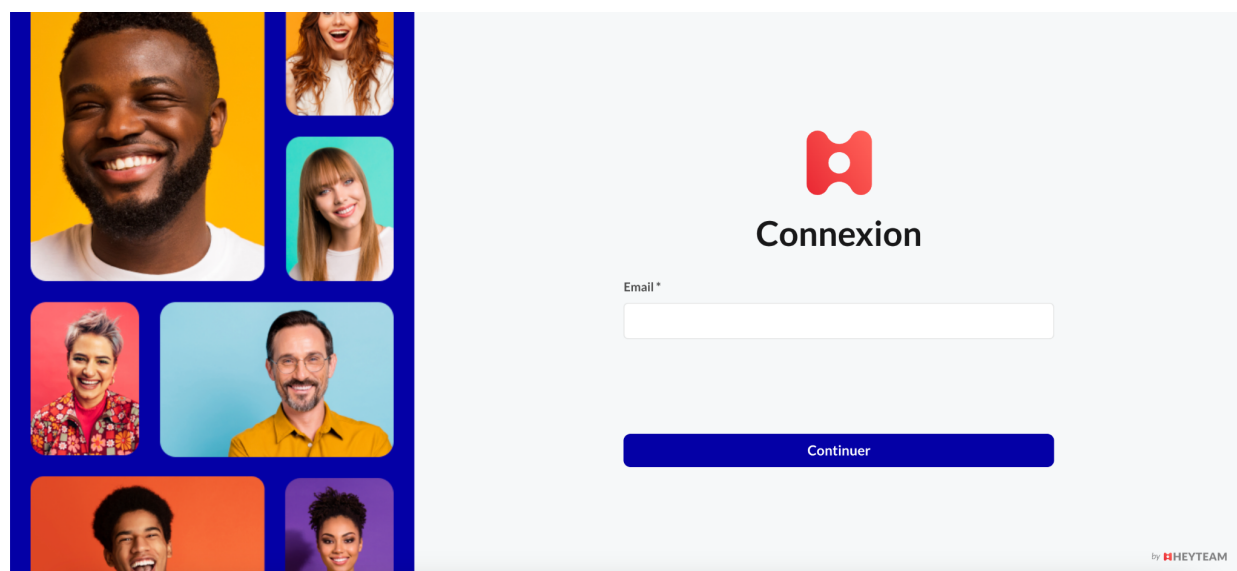


Mise en place du SSO

Microsoft Azure

Son fonctionnement

Pour se connecter via SSO, il faut se connecter via son adresse email professionnelle sur la page de connexion.



La redirection vers votre portail de connexion SSO sera alors effectuée automatiquement.

À noter : Une fois la première connexion effectuée sur votre portail SSO, celui-ci n'apparaîtra plus aux yeux de l'utilisateur et la connexion vers HeyTeam se fera directement.

Pour les nouveaux collaborateurs :

- Un nouveau collaborateur se connecte sur la plateforme HeyTeam via son adresse email personnelle jusqu'à son "jour d'arrivée dans l'entreprise + 1" (cette date est paramétrable sur la plateforme).
- Un passage vers l'adresse professionnelle est automatiquement fait à partir de cette date.

Cela signifie que dans un premier temps le nouveau collaborateur n'aura pas accès au SSO. Il devra créer un mot de passe et se connecter à HeyTeam de manière classique avec son adresse email personnelle.

Autres utilisateurs :

- Excepté les nouveaux collaborateurs, les utilisateurs invités sur HeyTeam se connectent directement avec leur adresse professionnelle, permettant d'accéder dès la première connexion au SSO mis en place.

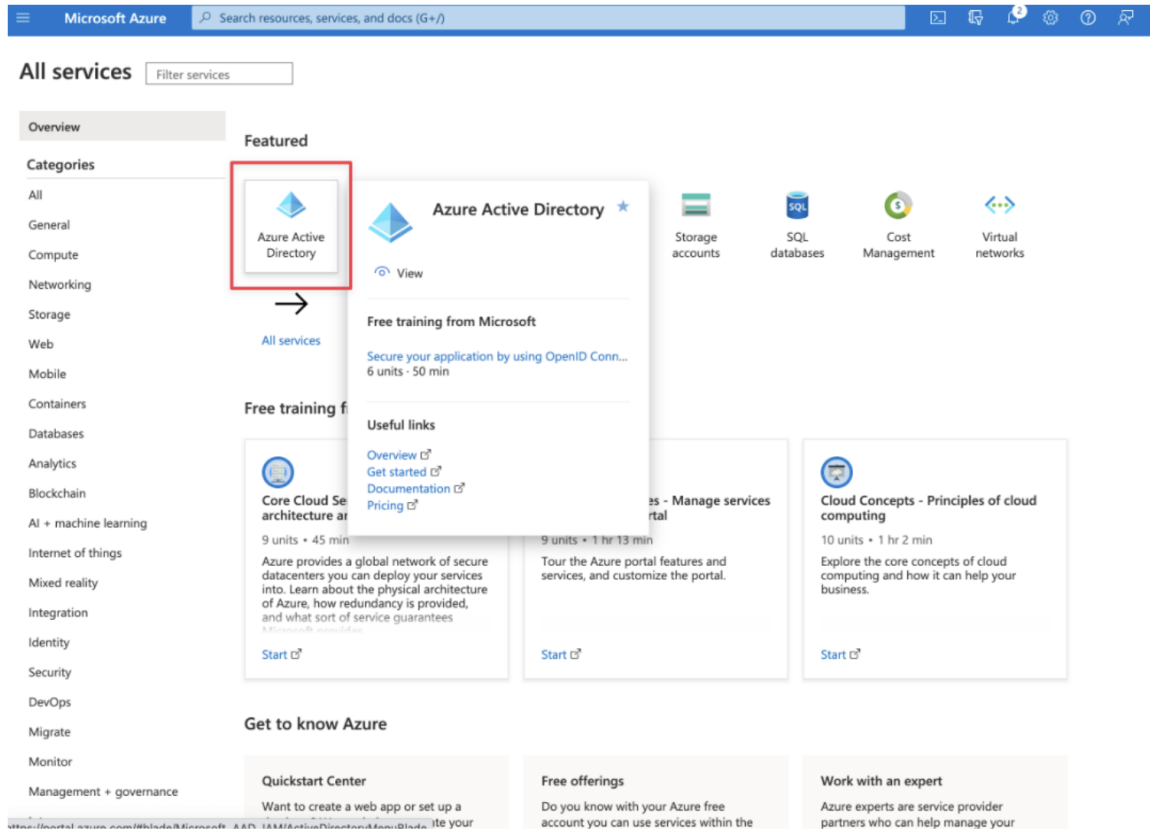
Lors de la première connexion à HeyTeam via le SSO :

- L'onglet "Mot de Passe" dans la section "Mon Compte" n'apparaît plus sur la plateforme HeyTeam. La section "Création du mot de passe" lors de la première connexion disparaît également.

Sa mise en place

Microsoft AZURE

1. Dans “All services”, cliquez sur “Azure”



2. Créer une nouvelle application

The screenshot shows the Microsoft Azure portal interface. At the top, the header includes the Microsoft Azure logo and a search bar. Below the header, the breadcrumb trail reads 'All services > Répertoire par défaut'. The main heading is 'Répertoire par défaut | App registrations'. The left sidebar contains a 'Manage' section with various links, including 'App registrations', which is highlighted with a red box. In the top navigation bar, the 'New registration' button is also highlighted with a red box. A red arrow points from the 'App registrations' link in the sidebar to the 'New registration' button. The main content area shows a message about the new App registrations search preview and a table of applications. The table has columns for 'Display name', 'Application (client) ID', and 'Created on'. Below the table, there are two buttons: 'View all applications in the directory' and 'View all applications from personal account'.

3. Remplir les paramètres de l'application :

Name : HeyTeam

Redirect URI : vous a été communiqué par HeyTeam. Elle est toujours dans le format suivant <https://<domaine>.heyteam.com/openid>

Microsoft Azure

Search resources, services, and docs (G+)

[All services](#) > [Répertoire par défaut](#) >

Register an application ...

* Name

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

HeyTeam ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Répertoire par défaut 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 ▼

https://kurmi.heyteam.com/openid ✓

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](#)

Register

4. **Une fois l'application créée, ajouter un client secret**
"Client credential" > Ajouter un nouveau client secret

Microsoft Azure Search resources, services, and docs (G+)

All services > Répertoire par défaut >

HeyTeam

Search (Cmd+/) Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Essentials

Display name : HeyTeam

Application (client) ID : e34abaf3-a8e5-4944-8536-a6a9d0f2855b

Object ID : c3bd45f5-ee2e-456f-b9a3-4c26741739e7

Directory (tenant) ID : c2cc16f2-b797-4542-a836-7ebb2d5f0eb3

Supported account types : My organization only

Client credentials : Add a certificate or secret

Redirect URIs : 1 web, 0 spa, 0 Add a certificate or secret

Application ID URI : Add an Application ID URI

Managed application in L... : HeyTeam

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 security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

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](#)

Call APIs

Sign in users in 5 minutes

Configure for your organization

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

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

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys

Upload certificate

Thumbprint	Start date	Expires	Certificate
No certificates have been added for this application.			

Client secrets

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.			

Preciser ensuite la durée de validité et vous pouvez ensuite valider.

Add a client secret

Description: Secret key

Expires: 24 months

5. Il est temps ensuite de copier les données dans l'interface HeyTeam.

Vous aurez besoin de :

- Client ID
- Client Secret
- Le "well-known"

a. Le client ID se trouve dans le champ "Application (client) ID" :

All services > Répertoire par défaut > HeyTeam

Search (Cmd+/)

Delete Endpoints Preview features

Overview

Quickstart Integration assistant

Manage

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

Support + Troubleshooting Troubleshooting New support request

Essentials

Display name : HeyTeam

Application (client) ID : e34abaf3-a8e5-4944-8536-af9d0f2855b

Object ID : c3bd45f5-ee2e-456f-b9a3-4c26741739e7

Directory (tenant) ID : c2cc16f2-b797-4542-a836-7ebb2d5f0eb3

Supported account types : My organization only

Client credentials : 0 certificate, 1 secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in L... : HeyTeam

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. Applications will need to 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](#)

b. Le secret ID se trouve dans la partie Certificates :

All services > Répertoire par défaut > HeyTeam

HeyTeam | Certificates & secrets

Search (Cmd+/) Got feedback?

Overview Quickstart Integration assistant

Manage

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

Support + Troubleshooting

- Troubleshooting
- New support request

Certificates

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.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID
No certificates have been added for this application.			

Client secrets

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 key	10/18/2023	zuq7Q~FGHjdm1UxXKrdW/hk8z... 1fa7c7ee-99b-4778-8d94-2f6ee1ad9b86

Copy to clipboard

c. L'authentification URI, le token URI ainsi que le User URI se trouvent dans vos metadata via le lien du .well_known.

Ces informations sont accessibles dans la partie "Overview" > "Endpoints".

Pour récupérer les 3 liens, vous pouvez faire une recherche des 3 informations :

- Auth uri = l'url se termine par "/authorize"
- Token uri = l'url se termine par "/token"
- User uri = l'url se termine par "userinfo"

All services > Répertoire par défaut > HeyTeam

HeyTeam

Search (Cmd+/) Delete Endpoints Preview features

Overview

- Quickstart
- Integration assistant

Manage

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

Support + Troubleshooting

- Troubleshooting
- New support request

Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/v2.0/.well-known/openid-configuration

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

Federation metadata document
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/federationmetadata/2007-06/federationmetadata.xml

WS-Federation sign-on endpoint
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/wsfed

SAML-P sign-on endpoint
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/saml2

SAML-P sign-out endpoint
https://login.microsoftonline.com/c2cc16f2-b797-4542-a836-7ebb2d5f0eb3/saml2

Copy to clipboard

6. Dans HeyTeam, se rendre dans Paramètres > Sécurité & confidentialité > SSO



← Retour au menu

Utilisateurs

Rôles

Entités

Plateforme

Page(s) entreprise

Notifications

Chatbot d'accueil

Communication

Langues

Intégration

Analyse de données

Sécurité & confidenti...

Champs personnalis...

Logs

Erwan

Rechercher

NAME

Mot de passe

SSO

Temps de session

Membres d'équipe

Suppression des données

Double authentification (2FA)

SSO

Activer

Choisissez votre plateforme de gestion des identités

Microsoft

Auth uri *

https://login.microsoftonline.com/common/oauth2/v2.0/authorize

Token uri *

https://login.microsoftonline.com/common/oauth2/v2.0/token

User uri *

https://graph.microsoft.com/oidc/userinfo

Scope *

openid profile email

Client id *

your-client-id

Client secret *

Domains Optionnel

7. Sélectionner ensuite le service “Microsoft”

SSO

×

Activer

Choisissez votre plateforme de gestion des identités

Google

Microsoft

Adfs

ForgeRock

Okta

PingFederate

Prco

Scope *

8- Puis copier-coller les informations de Microsoft Azure sur HeyTeam en renseignant :

- Auth uri : à récupérer dans le .well_known
- Token uri : à récupérer dans le .well_known
- User uri : à récupérer dans le .well_known
- Scope : toujours indiquer : “openid profile email”
- Client ID : à récupérer directement dans vos endpoint
- Client Secret : à récupérer directement dans vos endpoint

Vous pouvez également rajouter de manière optionnelle un domaine, par exemple heyteam.com. Cela veut dire que toutes les adresses mail se terminant avec ce nom de domaine seront associées au SSO.

9- Vous pouvez cliquer sur “Tester la configuration” pour vous assurez que tout est OK.