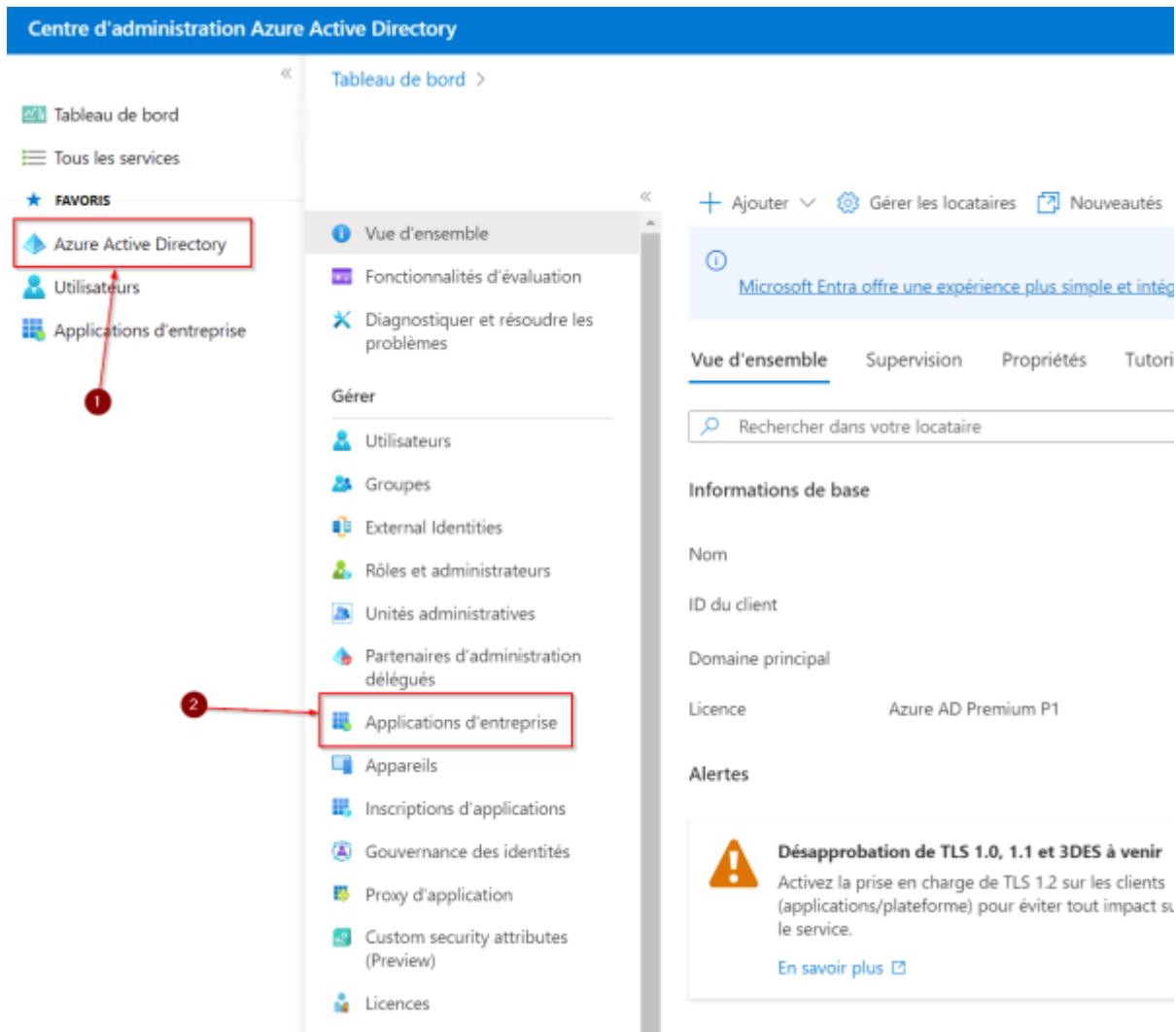


Microsoft Office 365

We're going to look at how to create and retrieve the elements needed to create a link between your ESIA system and Microsoft Office365.

Creating the application

Once you have logged into your Azure Active Directory administration centre. Click on “Azure Active Directory” and then on “Enterprise Applications”.



The screenshot shows the Azure Active Directory administration center. The left sidebar has a 'FAVORIS' section with 'Azure Active Directory' (highlighted with a red box and a red arrow labeled 1), 'Utilisateurs', and 'Applications d'entreprise'. The main content area shows 'Vue d'ensemble' with a 'Microsoft Entra offre une expérience plus simple et intégrée' message. Below it is the 'Applications d'entreprise' section, which is also highlighted with a red box and a red arrow labeled 2. The 'Vue d'ensemble' tab is selected. The 'Informations de base' section shows 'Nom' (empty), 'ID du client' (empty), 'Domaine principal' (empty), 'Licence' (Azure AD Premium P1), and an 'Alertes' section with a warning about TLS deprecation.

Then click on “New application”.

Affichez, filtrez et recherchez les applications de

La liste des applications conservées par votre orga

Rechercher par nom d'application ou par ...

Now go to “Create your own application”.

Créer votre propre application

Des commentaires ?

La galerie d'applications Azure

Rechercher dans l'application

Authentification unique : Tout

Gestion du compte utilisateur : All

Catég

Plateformes cloud

Amazon Web Services (AWS)

Google Cloud Platform

Ora

Ajouter une application locale

Configurer le proxy d'application Azure AD pour activer l'accès à distance sécurisé.

En savoir plus sur le proxy d'application

Découvrez comment utiliser le proxy d'application pour fournir un accès à distance sécurisé à vos applications locales.

SSO fédéré

Approvisionnement

Applications principales

Adobe Identity

Atlassian Cloud

AWS S

Enter the name of your application and tick the box “Register an application to integrate with Azure AD (app you are developing)”. Even if your interface is in French, this option is currently untranslated (10 October 2022).

Then click on “Create”.

Créer votre propre application

X

 Des commentaires ?

Si vous développez votre propre application, utilisez Proxy d'application ou souhaitez intégrer une application qui ne figure pas dans la galerie, vous pouvez créer votre propre application ici.

Quel est le nom de votre application ?

Esia



Que voulez-vous faire avec votre application ?

- Configurer le proxy d'application pour un accès à distance sécurisé à une application locale
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Nous avons trouvé les applications suivantes qui peuvent correspondre à votre entrée

Nous vous recommandons d'utiliser les applications de la galerie quand cela est possible.



UXPressia

 LeakslD



Asite



TESMA



Salestim



Créer

Select the account type “Account in this organisation directory only (XXXXX only - Single tenant)”.

Tableau de bord > Intradel SCRL | Applications d'entreprise > Applications d'entreprise | Toutes les applications > Parcourir la galerie Azure AD >

Inscrire une application

* Nom

Nom d'affichage côté utilisateur pour cette application (il peut être modifié ultérieurement).

Esia

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

- Comptes dans cet annuaire d'organisation uniquement (uniquement - Locataire unique)
- Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire)
- Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire) et comptes Microsoft personnels (par exemple, Skype, Xbox)
- Comptes Microsoft personnels uniquement

Aidez-moi à choisir...

URI de redirection (facultatif)

Nous retournerons la réponse d'authentification à cet URI une fois l'utilisateur authentifié. Fournir ceci maintenant est facultatif et cela peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.

Selectionner une plateforme ▾ par ex, https://example.com/auth

Inscrivez ici une application sur laquelle vous travaillez. Intégrez des applications de la galerie et d'autres applications externes à votre organisation en les ajoutant à partir de [Applications d'entreprise](#).

En continuant, vous acceptez les stratégies de la plateforme Microsoft [CG](#)

[S'inscrire](#)

Now you need to configure the application permissions. Click on “Azure Active Directory”, “All application”. In the search field, enter the name of the application (here: esia) and finally click on your application.

The screenshot shows the Azure Active Directory admin center. The left sidebar has 'Azure Active Directory' as a favorite (Step 1). Under 'Manage', 'All applications' is selected (Step 2). The main area shows a search bar with 'esia' (Step 3) and a table with one application named 'ESIA' (Step 4).

Authorisations

You are now in the application overview. Click on “Authorisations”.

The screenshot shows the Azure Active Directory application overview for 'esia'. The left sidebar has 'Authorisations' highlighted (Step 1). The main area shows the 'Properties' section with 'Nom' set to 'Esia' and four 'Getting Started' steps: 1. Attribuer des utilisateurs et des groupes, 2. Provisionner des comptes d'utilisateurs, 3. Accès conditionnel, and 4. Libre-service.

Now click on “Register the application” to give it the corresponding rights.

Tableau de bord > Esia

Esia | Autorisations Application d'entreprise

Vue d'ensemble Actualiser Révision des autorisations Des commentaires ?

Autorisations

Les applications peuvent se voir accorder des autorisations d'accès à votre organisation et ses données de trois manières différentes : Par un administrateur qui autorise l'application pour tous les utilisateurs, par un utilisateur qui autorise l'application ou par les utilisateurs directement à l'application. [En savoir plus.](#)

Pour demander des autorisations supplémentaires pour cette application, utilisez [l'inscription de l'application.](#)

En tant qu'administrateur, vous pouvez donner votre consentement au nom de tous les utilisateurs de ce locataire, en veillant à ce que les utilisateurs finaux ne soient pas priés de donner leur consentement lors de l'utilisation de l'application. Cliquez sur [Accorder un consentement d'administrateur pour Intradel SCR1](#).

Consentement de l'administrateur Consentement de l'utilisateur

Rechercher dans les autorisations

Nom de l'API	Valeur de revendication	Autorisation	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated

Gérer

- Propriétés
- Propriétaires
- Rôles et administrateurs
- Utilisateurs et groupes
- Authentification unique
- Approvisionnement
- Proxy d'application
- Libre-service
- Attributs de sécurité personnalisés (préversion)

Sécurité

- Accès conditionnel
- Autorisations

Click on “Add an authorisation”.

Esia | API autorisées

Rechercher Actualiser Des commentaires ?

Autorisations configurées

La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation, utilisateur ou application.

Ajouter une autorisation Accorder un consentement d'administrateur pour

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (1)	User.Read	Activer la connexion et lire le profil utilisateur	Non	Accordé pour

Pour afficher et gérer les autorisations et le consentement de l'utilisateur, essayez [Applications d'entreprise](#).

Gérer

- Personnalisation et propriétés
- Authentification
- Certificats & secrets
- Configuration du jeton
- API autorisées
- Exposer une API
- Rôles d'application
- Propriétaires
- Rôles et administrateurs
- Manifeste

Support + dépannage

- Résolution des problèmes
- Nouvelle demande de support

Select “Office 365 management APIs”.

Demander des autorisations d'API

Sélectionner une API

API Microsoft Graph API utilisées par mon organisation Mes API

API Microsoft couramment utilisées



Microsoft Graph



Tirez parti de la grande quantité de données dans Office 365, Enterprise Mobility + Security, et Windows 10. Accédez à Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner et plus, via un seul point de terminaison.

Azure Communication Services

Expériences de communication enrichies avec la même plateforme CPaaS sécurisée que celle utilisée par Microsoft Teams

Azure DevOps

Intégrer avec Azure DevOps et Azure DevOps Server

Azure Rights Management Services

Autoriser les utilisateurs validés à lire et à écrire du contenu protégé

Azure Service Management

Accès programmatique à la plupart des fonctionnalités disponibles via le portail Azure

Data Export Service for Microsoft Dynamics 365

Exporter les données de l'organisation Microsoft Dynamics CRM vers une destination externe

Dynamics 365 Business Central

Accès programmatique aux données et fonctionnalités dans Dynamics 365 Business Central



Dynamics CRM

Accéder aux fonctionnalités des logiciels d'entreprise CRM et des systèmes ERP

Flow Service

Intégrer des modèles de flux et gérer des flux

Intune

Accès par programmation aux données Intune



Office 365 Management APIs

Récupérer les informations sur l'utilisateur, l'administrateur, le système, ainsi que les actions et les événements de stratégie à partir des journaux d'activité Office 365 et Azure AD

OneNote

Créer et gérer les notes, les listes, les images, les fichiers et plus dans les blocs-notes OneNote

Power BI Service

Accès par programmation aux ressources du Tableau de bord comme les jeux de données, les tables et les lignes dans Power BI



SharePoint

Interagir à distance avec les données SharePoint



Skype for Business

Intégrer les fonctionnalités de présence en temps réel, messagerie sécurisée, appel et conférence



Universal Print

Accès programmatique pour créer et gérer des ressources d'imprimante et de travail d'impression

Click on “Application authorisation” and select the following rights:

- ActivityFeed.Read
- ActivityFeed.ReadId

- ServiceHealth.Read

Click on “Add authorisations”.

Demander des autorisations d'API

X

[Toutes les API](#)

Office 365 Management APIs

<https://manage.office.com/> [Documents](#)

Quel type d'autorisation votre application nécessite-t-elle ?

Autorisations déléguées

Votre application doit accéder à l'API en tant qu'utilisateur connecté.

Autorisations d'application

Votre application s'exécute en tant que service en arrière-plan ou démon sans utilisateur connecté.

Sélectionner des autorisations

[développer tout](#) Commencez à taper une autorisation pour filtrer ces résultats**Autorisation**[Consentement de l'administrateur r...](#)

ActivityFeed (2)

<input checked="" type="checkbox"/> ActivityFeed.Read <small> ⓘ</small>	Read activity data for your organization	Oui
<input checked="" type="checkbox"/> ActivityFeed.ReadDlp <small> ⓘ</small>	Read DLP policy events including detected sensitive data	Oui

ServiceHealth (1)

<input checked="" type="checkbox"/> ServiceHealth.Read <small> ⓘ</small>	Read service health information for your organization	Oui
--	---	-----

[Ajouter des autorisations](#)[Abandonner](#)

Click on “Grant administrator consent”.

Tableau de bord > Esia | Autorisations > Esia

Esia | API autorisées

Rechercher | Actualiser | Des commentaires ?

Vue d'ensemble | Démarrage rapide | Assistant Intégration

Gérer

- Personnalisation et propriétés
- Authentification
- Certificats & secrets
- Configuration du jeton
- API autorisées**
- Exposer une API
- Rôles d'application
- Propriétaires
- Rôles et administrateurs
- Manifeste
- Support + dépannage
- Résolution des problèmes
- Nouvelle demande de support

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

Ajouter une autorisation Accorder un consentement d'administrateur pour

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (1)				
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	✓ Accordé pour
Office 365 Management APIs (3)				
ActivityFeed.Read	Application	Read activity data for your organization	Oui	⚠ Pas accordé pour
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Oui	⚠ Pas accordé pour
ServiceHealth.Read	Application	Read service health information for your organization	Oui	⚠ Pas accordé pour

Pour afficher et gérer les autorisations et le consentement de l'utilisateur, essayez [Applications d'entreprise](#).

Answer “yes” to apply the rights.

Confirmation d'accord de consentement d'administrateur.

Voulez-vous donner le consentement pour les autorisations demandées pour tous les comptes dans

Oui | Non

? Cette action mettra à jour les consentements administrateur existants de cette application pour qu'ils correspondent à ce qui est indiqué ci-dessous.

The permissions panel should look like this:

Tableau de bord > Esia | Autorisations > Esia

Esia | API autorisées

Rechercher | Actualiser | Des commentaires ?

Vue d'ensemble | Démarrage rapide | Assistant Intégration

Gérer

- Personnalisation et propriétés
- Authentification
- Certificats & secrets
- Configuration du jeton
- API autorisées**
- Exposer une API
- Rôles d'application
- Propriétaires
- Rôles et administrateurs
- Manifeste
- Support + dépannage
- Résolution des problèmes
- Nouvelle demande de support

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

Ajouter une autorisation Accorder un consentement d'administrateur pour

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (1)				
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	✓ Accordé pour
Office 365 Management APIs (3)				
ActivityFeed.Read	Application	Read activity data for your organization	Oui	✓ Accordé pour
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Oui	✓ Accordé pour
ServiceHealth.Read	Application	Read service health information for your organization	Oui	✓ Accordé pour

Pour afficher et gérer les autorisations et le consentement de l'utilisateur, essayez [Applications d'entreprise](#).

Repeat the operation to apply permissions, but to add access rights to the graphics API.

Click on “Add a permission” and select “Microsoft Graphics”. The following rights are required:

- Agreement.Read.All
- APIConnectors.read.all
- Application.Read.All
- Directory.Read.All
- Organization.Read.All
- Reports.Read.All
- ServiceHealth.Read.All
- User.Read.All

In the end, your panel will look like this:

Tableau de bord > Applications d'entreprise | Toutes les applications > Esia | Autorisations > Esia

Esia | API autorisées

Rechercher Actualiser Des commentaires ?

Consentement administrateur donné pour les autorisations demandées.

La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation, utilisateur ou application.

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

Ajouter une autorisation Accorder un consentement d'administrateur pour

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (12)				
Agreement.Read.All	Application	Read all terms of use agreements	Oui	Accordé pour ... ***
APIConnectors.Read.All	Application	Read API connectors for authentication flows	Oui	Accordé pour ... ***
Application.Read.All	Application	Read all applications	Oui	Accordé pour ... ***
Directory.Read.All	Application	Read directory data	Oui	Accordé pour ... ***
Organization.Read.All	Application	Read organization information	Oui	Accordé pour ... ***
PrivilegedAccess.Read.AzureAD	Application	Read privileged access to Azure AD roles	Oui	Accordé pour ... ***
PrivilegedAccess.Read.AzureADc	Application	Read privileged access to Azure AD groups	Oui	Accordé pour ... ***
PrivilegedAccess.Read.AzureResc	Application	Read privileged access to Azure resources	Oui	Accordé pour ... ***
Reports.Read.All	Application	Read all usage reports	Oui	Accordé pour ... ***
ServiceHealth.Read.All	Application	Read service health	Oui	Accordé pour ... ***
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	Accordé pour ... ***
User.Read.All	Application	Read all users' full profiles	Oui	Accordé pour ... ***
Office 365 Management APIs (3)				
ActivityFeed.Read	Application	Read activity data for your organization	Oui	Accordé pour ... ***
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Oui	Accordé pour ... ***
ServiceHealth.Read	Application	Read service health information for your organization	Oui	Accordé pour ... ***

Pour afficher et gérer les autorisations et le consentement de l'utilisateur, essayez [Applications d'entreprise](#).

The rights are now configured.

Tenant ID, client ID and API key

You now need to configure the application key so that you can connect. Click on “Single sign-on” in the menu and look for the name of your application (here: “esia”) and click on it (red box in the screenshot).

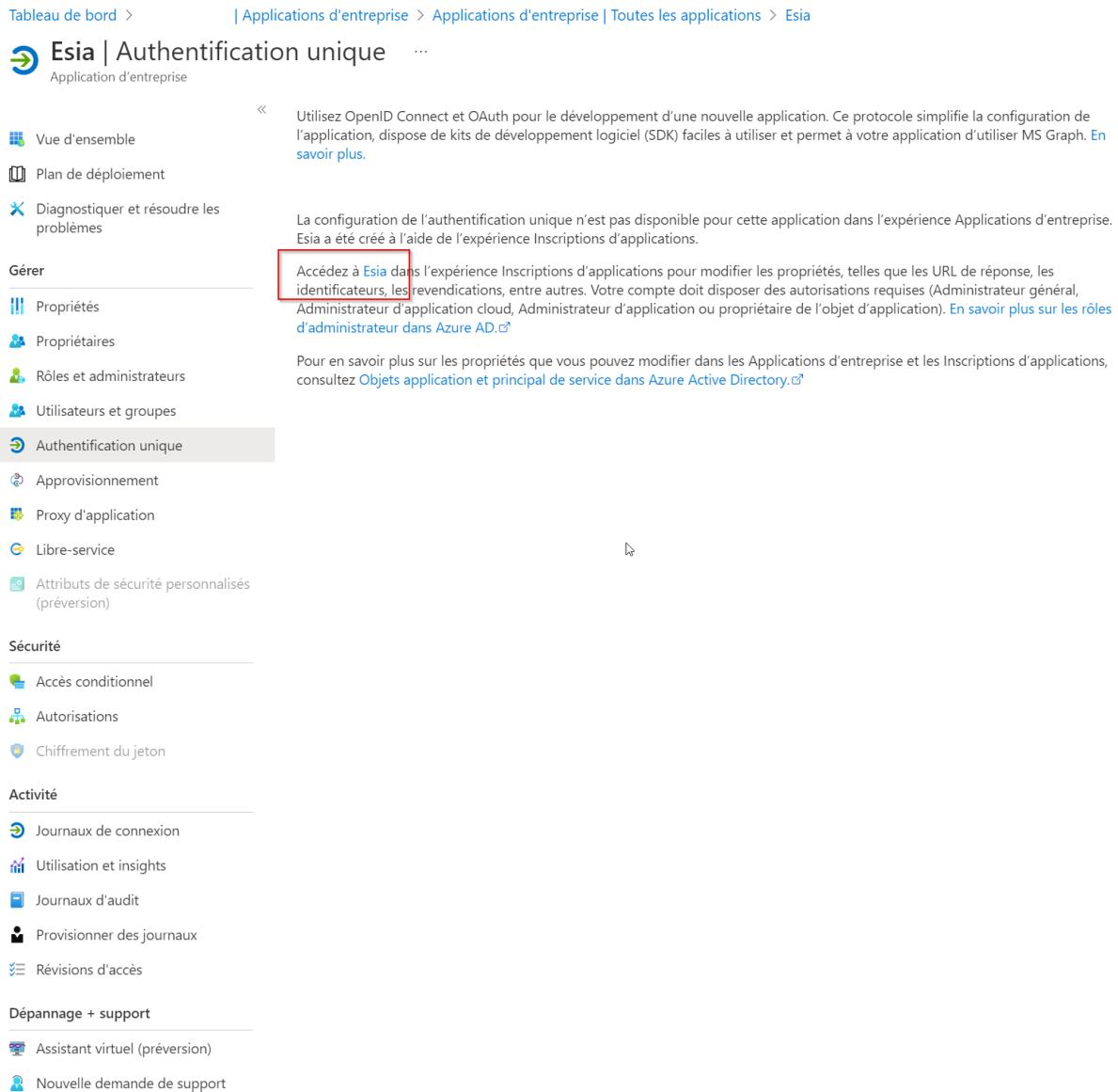


Tableau de bord > | Applications d'entreprise > Applications d'entreprise | Toutes les applications > Esia

Esia | Authentification unique

Application d'entreprise

Vue d'ensemble

Plan de déploiement

Diagnostiquer et résoudre les problèmes

Gérer

- Propriétés
- Propriétaires
- Rôles et administrateurs
- Utilisateurs et groupes
- Authentification unique**
- Approvisionnement
- Proxy d'application
- Libre-service
- Attributs de sécurité personnalisés (préversion)

Sécurité

- Accès conditionnel
- Autorisations
- Chiffrement du jeton

Activité

- Journaux de connexion
- Utilisation et insights
- Journaux d'audit
- Provisionner des journaux
- Révisions d'accès

Dépannage + support

- Assistant virtuel (préversion)
- Nouvelle demande de support

Click on “certificates & secrets” and then on “new client secret”.

Esia | Certificats & secrets

Rechercher Des commentaires ?

Vue d'ensemble Démarrage rapide Assistant Intégration

Gérer Personnalisation et propriétés

Authentification

Certificats & secrets

Configuration du jeton API autorisées Exposer une API Rôles d'application Propriétaires Rôles et administrateurs Manifeste

Support + dépannage Résolution des problèmes Nouvelle demande de support

Les informations d'identification permettent aux applications confidentielles de s'identifier auprès du service d'authentification lors de la réception de jetons à un emplacement adressable web (avec un schéma HTTPS). Pour un niveau plus élevé de sécurité, nous recommandons d'utiliser un certificat (au lieu d'un secret client) comme informations d'identification.

Les certificats d'inscription d'application, les secrets et les informations d'identification fédérées se trouvent dans les onglets ci-dessous.

Certificats (0) Secrets client (0) Informations d'identification fédérées (0)

Chaîne secrète que l'application utilise pour prouver son identité lors de la demande de jeton. Peut aussi être appelée mot de passe d'application.

+ Nouveau secret client

Description	Date d'expirat...	Valeur	ID de secret
Aucun secret client n'a été créé pour cette application.			

Select the key expiry date (maximum 24 months).

Ajouter un secret client

Description

Esia

Date d'expiration

24 mois

Ajouter

Annuler

Save the “Key value” in a text file and enter it in Esia.

Tableau de bord > Applications d'entreprise > Applications d'entreprise | Toutes les applications > Esia | Authentification unique > Esia

Esia | Certificats & secrets

Rechercher Des commentaires ?

Vue d'ensemble Démarrage rapide Assistant Intégration

Gérer Personnalisation et propriétés Authentication Certificats & secrets

Configuration du jeton API autorisées Exposer une API Rôles d'application Propriétaires Rôles et administrateurs Manifeste

Support + dépannage Résolution des problèmes Nouvelle demande de support

Des commentaires ? Vous avez une seconde pour nous faire part de vos commentaires ? →

Les informations d'identification permettent aux applications confidentielles de s'identifier auprès du service d'authentification lors de la réception de jetons à un emplacement adressable web (avec un schéma HTTPS). Pour un niveau plus élevé de sécurité, nous recommandons d'utiliser un certificat (au lieu d'un secret client) comme informations d'identification.

Les certificats d'inscription d'application, les secrets et les informations d'identification fédérées se trouvent dans les onglets ci-dessous.

Certificats (0) Secrets client (1) Informations d'identification fédérées (0)

Chaine secrète que l'application utilise pour prouver son identité lors de la demande de jeton. Peut aussi être appelée mot de passe d'application.

Nouveau secret client

Description	Date d'expirat...	Valeur	ID de secret
Esia	04/10/2024	00000000-0000-0000-0000-000000000000	00000000-0000-0000-0000-000000000000

Click on “Overview” and copy the application ID (ClientId) and directory ID (TenantId) into your file.

Tableau de bord > Applications d'entreprise > Applications d'entreprise | Toutes les applications > Esia | Authentification unique > Esia

Supprimer Points de terminaison Fonctionnalités en prévision

Vue d'ensemble Démarrage rapide Assistant Intégration

Gérer Personnalisation et propriétés Authentication Certificats & secrets Configuration du jeton API autorisées Exposer une API Rôles d'application Propriétaires Rôles et administrateurs Manifeste

Résolution des problèmes Nouvelle demande de support

Bases

Nom d'affichage : Esia

ID d'application (client) : 00000000-0000-0000-0000-000000000000

ID de l'objet : a0f3c242-ea7e-4bf0-9809-7770464e9053

ID de l'annuaire (locataire) : 00000000-0000-0000-0000-000000000000

Informations d'identificat... : Ajouter un certificat ou un secret

URI de redirection : Ajouter un URI de redirection

URI ID d'application : Ajouter un URI d'ID d'application

Application managée da... : Esia

À partir du 30 juin 2020, nous n'ajouterons plus de nouvelles fonctionnalités à Azure Active Directory Authentication Library (ADAL) et à Azure AD Graph. En savoir plus

Démarrer Documentation

Générez votre application avec la plateforme d'identités Microsoft

La plateforme d'identités Microsoft inclut un service d'authentification, des bibliothèques open source et des outils de gestion des applications. Vous pouvez créer des solutions d'authentification modernes, basées sur des normes, accéder à des API et les protéger, et ajouter une connexion pour vos utilisateurs et vos clients. En savoir plus

Appeler des API Connecter les utilisateurs en 5 minutes Configurer pour votre organisation

Appeler tous les guides de démarrage rap... Accéder à Applications d'entreprise

We now have all the data we need to create the link with Esia.

You can go to the following tutorial to complete the configuration:

[Installing and configuring the Office 365 module](#)

Display email addresses and not hashes

In order to comply with the GDPR, Microsoft has hidden user information by default. Consult your DPO or update your terms of use.

To display them, go to “Administration Centre”, then “Settings”, then “Organisation settings”, then “Services” and finally “Reports”.

Make sure the box is unchecked, as the translation can be confusing.

Rapports

Les rapports trouvés dans le Centre d'administration Microsoft 365 fournissent des informations sur les données d'utilisation de votre organisation. Les données de votre organisation sont gérées par des mesures de sécurité du cloud approuvées et de confidentialité.

Par défaut, les rapports affichent des informations avec des noms identifiables pour les utilisateurs, les groupes et les sites. Si vous préférez ou si les stratégies de votre organisation l'exigent, vous pouvez choisir d'afficher les informations de déidentifie.

Ce paramètre s'applique aux rapports d'utilisation dans le centre d'administration Microsoft 365 et le centre d'administration Microsoft Teams.

- Dans tous les rapports, afficher les noms identifiés pour les utilisateurs, les groupes et les sites.

The next time esia is tested, the data is reloaded (+- 30 min). If you don't want to wait, you can delete the cache.

```
rm /tmp/o365/*
```

From:
<https://wiki.esia-sa.com/> - **Esia Wiki**



Permanent link:
https://wiki.esia-sa.com/en/advanced/config_365

Last update: **2023/11/09 18:06**