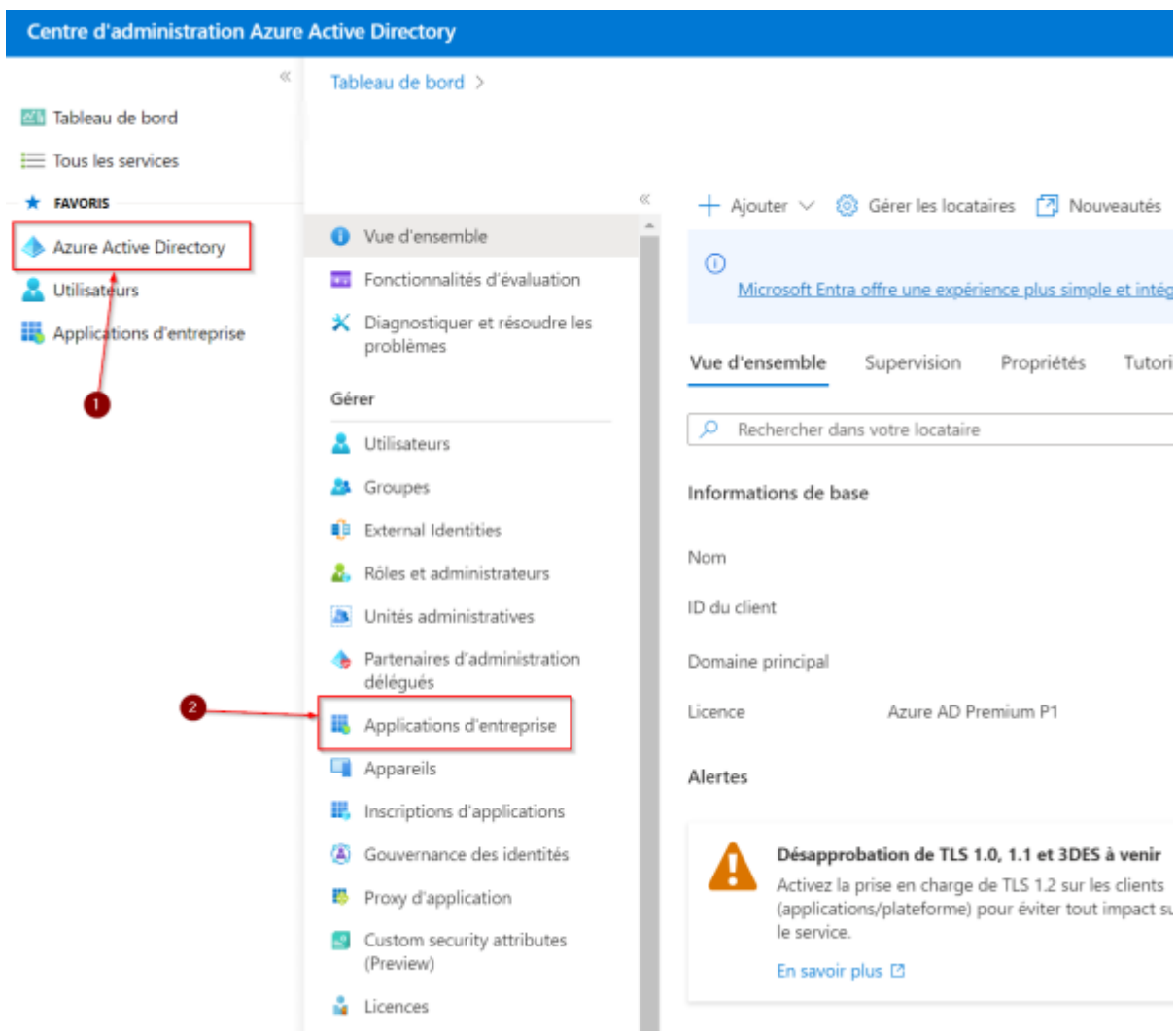


Microsoft Office 365

Nous allons voir comment créer et récupérer les éléments permettant de réaliser une liaison entre votre système ESIA et Microsoft Office365

Création de l'application

Une fois connecté dans votre centre d'administration Azure Active Directory. Cliquez sur « Azure Active Directory » et ensuite sur « Applications d'entreprise ».

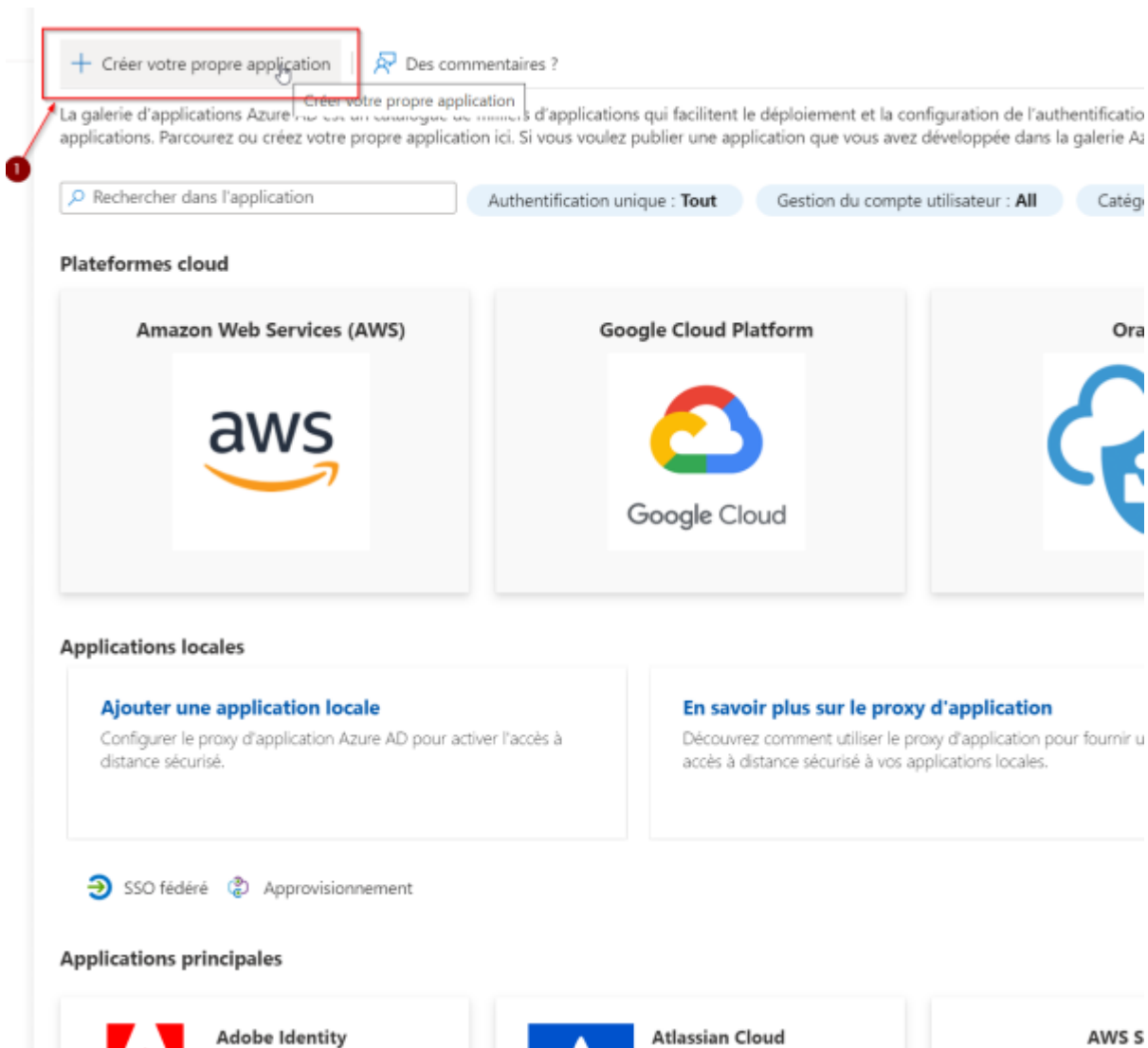


Il faut ensuite cliquer sur « Nouvelle application ».

[+ Nouvelle application](#) [Actualiser](#) [↓](#)

Affichez, filtrez et recherchez les applications de
La liste des applications conservées par votre or

Maintenant, allez sur « Créer votre propre application »



Indiquer le nom de votre application et cocher la case « Register an application to integrate with Azure AD (app you are developing) ». Même si votre interface est en français cette option est non traduite actuellement (10 octobre 2022).

Cliquez ensuite sur « Créer ».

Créer votre propre application



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 ?

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
- LeaksID
- Asite
- TESMA
- Salestim

Créer

Sélectionner le type de compte « Compte dans cet annuaire d’organisation uniquement (XXXXX uniquement – Locataire unique) ».

Tableau de bord > Intradef 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).

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

- Comptes dans cet annuaire d'organisation uniquement (XXXXX 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)

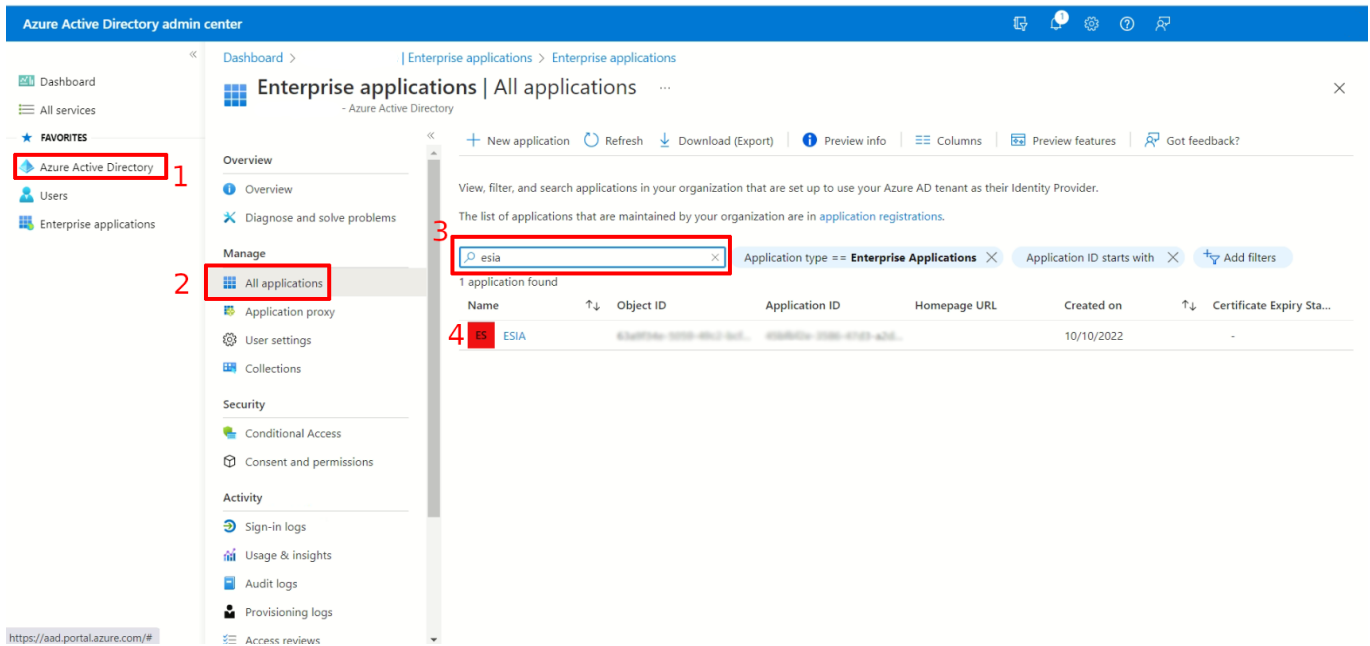
Nous retournerons la réponse d'authentification à cet URI une fois l'utilisateur authentifié. Fournir ceci maintenant est facultatif et cela peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.

Sélectionner une plateforme ▼

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](#).

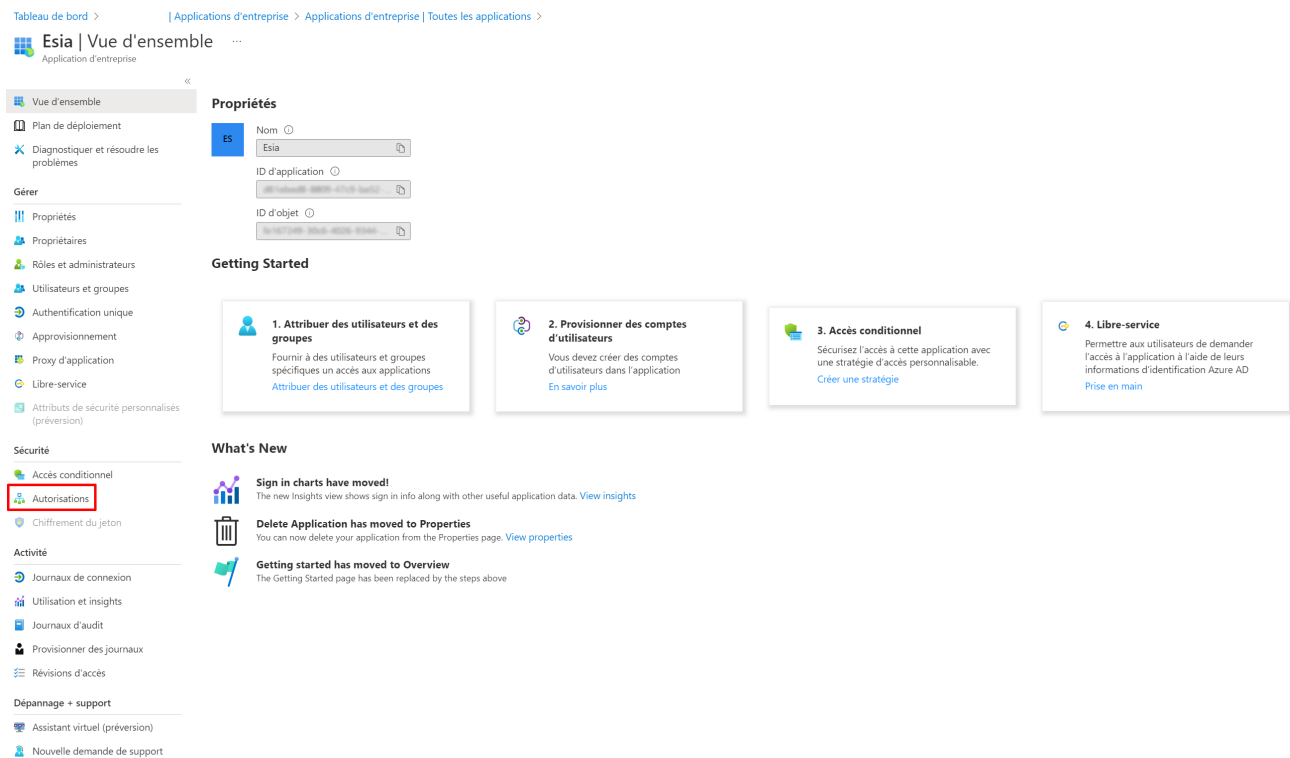
En continuant, vous acceptez les stratégies de la plateforme Microsoft ☑

Il faut maintenant configurer les autorisations de l'application, Cliquez sur “Azure Active Directory”, “All application”. Dans le champ de recherche, indiquez le nom de l'application (ici: esia) et pour terminer cliquez sur votre application.



Autorisations

Vous voilà maintenant dans la vue d'ensemble de l'application. Cliquez sur « Autorisations »



Maintenant, cliquez sur « Inscription de l'application » afin de lui donner les droits correspondants.

Tableau de bord > Esia

Esia | Autorisations

Application d'entreprise

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 un utilisateur 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 l'icône de consentement.

Accorder un consentement d'administrateur pour Intradel SCRL

Consentement de l'administrateur Consentement de l'utilisateur

Rechercher dans les autorisations

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

Cliquez sur « Ajouter une autorisation »

Esia | API autorisées

Rechercher Actualiser Des commentaires ?

Vue d'ensemble Démarrage rapide Assistant Intégration

API autorisées

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 par utilisateur.

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

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

















Sélectionnez « 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

Cliquez sur « Autorisation d'application » et sélectionnez les droits suivants :

- ActivityFeed.Read
- ActivityFeed.ReadIpl

- ServiceHealth.Read

Cliquez sur « Ajouter des autorisations ».

Demander des autorisations d'API



[< 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](#)

Autorisation

Consentement de l'administrateur r...

ActivityFeed (2)

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

ServiceHealth (1)

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



Ajouter des autorisations

Abandonner

Cliquez sur « Accorder un consentement d'administrateur »

Tableau de bord > Esia | Autorisations > Esia

Esia | API autorisées

Rechercher Actualiser Des commentaires ?

Vous êtes en train de modifier une ou plusieurs autorisations pour votre application, les utilisateurs doivent donner leur consentement, même s'ils l'ont déjà fait précédemment.

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.

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](#).

Répondez « oui » pour appliquer les droits.

Confirmation d'accord de consentement d'administrateur.

Voulez-vous donner le consentement pour les autorisations demandées pour tous les comptes dans ? Cette action mettra à jour les consentements administrateur existants de cette application pour qu'ils correspondent à ce qui est indiqué ci-dessous.

Vous devriez avoir le panneau des autorisations qui ressemble à ceci :

Tableau de bord > Esia | Autorisations > Esia

Esia | API autorisées

Rechercher Actualiser Des commentaires ?

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.

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](#).

Recommencez l'opération d'application des autorisations, mais afin d'ajouter les droits d'accès à l'API des graphiques.

Cliquez sur « Ajouter une autorisation » et sélectionnez « Microsoft Graphique ». Les droits suivants sont nécessaires :

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

Au final votre panneau ressemblera à ceci:

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 ap

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.AzureRes	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](#).

Les droits sont maintenant configurés.

Tenant ID, client ID et clé d'API

Il faut configurer maintenant la clé d'application afin de pouvoir se connecter. Cliquez dans le menu sur « Authentification unique » et cherchez le nom de votre application (ici : « esia ») et cliquez dessus (encadré rouge dans la capture d'écran).

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

« Utilisez OpenID Connect et OAuth pour le développement d'une nouvelle application. Ce protocole simplifie la configuration de l'application, dispose de kits de développement logiciel (SDK) faciles à utiliser et permet à votre application d'utiliser MS Graph. [En savoir plus.](#)

La configuration de l'authentification unique n'est pas disponible pour cette application dans l'expérience Applications d'entreprise. Esia a été créé à l'aide de l'expérience Inscriptions d'applications.

Accédez à **Esia** dans l'expérience Inscriptions d'applications pour modifier les propriétés, telles que les URL de réponse, les identificateurs, les revendications, entre autres. Votre compte doit disposer des autorisations requises (Administrateur général, Administrateur d'application cloud, Administrateur d'application ou propriétaire de l'objet d'application). [En savoir plus sur les rôles d'administrateur dans Azure AD.](#)

Pour en savoir plus sur les propriétés que vous pouvez modifier dans les Applications d'entreprise et les Inscriptions d'applications, consultez [Objets application et principal de service dans Azure Active Directory.](#)

Cliquez sur « certificats & secrets » et ensuite sur « nouveau secret client ».

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.

Sélectionnez la Date d'expiration de la clé (maximum 24 mois).

Ajouter un secret client

Description

Date d'expiration

Sauvegarder la « Valeur de la clé » dans un fichier texte, il faudra la renseigner dans Esia.

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

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)

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
Esia	04/10/2024	-----	-----

Cliquez sur « vue d'ensemble » et copiez dans votre fichier l'ID d'application (ClientID) et ID de l'annuaire (TenantID).

The screenshot shows the 'Bases' configuration page for an application named 'Esia'. Key fields are highlighted with red boxes:

- ID d'application (Client)**: 01111111-1111-1111-1111-111111111111
- ID de l'objet**: 11111111-1111-1111-1111-111111111111
- ID de l'annuaire (locataire)**: 11111111-1111-1111-1111-111111111111

Other visible information includes:

- URI de redirection: Ajouter un URI de redirection
- URI ID d'application: Ajouter un URI d'ID d'application
- Application gérée par: Esia

Below the configuration, there is a section titled 'Générez votre application avec la plateforme d'identités Microsoft' with three main steps:

- Appeler des API**: Générer des applications plus puissantes avec des données utilisateur et entreprise riches à partir des services Microsoft et des sources de données de votre entreprise. [Afficher les autorisations de l'API](#)
- Connecter les utilisateurs en 5 minutes**: Utilisez nos SDK pour connecter des utilisateurs et appeler des API en quelques étapes. Utilisez les guides de démarrage rapide pour démarrer une application web, une application mobile, une SPA ou une application démon. [Afficher tous les guides de démarrage rap...](#)
- Configurer pour votre organisation**: Affectez des utilisateurs et des groupes, appliquez des stratégies d'accès conditionnel, configurez l'authentification unique et plus encore dans Applications d'entreprise. [Accéder à Applications d'entreprise](#)

Nous avons maintenant toutes les données pour créer la liaison avec Esia.

Vous pouvez vous rendre sur le tuto suivant afin de terminer la configuration:

[Installation & Configuration du module Office 365](#)

Afficher les adresses mails et pas les hashes

Afin de respecter le GDPR, Microsoft a caché par défaut les informations utilisateurs, consulter votre

DPO ou mettez à jour vos conditions d'utilisation..

Pour les afficher, aller dans "Centre d'administration" ensuite "Paramètres" puis "Paramètres de l'organisation", puis "Services" et enfin "Rapports."

Assurez vous que la case est bien décocher, la traduction peut prêter à confusion.

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.

Au prochain test d'esia les données sont rechargées (+- 30 min), si vous ne souhaitez pas attendre, vous pouvez supprimer le cache.

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

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

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

Last update: **2023/02/10 10:54**

