

DOCUMENTATION / SUPPORT DE FORMATION



Table des matières

Authentifications externes	3
Authentification Google Apps	3
Authentification Office 365	4
Authentification Azure Active Directory (Office 365 enterprise)	4
Authentification via le portail Web	5
Authentification via les applications mobile	9

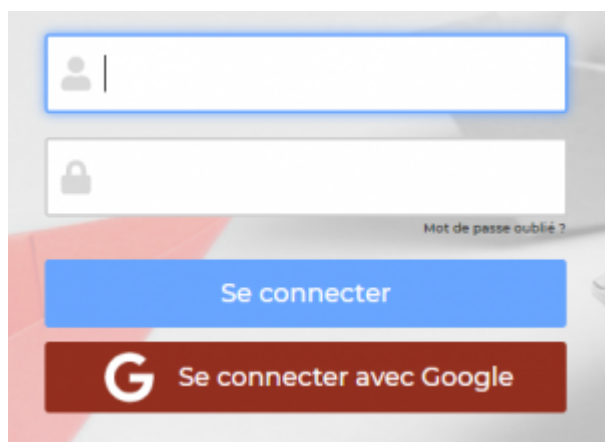
Authentifications externes

L'application vous permet d'utiliser un système externe pour l'authentification de vos utilisateurs.

Plusieurs modes d'authentification sont disponibles

- Authentification Google Apps
- Authentification Office 365 directe
- Authentification Azure Active Directory (fonctionne avec Office 365 enterprise)

Authentification Google Apps



L'application vous permet d'utiliser Google Apps pour authentifier les utilisateurs. Cette méthode est possible uniquement si vous disposez d'un domain Google Apps pour gérer vos email d'entreprise.

Cette méthode permet à vos utilisateur de ne pas avoir à mémoriser ou gérer un autre identifiant et mot de passe pour l'accès à l'application.

L'authentification est intégralement gérée par Google via le protocole oauth 2.0.

Pour activer l'authentification Google Apps

1. Contacter le support Veryswing directement depuis l'application en demandant l'activation de ce mode d'authentification dans votre environnement.
2. Nous faisons ensuite l'activation pour vous et nous faisons le nécessaire auprès de Google
3. Une fois ce mode d'authentification activée, une image rouge "Se connecter avec Google" apparait sur l'écran de connexion
4. Il est nécessaire de changer le mode d'authentification de vos utilisateurs depuis l'écran Administration > Utilisateur

Dans le formulaire, vous devez choisir explicitement le mode d'authentification Google dans le formulaire de gestion de l'utilisateur. Il existe également une action de masse pour le faire sur plusieurs utilisateurs en même temps.

Une fois l'authentification Google activée sur un utilisateur, il doit obligatoire cliquer sur le bouton "Se

connecter avec Google” pour accéder à l'application. Il sera alors redirigé vers le site Google qui gère l'authentification puis redirigé vers l'application.

Authentification Office 365

L'application vous permet également d'utiliser Office 365 pour authentifier vos utilisateurs.

Si vous disposez d'un abonnement Office 365 qui n'est pas de la famille Enterprise (donc que vous ne disposez pas d'un annuaire Azure Active Directory)

1. demandez l'activation de l'authentification Office 365 auprès du support directement depuis le formulaire support dans l'interface de l'application
2. Nous faisons ensuite l'activation pour vous
3. Une fois activé, il est nécessaire de changer le mode d'authentification de vos utilisateurs depuis l'écran Administration > Utilisateur

Vos utilisateurs qui utilisent ce mode d'authentification devront continuer à utiliser les zones identifiant et mot de passe de la page de connexion à l'application. Ils devront saisir leur identifiant et mot de passe office 365.



Attention, ce mode d'authentification n'est pas compatible avec l'authentification double facteur proposée par Microsoft. Si vous activez l'authentification double facteur, vous ne pourrez plus vous connecter à l'application. Seule l'authentification avec Azure Active Directory fonctionne avec la double authentification.

Authentification Azure Active Directory (Office 365 enterprise)

Si vous disposez d'un abonnement Azure avec Active Directory ou Office 365 enterprise, vous pouvez disposer d'une authentification sécurisée via Azure Active Directory.

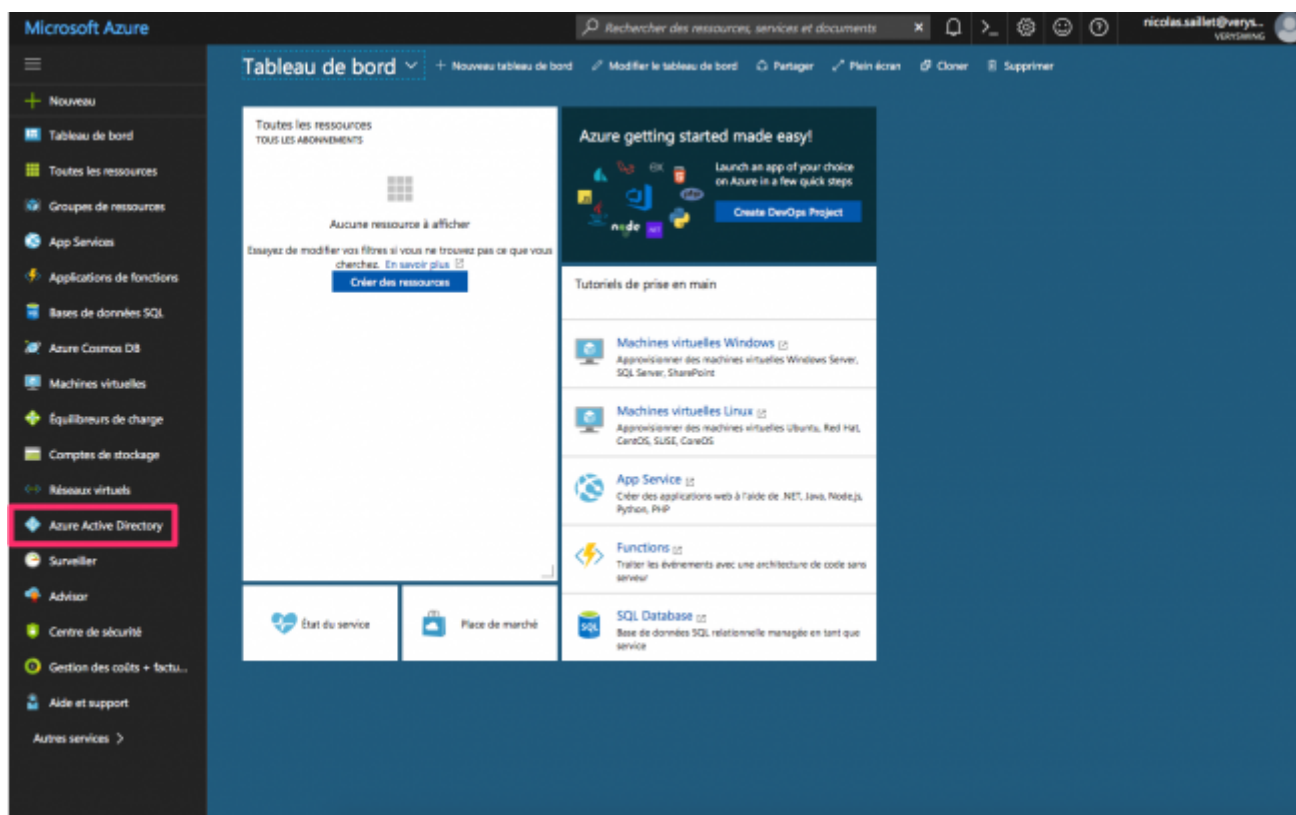
Cette méthode permet à vos utilisateurs de ne pas avoir à mémoriser ou gérer un autre identifiant et mot de passe pour l'accès à l'application.

L'authentification est intégralement gérée par Microsoft via le protocole oauth 2.0 sur la plateforme Azure.

Vous trouverez ci-dessous les différentes étapes pour activer ce mode d'authentification pour le portail Web et ensuite pour les applications mobiles.

Authentification via le portail Web

Depuis la console Azure Management



Depuis votre console Azure, cliquez sur ACTIVE DIRECTORY dans les items à gauche.

Une fois dans la zone active directory, cliquez sur le tenant qui devra permettre l'authentification dans l'application.

Cliquez ensuite sur l'onglet APPLICATIONS.

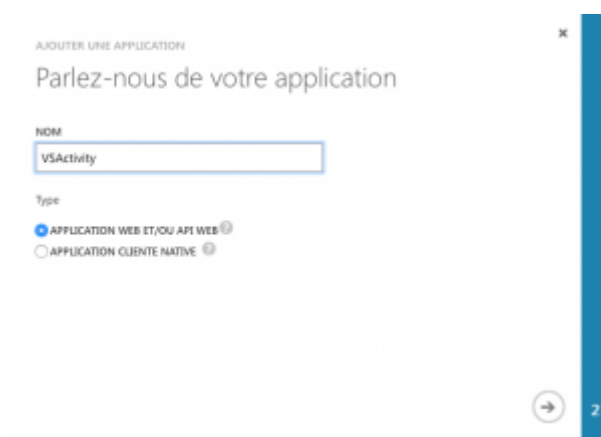
Cliquez sur AJOUTER+ en bas de l'interface pour ajouter une application à votre tenant Azure AD. Choisir "Ajouter une application développée par mon organisation".

Que souhaitez-vous faire ?

➔ Ajouter une application développée par mon organisation

➔ Ajouter une application à partir de la galerie

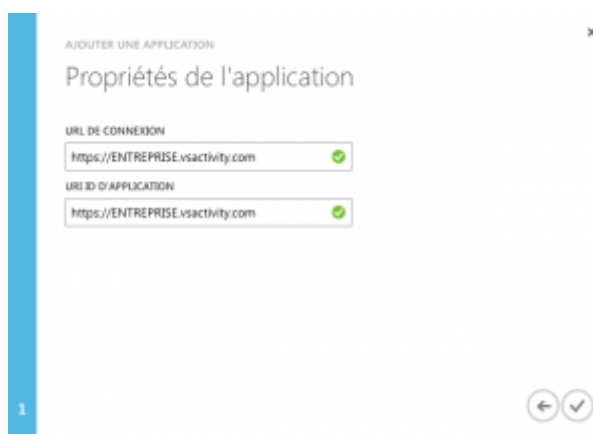
Indiquez le nom de l'application, VSActivity. Laissez cocher la case "APPLICATION WEB ET/OU API WEB".



Indiquez l'url de votre environnement VSA dans le formulaire suivant :
<https://ENTREPRISE.vsactivity.com>

Remplacez ENTREPRISE par le préfixe de l'url d'accès à votre environnement.

Idem dans le champ URI ID D'APPLICATION. <https://ENTREPRISE.vsactivity.com>



Une fois l'application créée, cliquez sur l'onglet CONFIGURER.

Allez jusqu'à **clés**.

Choisissez 2 ans.



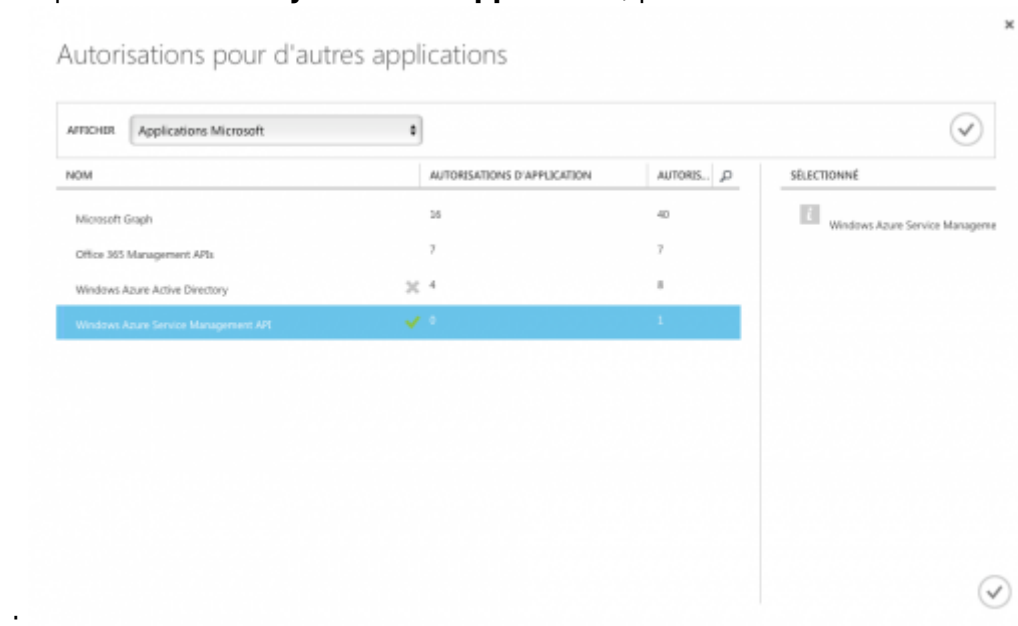
	VALIDE DEPUIS	EXPIRE LE	LA VALEUR DE LA CLÉ S'AFFICHERA APRÈS SON ENREGISTREMENT
2 années	01/12/2015	01/12/2017	LA VALEUR DE LA CLÉ S'AFFICHERA APRÈS SON ENREGISTREMENT

Attention la clé sera générée à l'enregistrement et n'apparaîtra qu'une seule fois. Il sera nécessaire de la sauvegarder pour nous la communiquer. Il sera ensuite impossible de la voir à nouveau.

Allez ensuite au bloque **URL DE RÉPONSE**

Indiquez l'url suivante : <https://entreprise.vsactivity.com/common/azuread/callback.php>

Cliquez ensuite sur **Ajouter une application**, puis cochez Windows Azure Services Management API



Cliquez ensuite ENREGISTRER en bas de l'interface. Le console va travailler quelques secondes.

Une fois l'enregistrement effectué, la clé secrète apparaitra au niveau de **clés**, il faut la copier et l'enregistrer ailleurs pour pouvoir nous la communiquer.

Les informations à nous communiquer

Une fois l'application ajoutée dans votre console Azure, il est nécessaire de nous communiquer :

- L'id de l'application disponible dans l'onglet **CONFIGURER ID CLIENT**
- La clé secrète
- Le point de terminaison de jeton oauth 2.0, il est disponible en cliquant sur **POINT DE TERMINAISON** en base de l'interface quand vous êtes dans l'onglet CONFIGURER de l'application

Points de terminaison d'app

Si vous développez une application qui s'intègre à Microsoft Azure AD, mettez votre code à jour afin d'utiliser ces points de terminaison pour l'authentification unique et l'accès aux annuaires.

DOCUMENT DE MÉTADONNÉES DE FÉDÉRATION ?

<https://login.microsoftonline.com/4b118114-a79b-4d78-96d1-d74c9c23b464>

POINT DE TERMINAISON DE CONNEXION WS-FEDERATION ?

<https://login.microsoftonline.com/4b118114-a79b-4d78-96d1-d74c9c23b464>

POINT DE TERMINAISON DE CONNEXION SAML-P ?

<https://login.microsoftonline.com/4b118114-a79b-4d78-96d1-d74c9c23b464>

POINT DE TERMINAISON DE DÉCONNEXION SAML-P ?

<https://login.microsoftonline.com/4b118114-a79b-4d78-96d1-d74c9c23b464>

POINT DE TERMINAISON DE L'API MICROSOFT AZURE AD GRAPH ?

<https://graph.windows.net/4b118114-a79b-4d78-96d1-d74c9c23b464>

POINT DE TERMINAISON DE JETON OAUTH 2.0 ?

<https://login.microsoftonline.com/4b118114-a79b-4d78-96d1-d74c9c23b464>

POINT DE TERMINAISON D'AUTORISATION OAUTH 2.0 ?

<https://login.microsoftonline.com/4b118114-a79b-4d78-96d1-d74c9c23b464>

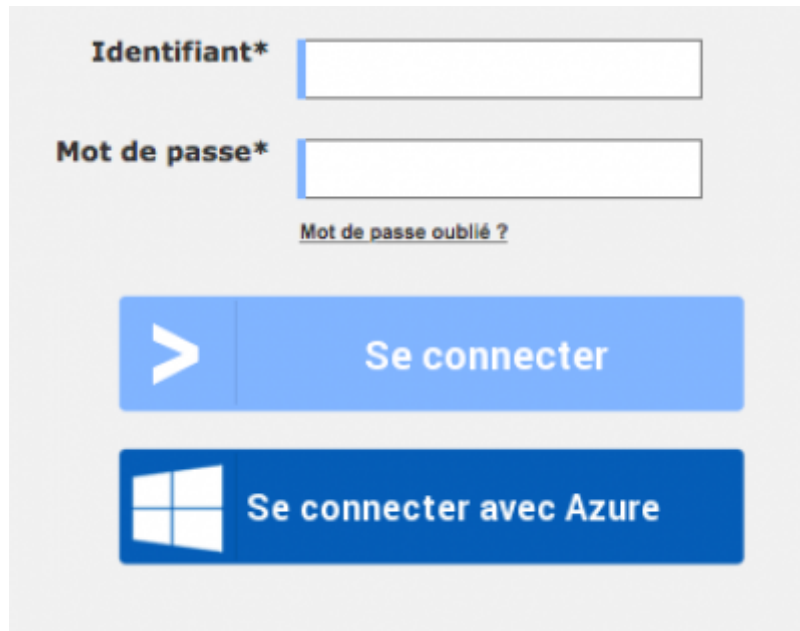


Une fois que le mode d'authentification Azure AD est activé

Il est nécessaire de changer le mode d'authentification de vos utilisateurs depuis l'écran Administration > Utilisateur

Dans le formulaire, vous devez choisir explicitement le mode d'authentification Azure Active Directory dans le formulaire de gestion de l'utilisateur. Il existe également une action de masse pour le faire sur plusieurs utilisateurs en même temps.

Une fois l'authentification Azure Active Directory activée sur un utilisateur, il doit obligatoirement cliquer sur le bouton "Se connecter avec Azure" pour accéder à l'application. Il sera alors redirigé vers le site Microsoft qui gère l'authentification puis redirigé vers l'application.




Identifiant*

Mot de passe*

[Mot de passe oublié ?](#)

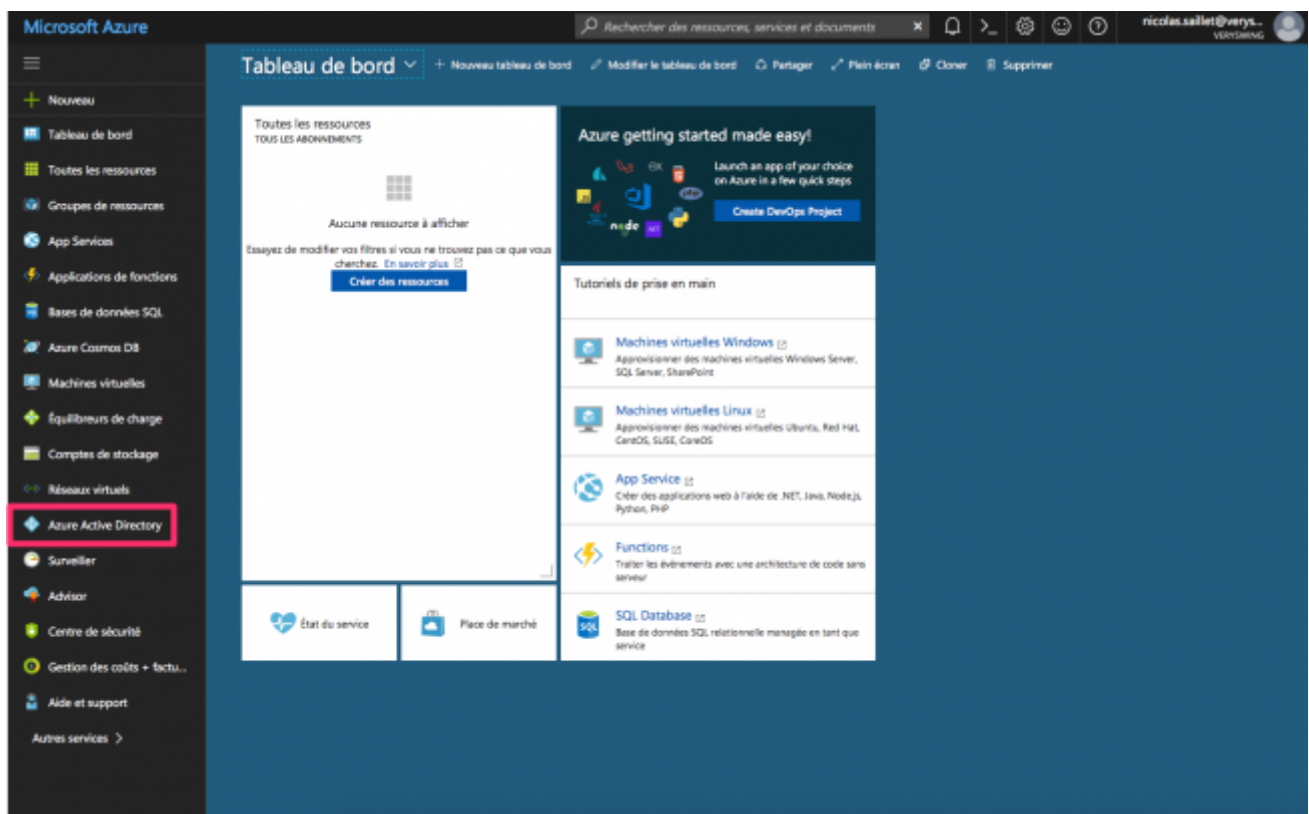
> Se connecter

 Se connecter avec Azure

Authentification via les applications mobile

Avant d'activer l'authentification Azure Active Directory pour les applications mobiles VSActivity, il est essentiel d'avoir tout d'abord activé l'authentification pour l'interface Web.

Depuis la console Azure Management



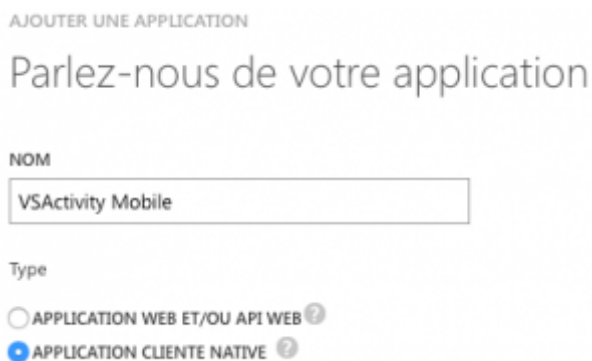
Depuis votre console Azure, cliquez sur ACTIVE DIRECTORY dans les items à gauche.

Une fois dans la zone active directory, cliquez sur le tenant **où vous avez ajouté l'authentification Azure Active Directory pour la partie Web**.

Cliquez ensuite sur l'onglet APPLICATIONS.

Cliquez sur AJOUTER+ en bas de l'interface pour ajouter une application à votre tenant Azure AD. Choisir "Ajouter une application développée par mon organisation".

Indiquez le nom de l'application, VSActivity Mobile. Cocher la case "APPLICATION CLIENTE NATIVE".



AJOUTER UNE APPLICATION

Parlez-nous de votre application

NOM

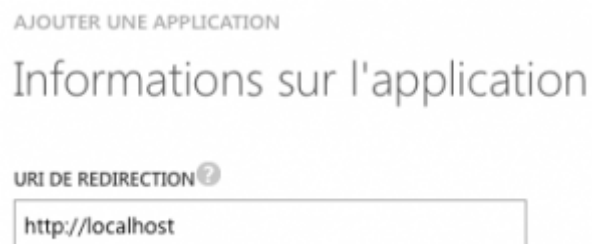
VSActivity Mobile

Type

☐ APPLICATION WEB ET/OU API WEB ?

☒ APPLICATION CLIENTE NATIVE ?

Indiquez l'url suivant dans le formulaire : <http://localhost>



AJOUTER UNE APPLICATION

Informations sur l'application

URI DE REDIRECTION ?

http://localhost

Une fois l'application créée, cliquez sur l'onglet CONFIGURER.

Cliquez ensuite sur **Ajouter une application**, puis cochez Windows Azure Services Management API

Autorisations pour d'autres applications

AFFICHER Applications Microsoft

NOM	AUTORISATIONS D'APPLICATION	AUTORIS...	SÉLECTIONNÉ
Microsoft Graph	36	40	
Office 365 Management APIs	7	7	
Windows Azure Active Directory	4	8	
Windows Azure Service Management API	0	1	Windows Azure Service Manageme

Cliquez ensuite ENREGISTRER en bas de l'interface. Le console va travailler quelques secondes.


Les informations à nous communiquer

Une fois l'application ajoutée dans votre console Azure, il est nécessaire de nous communiquer :

- L'id de l'application disponible dans l'onglet CONFIGURER **ID CLIENT**

Une fois que le mode d'authentification Azure AD est activé

Une fois activé, tous les utilisateurs ayant le mode d'authentification "Azure Active Directory" pourront s'authentifier avec leurs comptes Microsoft Azure Active Directory sur nos applications mobiles. L'utilisateur devra obligatoirement cliquer sur le bouton "Se connecter avec Azure" pour accéder à l'application. Il sera alors redirigé vers le site Microsoft qui gère l'authentification puis redirigé vers l'application.

 Se connecter avec Azure

Identifiant

Mot de passe

Authentification