

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 ».

The screenshot shows the Azure Active Directory management portal. On the left, there's a sidebar with 'FAVORIS' containing 'Azure Active Directory' (which is highlighted with a red box and has a red arrow pointing to it), 'Utilisateurs', and 'Applications d'entreprise'. The main area has a 'Vue d'ensemble' card with a message about Microsoft Entra. Below it, under 'Gérer', the 'Applications d'entreprise' option is highlighted with a red box and has a red arrow pointing to it. The right side shows the 'Vue d'ensemble' tab of the 'Applications d'entreprise' blade, which includes sections for 'Informations de base' (Nom: 'Office 365', ID du client: '00000000-0000-0000-0000-000000000000', Domaine principal: 'esia-sa.com', Licence: 'Azure AD Premium P1') and 'Alertes' (warning about TLS 1.0, 1.1, and 3DES). There are tabs for 'Supervision', 'Propriétés', and 'Tutori'.

Il faut ensuite cliquer sur « Nouvelle application ».

Nouvelle application Actualiser

Affichez, filtrez et recherchez les applications de

La liste des applications conservées par votre orga

Rechercher par nom d'application ou par ...

Maintenant, allez sur « Créez votre propre application »

Créer votre propre application Des commentaires ?

La galerie d'applications Azure contient des milliers d'applications qui facilitent le déploiement et la configuration de l'authentification pour vos applications. Parcourez ou créez votre propre application ici. Si vous voulez publier une application que vous avez développée dans la galerie Azure, utilisez ce bouton.

Rechercher dans l'application Authentification unique : Tout Gestion du compte utilisateur : All Catégories

Plateformes cloud

- Amazon Web Services (AWS)
- Google Cloud Platform
- Ora

Applications locales

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



AWS S

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 « Créez ».

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

ID LeaksID



Asite



TESMA



Salestim



Créer

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

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 (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.



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.

The screenshot shows the Azure Active Directory admin center interface. On the left, there's a sidebar with 'FAVORITES' containing 'Azure Active Directory' (marked with a red box and number 1). Under 'Manage', 'All applications' is selected (marked with a red box and number 2). The main area shows a search bar with 'esia' (marked with a red box and number 3) and a table of application results. One result, 'ESIA', is highlighted with a red box and number 4.

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Sta...
ESIA	82e0f7ff-3089-4e22-9efc-420000000000	82e0f7ff-3089-4e22-9efc-420000000000		10/10/2022	-

Autorisations

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

The screenshot shows the 'Esia | Vue d'ensemble' page. On the left, the 'Gérer' sidebar has 'Propriétés' selected (marked with a red box). The main area shows 'Propriétés' details (Name: Esia, Application ID: 82e0f7ff-3089-4e22-9efc-420000000000, Object ID: 82e0f7ff-3089-4e22-9efc-420000000000) and a 'Getting Started' section with four steps: 1. Attribuer des utilisateurs et des groupes, 2. Provisionner des comptes d'utilisateurs, 3. Accès conditionnel, and 4. Libre-service. Below this is a 'What's New' section with three items: 'Sign in charts have moved!', 'Delete Application has moved to Properties', and 'Getting started has moved to Overview'. The bottom sidebar has 'Autorisations' selected (marked with a red box).

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

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 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	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

Cliquez sur « Ajouter une autorisation »

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 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... Microsoft Graph (1)	Statut
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](#).

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

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.ReadIp

- ServiceHealth.Read

Cliquez sur « Ajouter des autorisations ».

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 ⓘ	Oui
<input checked="" type="checkbox"/> ActivityFeed.ReadDlp ⓘ	Oui

ServiceHealth (1)

<input checked="" type="checkbox"/> ServiceHealth.Read ⓘ	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 ?

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	Déléguee	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.](#)

Oui Non

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

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	Déléguee	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 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.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	Déléguee	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 chercher 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 ».

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

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

Esia

Date d'expiration

24 mois

Ajouter

Annuler

Sauvegarder la « Valeur de la clé » dans un fichier texte, il faudra la renseigner dans 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
- Authentification
- Certificats & secrets**
- Configuration du jeton
- API autorisées
- Exposer une API
- Rôles d'application
- Propriétaires
- Rôles et administrateurs
- Manifeste

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)								
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 <table border="1"> <thead> <tr> <th>Description</th> <th>Date d'expirat...</th> <th>Valeur ⓘ</th> <th>ID de secret</th> </tr> </thead> <tbody> <tr> <td>Esia</td> <td>04/10/2024</td> <td>00000000-0000-0000-0000-000000000000</td> <td></td> </tr> </tbody> </table>			Description	Date d'expirat...	Valeur ⓘ	ID de secret	Esia	04/10/2024	00000000-0000-0000-0000-000000000000	
Description	Date d'expirat...	Valeur ⓘ	ID de secret							
Esia	04/10/2024	00000000-0000-0000-0000-000000000000								

Support + dépannage

Résolution des problèmes Nouvelle demande de support

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

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

Vue d'ensemble

Supprimer Points de terminaison Fonctionnalités en prévision

Bases

Nom d'affichage : Esia	Informations d'identificat... : Ajouter un certificat ou un secret
ID d'application (Client) : 00000000-0000-0000-0000-000000000000	URI de redirection : Ajouter un URI de redirection
ID de l'objet : afbc3a42-ea4f-46ef-8000-777777777777	URI ID d'application : Ajouter un URI d'ID d'application
ID de l'annuaire (locataire) : https://login.microsoftonline.com/00000000-0000-0000-0000-000000000000	Application managée da... : Esia

Types de comptes pris en... : Mon organisation uniquement

À partir du 30 juin 2020, nous n'ajoutons plus de nouvelles fonctionnalités à Azure Active Directory Authentication Library (ADAL) et à Azure AD Graph. Nous continuons à fournir un support technique et des mises à jour de sécurité, mais nous ne proposerons plus de mises à jour des fonctionnalités. Les applications Authentication Library (MSAL) et Microsoft Graph. [En savoir plus](#)

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

Générez 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 démarrez 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**