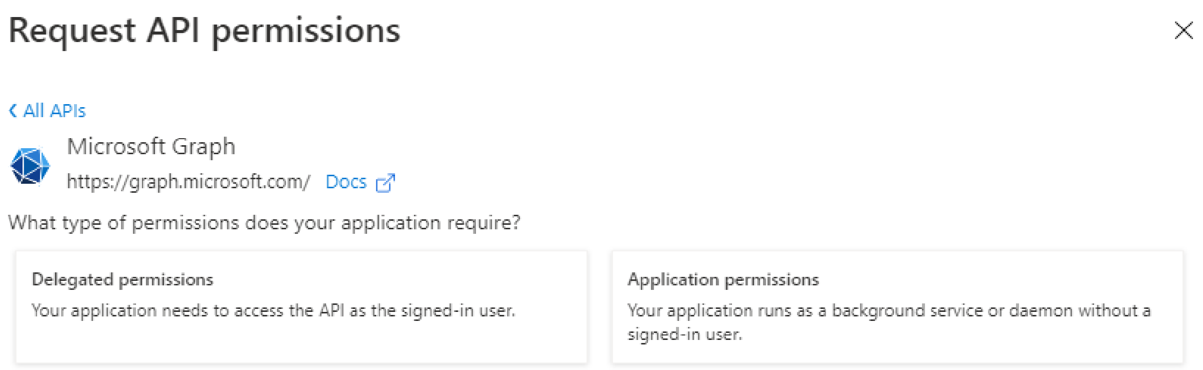
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

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 (delegated needed in this case)

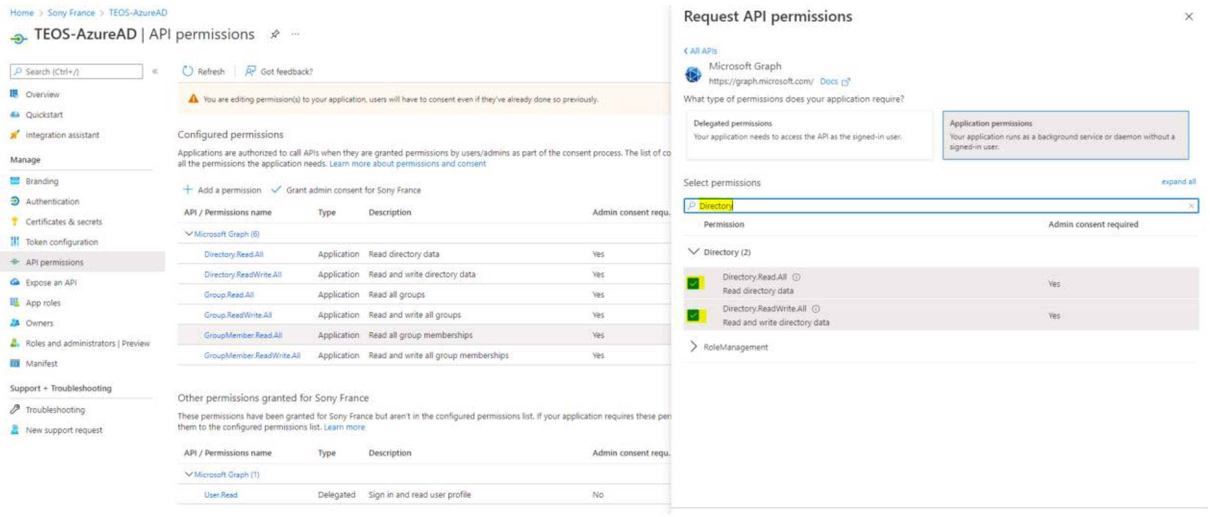


What type of permissions does your application require?

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

+ Add a permission ✓ Grant admin consent for Sony France

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

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.

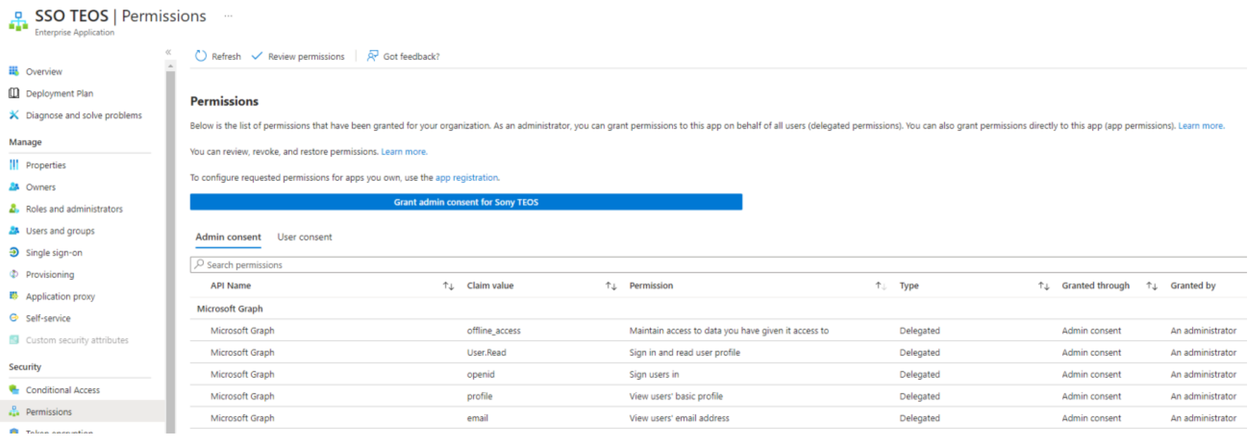
Select permissions expand all

Directory

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

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

Permission name	Type	Description
email	Delegated	View users' email address
profile	Delegated	View user basic profile
openid	Delegated	Sign users in
Offline_access	Delegated	Maintain access to data you have given it access to
User.read	Delegated	Sign in and read user profile



Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). Learn more.

You can review, revoke, and restore permissions. Learn more.

To configure requested permissions for apps you own, use the app registration.

Grant admin consent for Sony TEOS

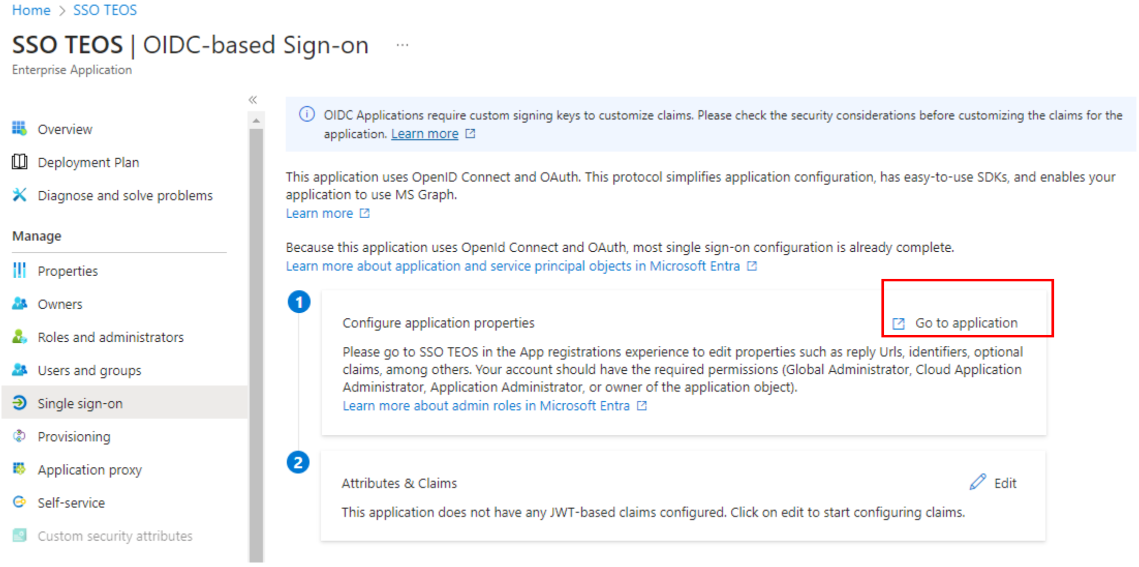
Admin consent User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph					
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read	Sign in and read user profile	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	email	View users' email address	Delegated	Admin consent	An administrator

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.

6) Go to Single sign on and click on go to application



SSO TEOS | OIDC-based Sign-on ···

Enterprise Application

OIDC Applications require custom signing keys to customize claims. Please check the security considerations before customizing the claims for the application. Learn more

This application uses OpenID Connect and OAuth. This protocol simplifies application configuration, has easy-to-use SDKs, and enables your application to use MS Graph.
Learn more

Because this application uses OpenId Connect and OAuth, most single sign-on configuration is already complete.
Learn more about application and service principal objects in Microsoft Entra

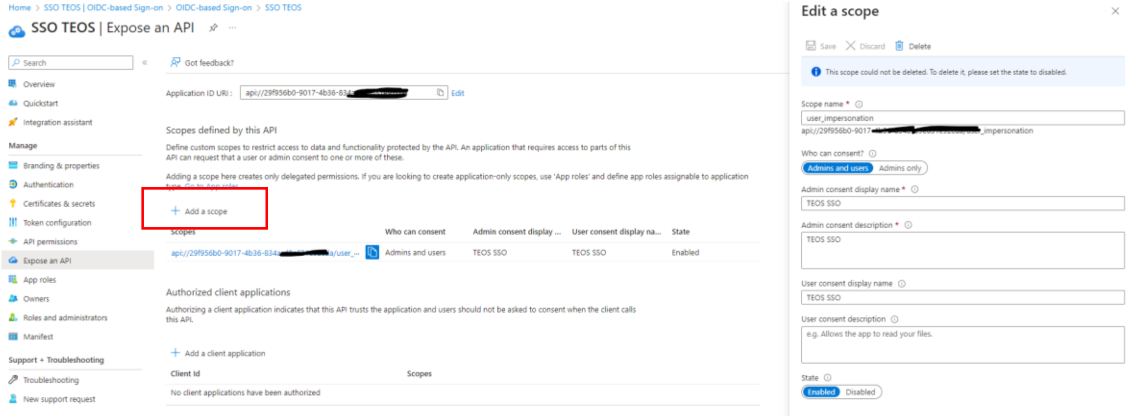
1 Configure application properties

Please go to SSO TEOS in the App registrations experience to edit properties such as reply Urls, identifiers, optional claims, among others. Your account should have the required permissions (Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the application object).
Learn more about admin roles in Microsoft Entra

2 Attributes & Claims

This application does not have any JWT-based claims configured. Click on edit to start configuring claims.

7) Go to Expose an API section and add a scope, this will create the api access for TEOS to connect. Define as scope name user_impresonation and give consent to admins and Users. Define a name for the admin consent display name (like TEOS SSO for example) and a description to be able to save



SSO TEOS | Expose an API

Application ID URI : api://29f956b0-9017-4b36-834[redacted]

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

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
api://29f956b0-9017-4b36-834[redacted]a/user_...	Admins and users	TEOS SSO	TEOS SSO	Enabled

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.

Client Id	Scopes
No client applications have been authorized	

Edit a scope

This scope could not be deleted. To delete it, please set the state to disabled.

Scope name * : user_impersonation
api://29f956b0-9017[redacted]_impersonation

Who can consent? : ● Admins and users ○ Admins only

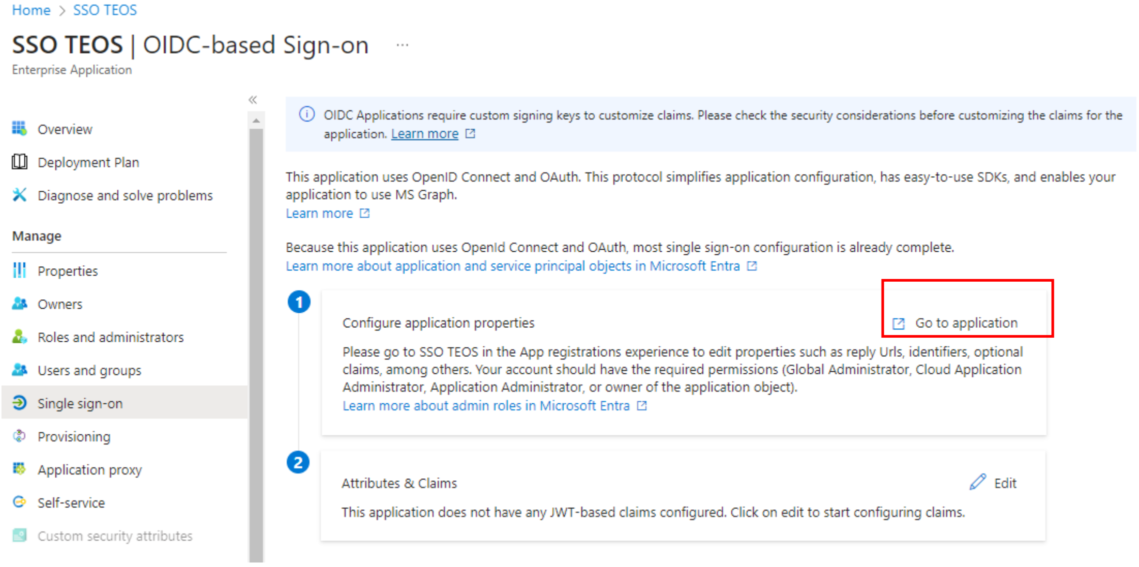
Admin consent display name * : TEOS SSO

Admin consent description * : TEOS SSO

User consent display name : TEOS SSO

User consent description : e.g. Allows the app to read your files.

State : ● Enabled ○ Disabled


Home > SSO TEOS

SSO TEOS | OIDC-based Sign-on ···

Enterprise Application

OIDC Applications require custom signing keys to customize claims. Please check the security considerations before customizing the claims for the application. Learn more

This application uses OpenID Connect and OAuth. This protocol simplifies application configuration, has easy-to-use SDKs, and enables your application to use MS Graph.
Learn more

Because this application uses OpenId Connect and OAuth, most single sign-on configuration is already complete.
Learn more about application and service principal objects in Microsoft Entra

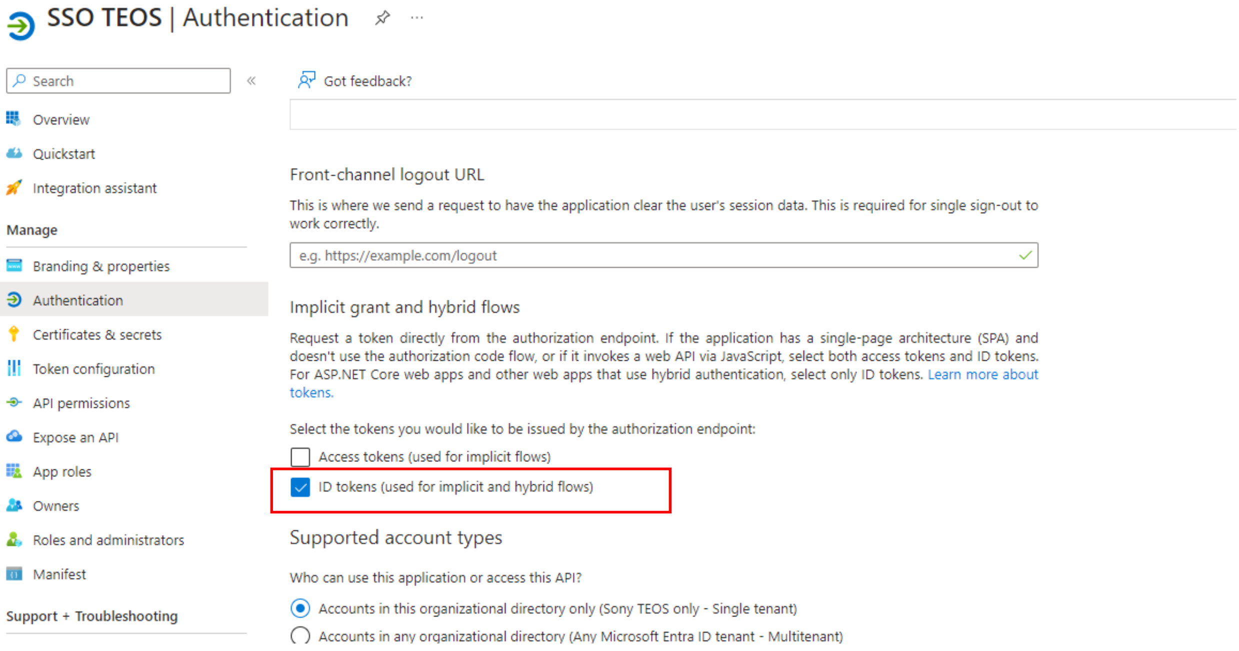
1 Configure application properties

Please go to SSO TEOS in the App registrations experience to edit properties such as reply Urls, identifiers, optional claims, among others. Your account should have the required permissions (Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the application object).
Learn more about admin roles in Microsoft Entra

2 Attributes & Claims

This application does not have any JWT-based claims configured. Click on edit to start configuring claims.

8) Go to authentication and make sure the option ID tokens (used for implicit and hybid flows) is enabled.



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)

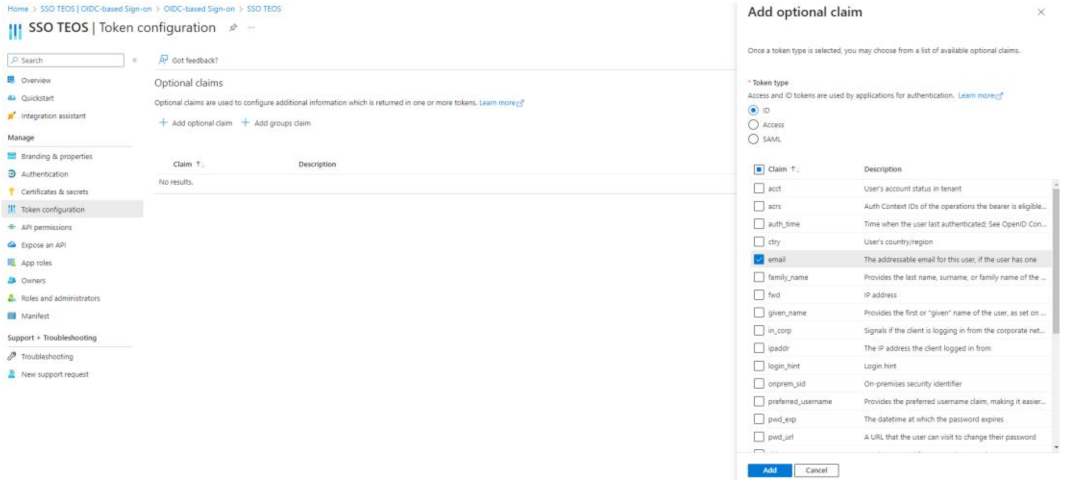
Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Sony TEOS only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

9) Go to token configuration and add an optional claim with ID and email



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

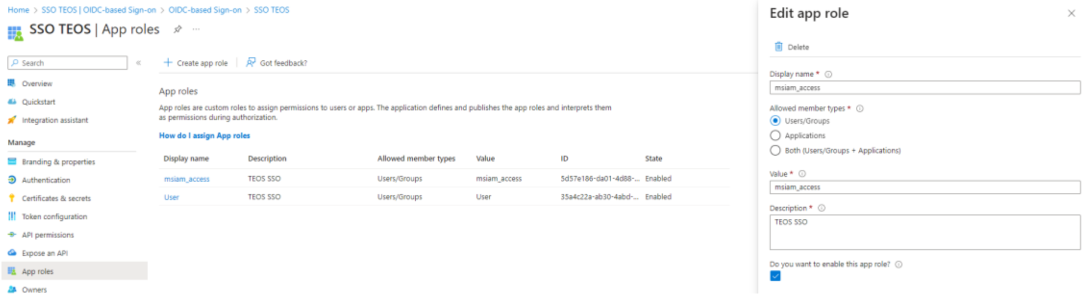
* Token type

Access and ID tokens are used by applications for authentication. Learn more

● ID
○ Access
○ SAML

	Claim	Description
□	acct	User's account status in tenant
□	acrs	Auth Context IDs of the operations the bearer is eligible...
□	auth_time	Time when the user last authenticated; See OpenID Con...
□	ctry	User's country/region
☑	email	The addressable email for this user, if the user has one
□	family_name	Provides the last name, surname, or family name of the ...
□	fwd	IP address
□	given_name	Provides the first or "given" name of the user, as set on ...
□	in_corp	Signals if the client is logging in from the corporate net...
□	ipaddr	The IP address the client logged in from
□	login_hint	Login hint
□	onprem_sid	On-premises security identifier
□	preferred_username	Provides the preferred username claim, making it easier...
□	pwd_exp	The datetime at which the password expires
□	pwd_url	A URL that the user can visit to change their password

10) Go to App roles and add the roles user (with user/groups type member) and value “User” as well as the the msiam_access with same value and user/group type member



App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
msiam_access	TEOS SSO	Users/Groups	msiam_access	5d57e186-da01-4d88-...	Enabled
User	TEOS SSO	Users/Groups	User	35a4c22a-ab30-4abd-...	Enabled

Edit app role

Display name *: msiam_access

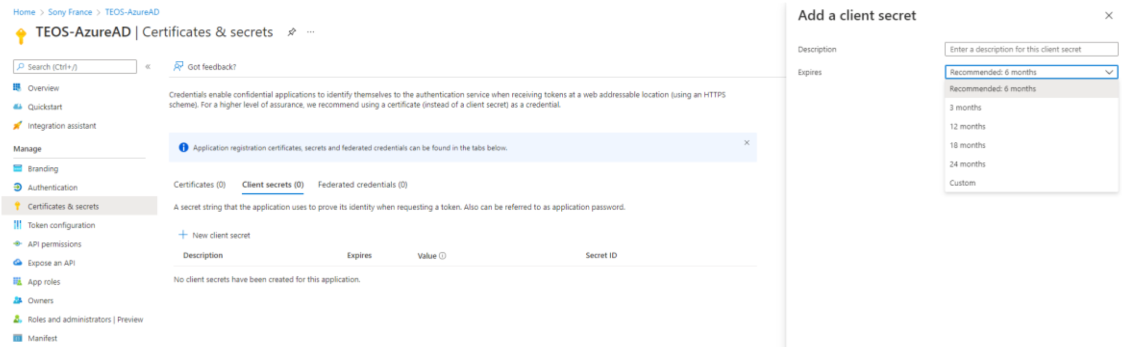
Allowed member types *
● Users/Groups
○ Applications
○ Both (Users/Groups + Applications)

Value *: msiam_access

Description *: TEOS SSO

Do you want to enable this app role? ☑

11) 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.



Home > Sony France > TEOS-AzureAD

TEOS-AzureAD | Certificates & secrets

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.

Certificates (0) | Client secrets (0) | Federated credentials (0)

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

+ New client secret

Description	Expires	Value	Secret ID

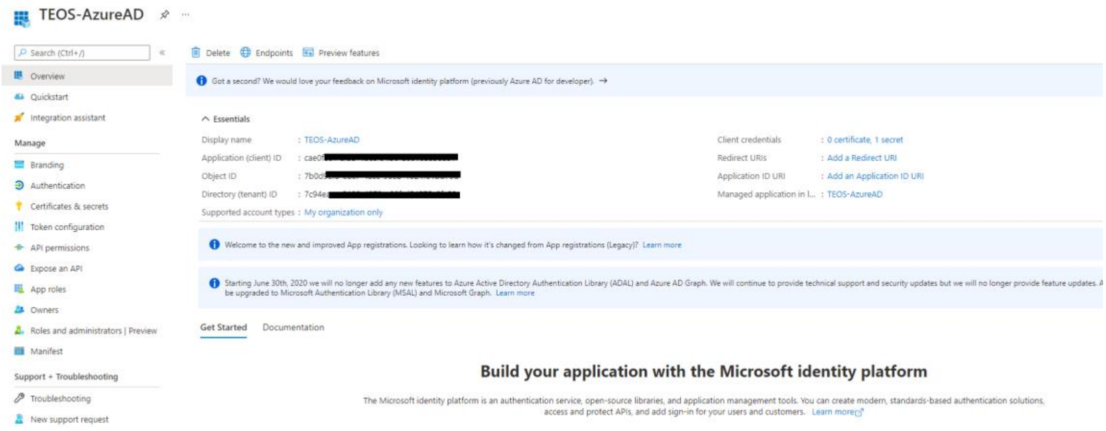
No client secrets have been created for this application.

Add a client secret

Description: Enter a description for this client secret

Expires: Recommended: 6 months

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



TEOS-AzureAD

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

Essentials

Display name : TEOS-AzureAD
Application (client) ID : cae0f[redacted]
Object ID : 7b0d[redacted]
Directory (tenant) ID : 7c94e[redacted]
Supported account types : My organization only

Client credentials : 0 certificate, 1 secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : TEOS-AzureAD

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

Get Started | Documentation

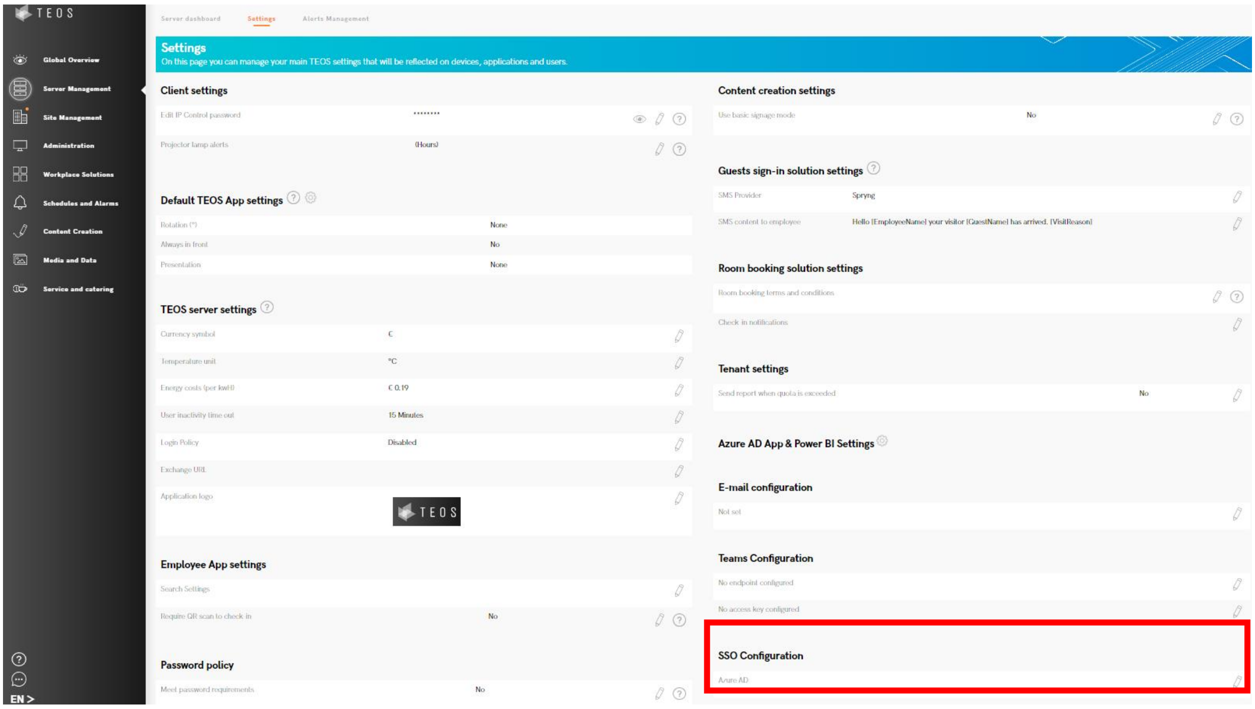
Build your application with the Microsoft identity platform

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

5.2 Configuration under TEOS

After making sure you have all your users including admin users, Go to server management > settings.

Under settings from Version 3.2.1 you can find the option, click on the pensil to edit it



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 15 Minutes
Login Policy Disabled
Exchange URL
Application logo TEOS

Employee App settings

Search Settings
Require QR scan to check in No

Password policy

Meet password requirements No

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
Check in notifications

Tenant settings

Send report when quota is exceeded No

Azure AD App & Power BI Settings

E-mail configuration

Not set

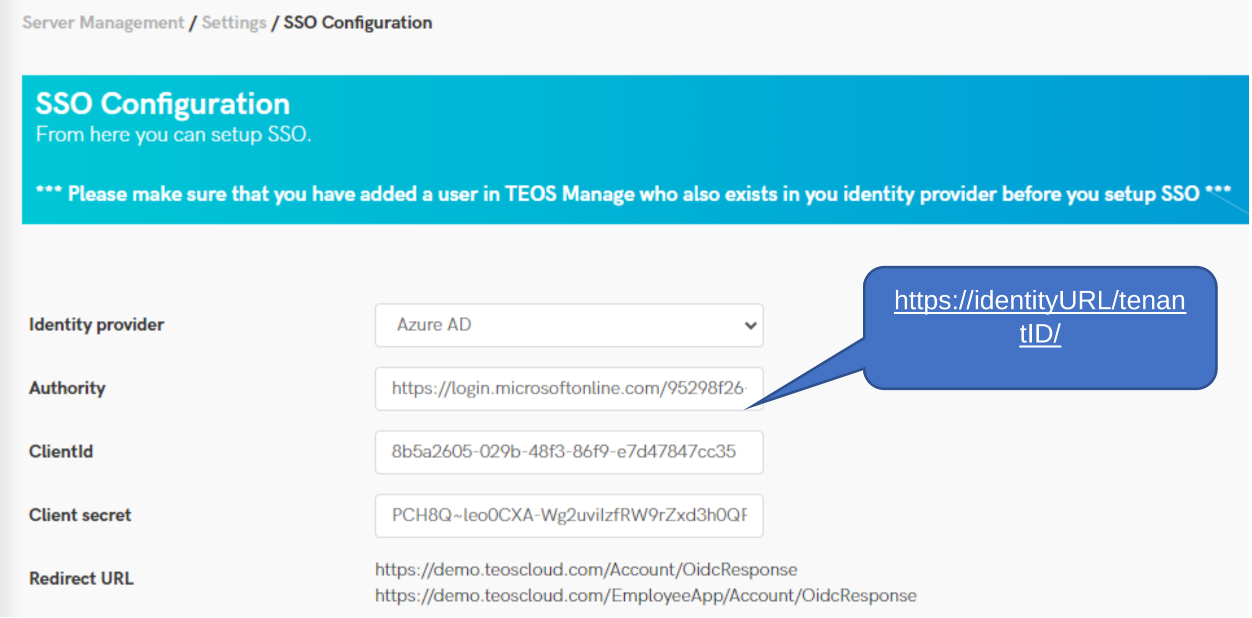
Teams Configuration

No endpoint configured
No access key configured

SSO Configuration

Azure AD

Within this section you will be able to select Azure AD (or Entra ID) as Identity provider or Ping One as another identity provider. As an example below the Entra ID configuration will be done base on Azure configuration. As the protocol use is OIDC, any other identity provider should work and the fields for the other identity providers can be used.



Server Management / Settings / SSO Configuration

SSO Configuration

From here you can setup SSO.

*** Please make sure that you have added a user in TEOS Manage who also exists in you identity provider before you setup SSO ***

Identity provider: Azure AD

Authority: https://login.microsoftonline.com/95298f26-

ClientId: 8b5a2605-029b-48f3-86f9-e7d47847cc35

Client secret: PCH8Q~leo0CXA-Wg2uvilzfRW9rZxd3h0QF

Redirect URL: https://demo.teoscloud.com/Account/OidcResponse
https://demo.teoscloud.com/EmployeeApp/Account/OidcResponse

https://identityURL/tenantID/

Make sure on your identity provider, the redirect URL are copied from your own TEOS tenant name.

You need then to add the authority of the Identity provider in TEOS SSO configuration tab (this mainly includes the URL of the identity provider and the tenant ID (https://identityURL/tenantID/ for our example with Azure Open ID connect: https://login.microsoftonline.com/tenantID/). Finish by the client ID and client secret needed to get the Application access with the permission to consult user email for the login to the platform.

Click save on the right top page.

Log off and try to login again, the SSO access must be directly active, and the admin local account should not be accessible anymore.

If any issue on configuration happens, contact us to supprt@teos.support

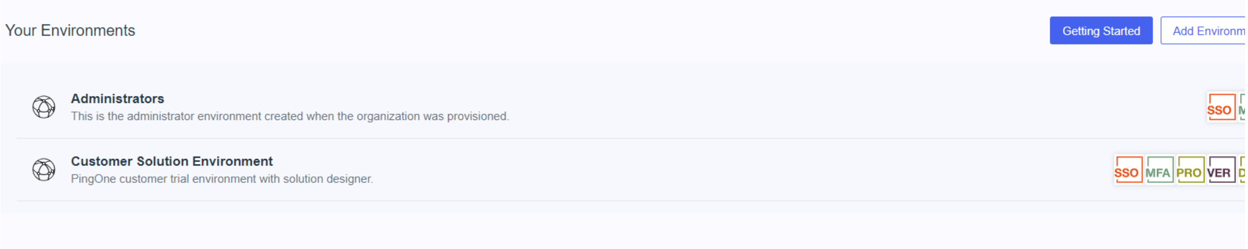
6. Configuration of Single Sign On (SSO) in Ping Identity

6.1 Example of configuration in Ping Identity

You will need to go to https://console.pingone.eu/?env=ENV_ID (complete URL is different for each customer) to start the configuration for TEOS in your Tenant.

Sign-in with admin rights to be able to create applications and configure the required application settings.

1) On the dashboard, select your environment to open it.

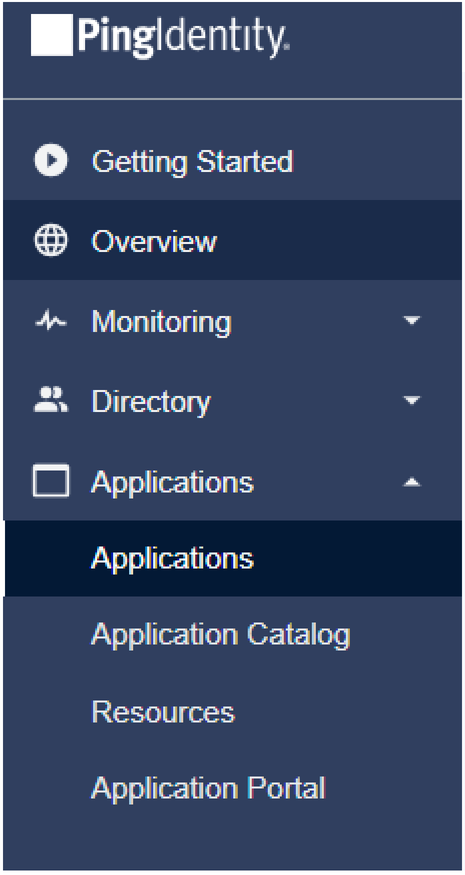


Your Environments

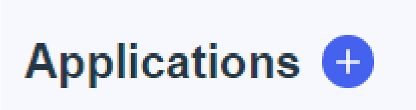
Administrators
This is the administrator environment created when the organization was provisioned.

Customer Solution Environment
PingOne customer trial environment with solution designer.

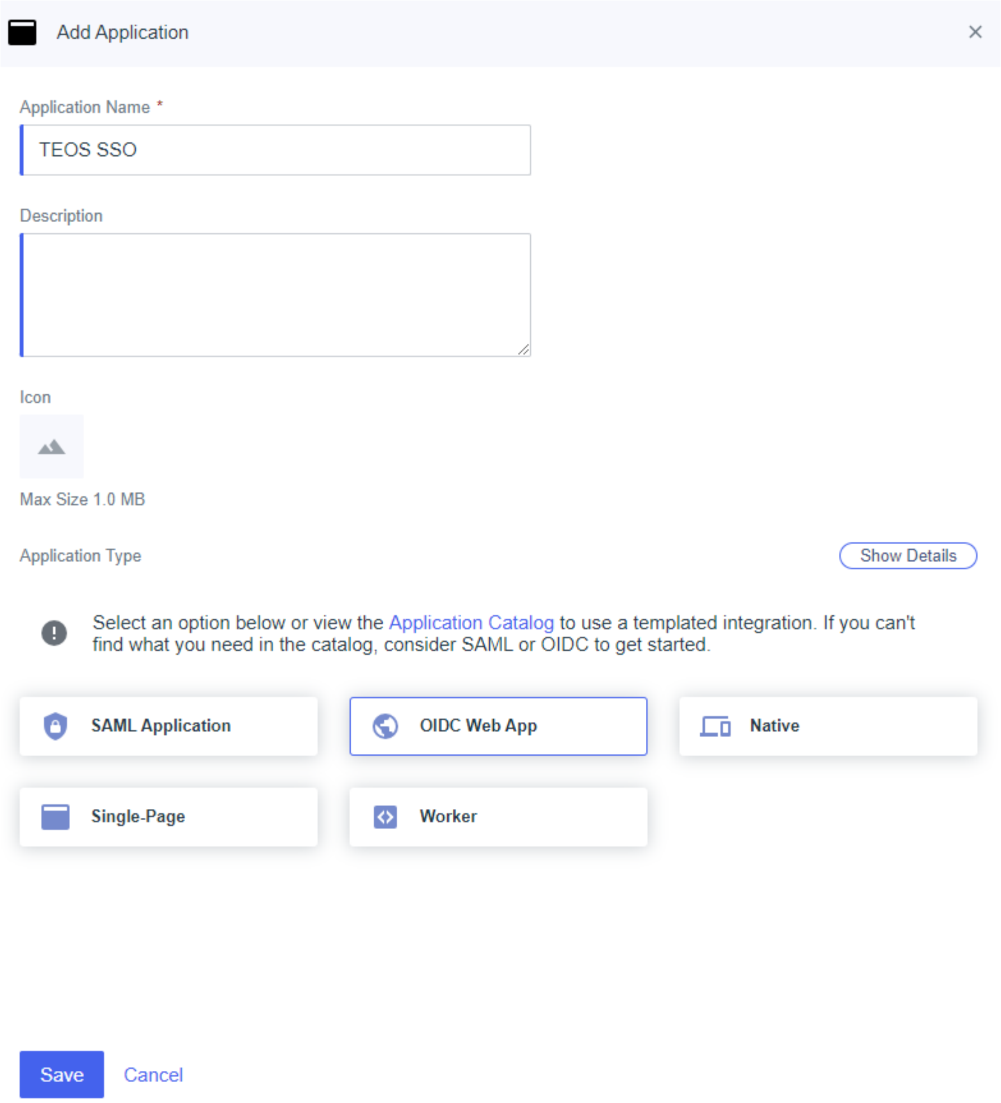
2) Next navigate in the sidebar to applications -> Applications



3) Create a new application by clicking on the + in the top right



You need to give your application a name, and optional a description. The type of application needs to be: OIDC Web App. After configuring this, press “Save”.


Add Application

Application Name *

TEOS SSO

Description

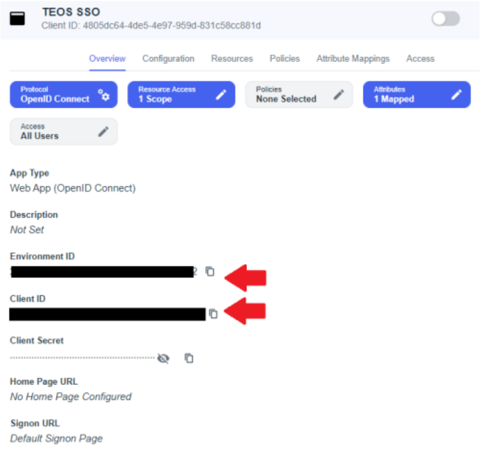
Icon

Max Size 1.0 MB

Application Type

Select an option below or view the Application Catalog to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

4) In this next page you can find your Client ID and Secret. Copy these for use in TEOS Manage later.


TEOS SSO
Client ID: 4805dc64-4de5-4e97-959d-831c58cc881d

Protocol: OpenID Connect
Resource Access: 1 Scope
Policies: None Selected
Attributes: 1 Mapped
Access: All Users

App Type
Web App (OpenID Connect)

Description
Not Set

Environment ID
[redacted]

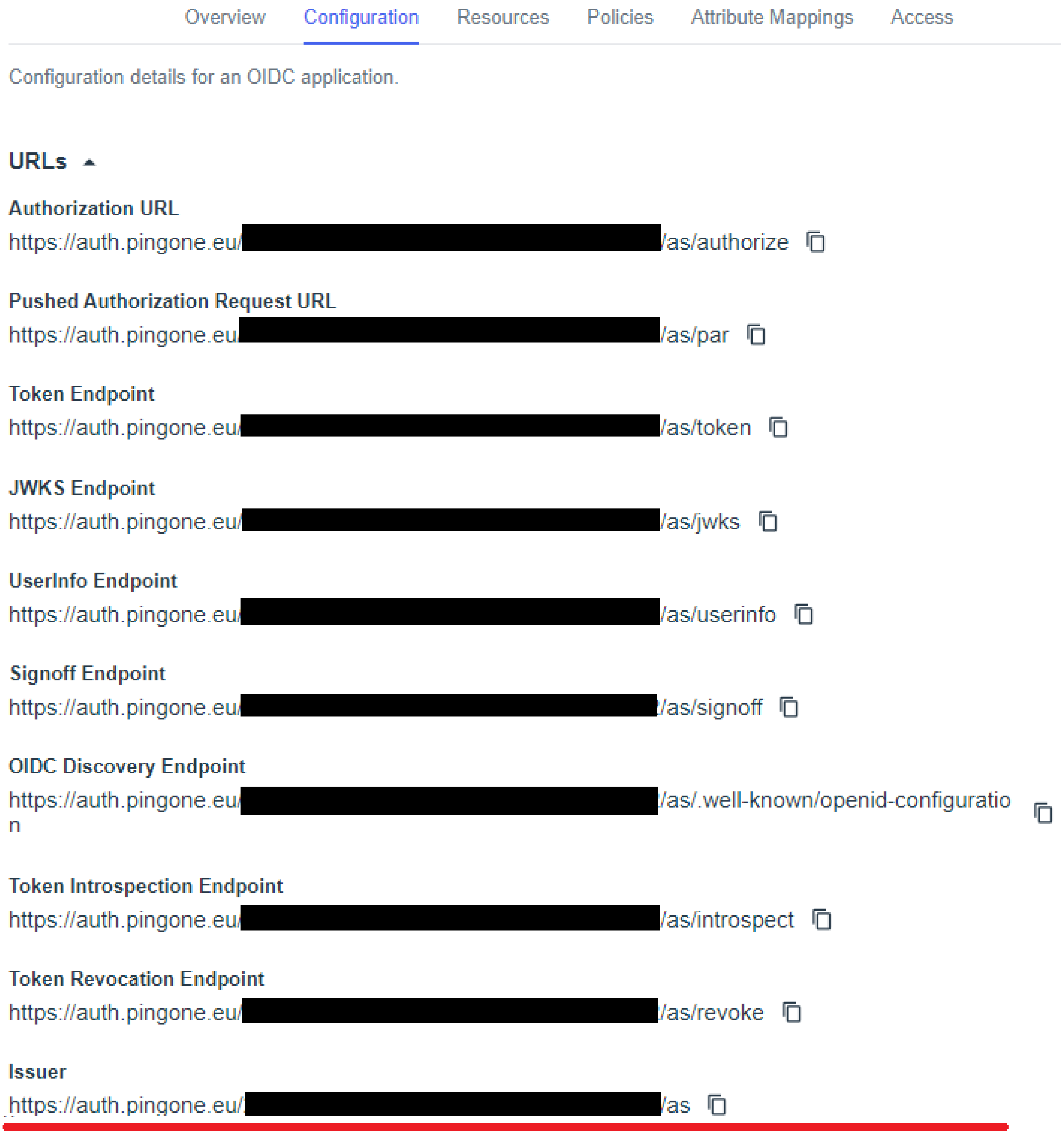
Client ID
[redacted]

Client Secret
··································

Home Page URL
No Home Page Configured

Signon URL
Default Signon Page

5) Next open the Configuration tab, and expand the URLs section.
TEOS needs to know the Issuer URL, so for this copy the last url:
Issuer: https://auth.pingone.eu/<Environment-ID>/as



Configuration details for an OIDC application.

URLs ▴

Authorization URL
https://auth.pingone.eu/[redacted]/as/authorize

Pushed Authorization Request URL
https://auth.pingone.eu[redacted]/as/par

Token Endpoint
https://auth.pingone.eu[redacted]/as/token

JWKS Endpoint
https://auth.pingone.eu/[redacted]/as/jwks

UserInfo Endpoint
https://auth.pingone.eu[redacted]/as/userinfo

Signoff Endpoint
https://auth.pingone.eu[redacted]/as/signoff

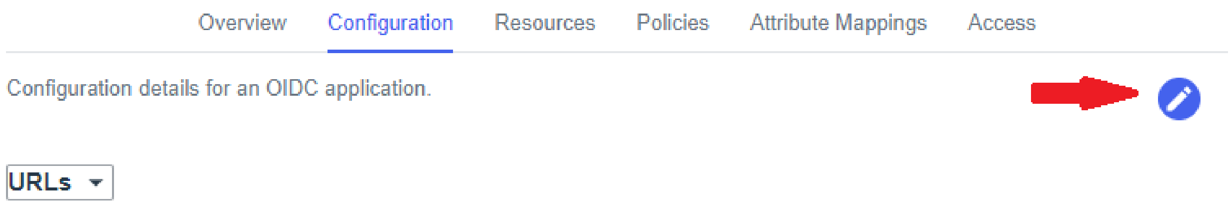
OIDC Discovery Endpoint
https://auth.pingone.eu[redacted]/as/.well-known/openid-configuration

Token Introspection Endpoint
https://auth.pingone.eu[redacted]/as/introspect

Token Revocation Endpoint
https://auth.pingone.eu/[redacted]/as/revoke

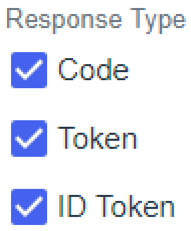
Issuer
https://auth.pingone.eu/[redacted]/as

6) After copying the URL, press the edit button on the right of the page.



Configuration details for an OIDC application.

a. For Response Type, enable all 3 items
   i. Code
   ii. Token
   iii. ID Token



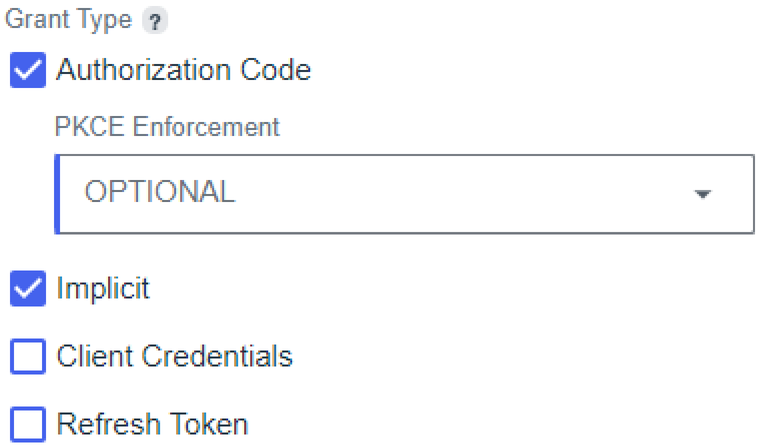
Response Type

☑ Code

☑ Token

☑ ID Token

b. Grant type keep as default on Authorization code enabled: OPTIONAL. And the option implicit enabled.



Grant Type

☑ Authorization Code

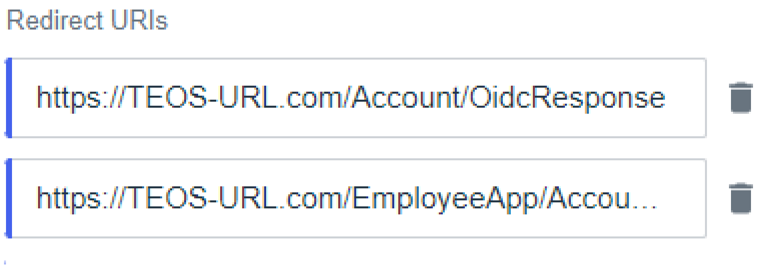
PKCE Enforcement: OPTIONAL

☑ Implicit

□ Client Credentials

□ Refresh Token

c. Enter the two redirect URLs you can find in TEOS. These URLs are (replace TEOS-URL.com with your own domainname):
- https://TEOS-URLcom/Account/OidcResponse
- https://TEOS-URLcom/EmployeeApp/Account/OidcResponse
-

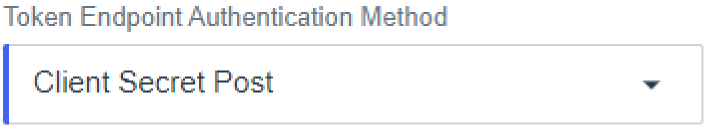


Redirect URIs

https://TEOS-URL.com/Account/OidcResponse

https://TEOS-URL.com/EmployeeApp/Accou…

d. Next change the Token Endpoint Authentication Method to “Client Secret Post”

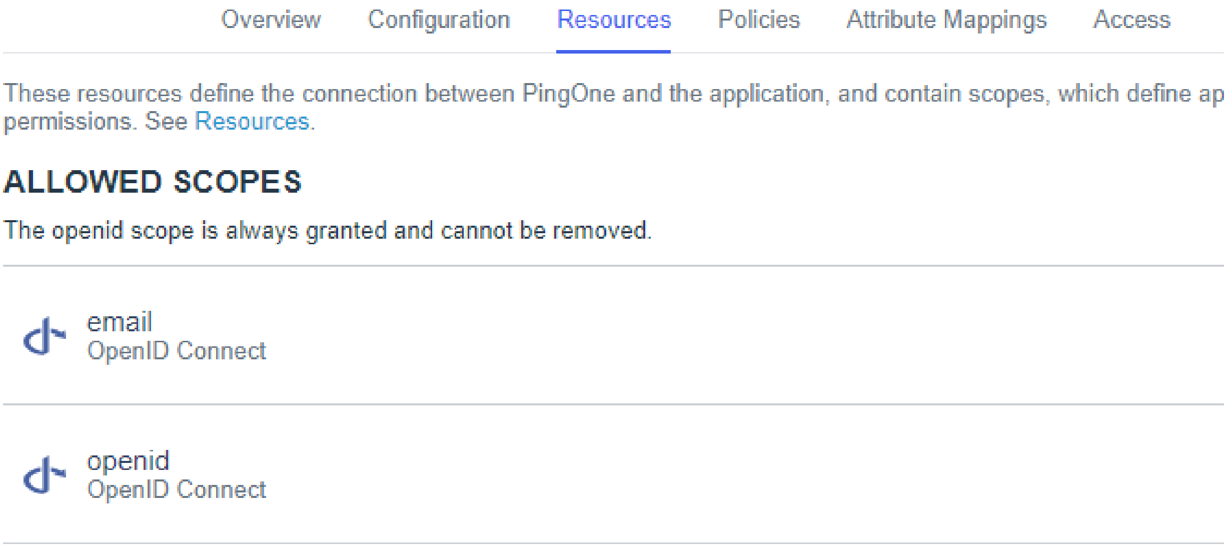


Token Endpoint Authentication Method

Client Secret Post

After this last setting, scroll down and press Save.

7) Following on the resource tab, add the resource: email. The resource for openid is added by default already. Afterwards it will look like this:



These resources define the connection between PingOne and the application, and contain scopes, which define ap permissions. See Resources.

ALLOWED SCOPES

The openid scope is always granted and cannot be removed.

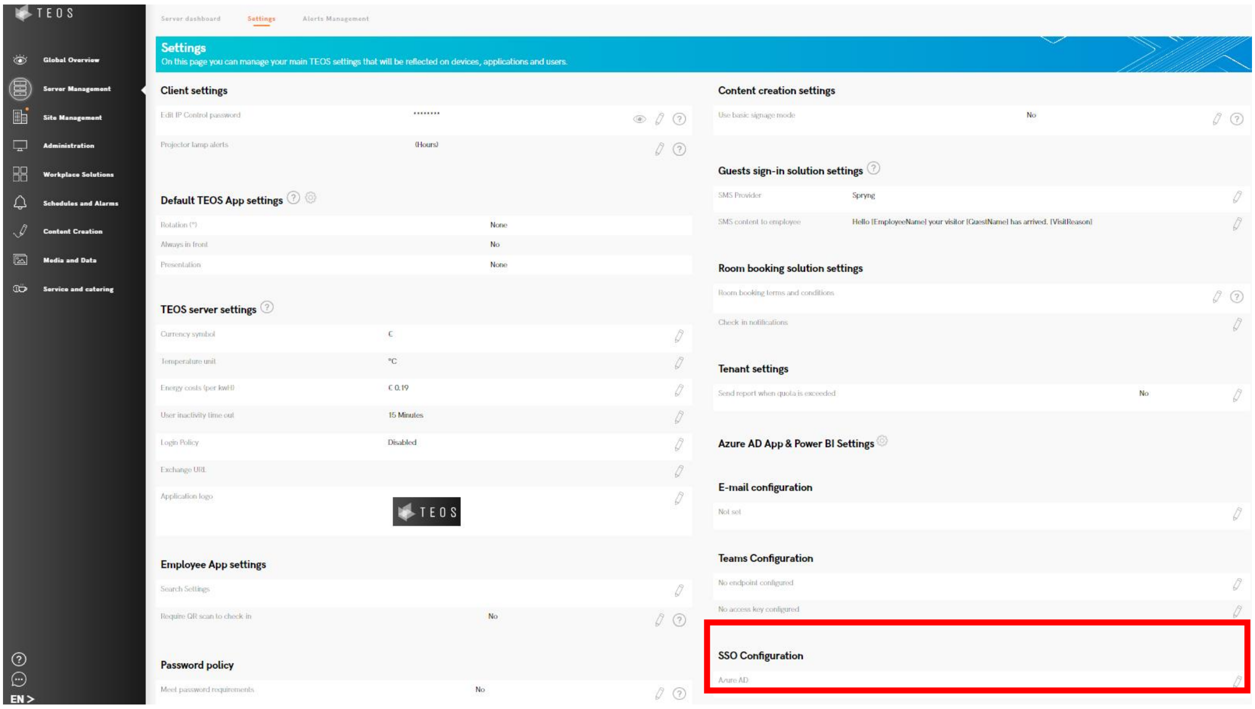
email
OpenID Connect

openid
OpenID Connect

6.2 Configuration under TEOS

After making sure you have all your users including admin users, Go to server management > settings.

Under settings from Version 3.2.1 you can find the option in Servermanagement -> Settings., click on the pencil to edit it



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	15 Minutes
Login Policy	Disabled
Exchange URL	
Application logo	TEOS

Employee App settings

Search Settings	
Require QR scan to check in	No

Password policy

Meet password requirements	No

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

Check in notifications

Tenant settings

Send report when quota is exceeded	No

Azure AD App & Power BI Settings

E-mail configuration

Not set

Teams Configuration

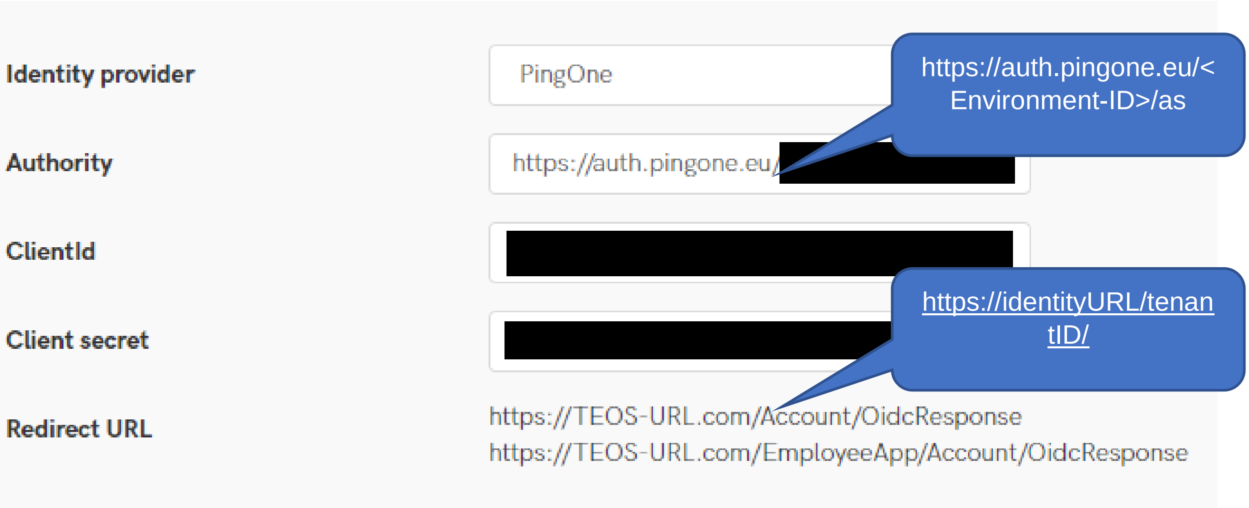
No endpoint configured

No access key configured

SSO Configuration

Azure AD

Within this section you will be able to select Azure AD (or Entra ID) as Identity provider or Ping One as another identity provider. As an example below the PingOne configuration will be done base on Ping Identity configuration.



Identity provider	PingOne
Authority	https://auth.pingone.eu/[redacted]
ClientId	[redacted]
Client secret	[redacted]
Redirect URL	https://TEOS-URL.com/Account/OidcResponse https://TEOS-URL.com/EmployeeApp/Account/OidcResponse

https://auth.pingone.eu/<Environment-ID>/as

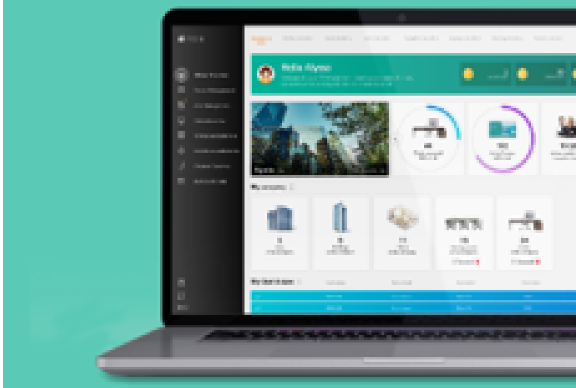
https://identityURL/tenantID/

Make sure on your identity provider, the redirect URL are copied from your own TEOS tenant name.

You need then to add the authority of the Identity provider in TEOS SSO configuration tab (this mainly includes the URL of the identity provider and the Client ID and Secret . After filling the URL, ID and secret from the application created above, Click save on the right top page.

Log off and try to login again, the SSO access must be directly active, and the admin local account should not be accessible anymore.

If any issue on configuration happens, contact us to supprt@teos.support



Visit us on

https://teos.solutions

© 2024 Sony Corporation