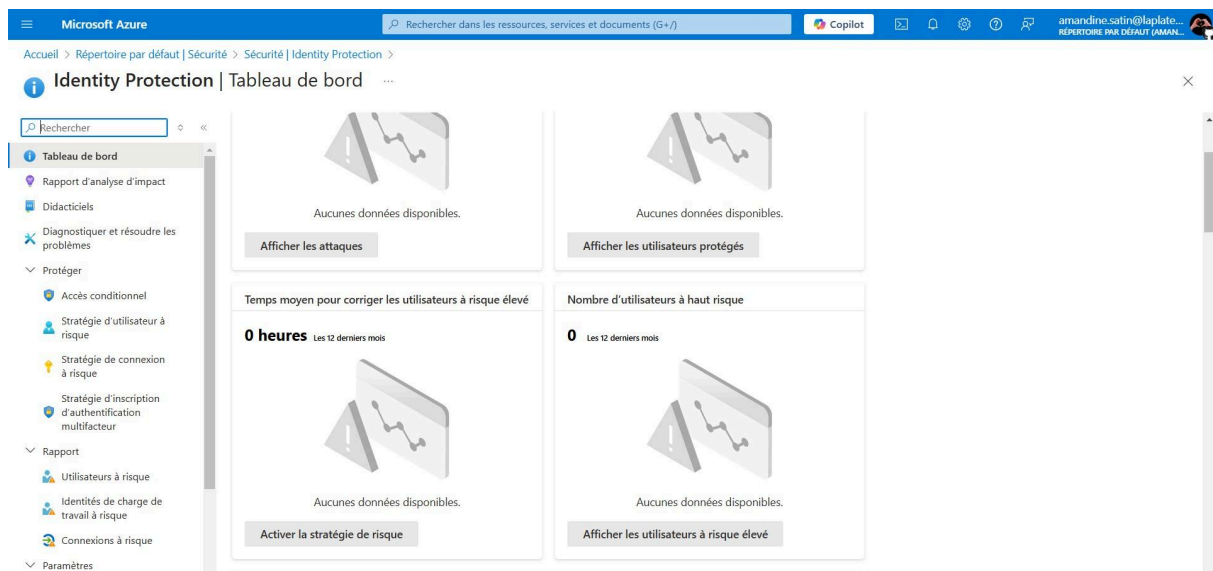


AD-entreprise

Sécurité Avancée et Politiques de Sécurité

Mettez en place des politiques pour détecter et bloquer les attaques contre les identités des membres d'équipe.

Pour gérer la sécurité on utilise Identity Protection depuis le tableau de bord on peut voir les attaque , les utilisateurs protégés, activer une stratégie de risque et afficher les utilisateur à risque élevé.



ou bien créer des stratégie conditionnelle

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

amandine.satin@laplate...

Accueil > Identity Protection | Accès conditionnel > Accès conditionnel

Microsoft Entra ID

Stratégies

Vue d'ensemble
Stratégies
Insights et rapports
Diagnostic et résolution des problèmes
Gérer
Emplacements nommés
Contrôles personnalisés (préversion)
Conditions d'utilisation
Connectivité VPN
Contextes d'authentification
Points forts d'authentification
Stratégies classiques
Supervision
Dépannage + support

Nouvelle stratégie
Nouvelle stratégie à partir de modèles
Charger un fichier de stratégie
What If
Fonctionnalités d'évaluation
Des commentaires ?

Créez vos propres stratégies et ciblez des conditions spécifiques telles que les applications cloud, les connexions à risque et les plateformes d'appareils avec Microsoft Entra ID Premium.

Qu'est-ce que l'accès conditionnel ?

L'accès conditionnel vous donne la possibilité d'appliquer des exigences d'accès quand des conditions spécifiques se produisent. Examinons quelques exemples

[En savoir plus](#)

Conditions	Contrôles
Quand un utilisateur est en dehors du réseau de société	Ils doivent se connecter avec l'authentification multifactor
Quand des utilisateurs du groupe 'Responsables' se connect...	Ils doivent être sur un appareil Intune ou joint au domaine

Prise en main

1. Créez votre première stratégie en cliquant sur « + Créer une stratégie »
2. Spécifiez les conditions et contrôles de la stratégie
3. Quand vous avez terminé, n'oubliez pas d'activer la stratégie et de la créer

[Vous êtes intéressé par les scénarios courants ?](#)

on peut gérer une stratégie d'utilisateur à risque (Cela permet d' **identifier rapidement des comportements inhabituels** et de **réagir avant qu'une compromission ne devienne un problème majeur**)

The screenshot shows the Microsoft Azure portal interface for configuring a 'Stratégie d'utilisateur à risque' (Risk User Strategy). The left sidebar contains navigation options: Tableau de bord, Rapport d'analyse d'impact, Didacticiels, Diagnostiquer et résoudre les problèmes, Protéger (Access conditionnel, Stratégie d'utilisateur à risque, Stratégie de connexion à risque, Stratégie d'inscription d'authentification multifactor), Rapport (Utilisateurs à risque, Identités de charge de travail à risque, Connexions à risque), and Paramètres. The main content area has a header 'Identity Protection | Stratégie d'utilisateur à risque'. Below this is a search bar and a list of navigation items. The main configuration section includes a warning banner about migrating to conditional access, a 'Nom de la stratégie' field with the value 'Stratégie de remédiation des risques liés aux utilisateurs', an 'Affectations' section with 'Utilisateurs' and 'Tous les utilisateurs' selected, a 'Contrôle' section with 'Accès' selected, and an 'Application de stratégies' section with 'Activé' selected. A 'Enregistrer' button is at the bottom.

une stratégie de connexion à risque (permet de **détecter et de répondre automatiquement aux connexions suspectes** ou à risque. L'objectif principal est de renforcer la sécurité des comptes utilisateurs en analysant les connexions pour identifier des activités anormales qui pourraient indiquer un potentiel compromis.)

The screenshot shows the Microsoft Azure portal interface for configuring a 'Stratégie de connexion à risque' (Risk Connection Strategy). The left sidebar contains navigation options: Tableau de bord, Rapport d'analyse d'impact, Didacticiels, Diagnostiquer et résoudre les problèmes, Protéger (Access conditionnel, Stratégie d'utilisateur à risque, Stratégie de connexion à risque, Stratégie d'inscription d'authentification multifactor), Rapport (Utilisateurs à risque, Identités de charge de travail à risque, Connexions à risque), and Paramètres. The main content area has a header 'Identity Protection | Stratégie de connexion à risque'. Below this is a search bar and a list of navigation items. The main configuration section includes a warning banner about migrating to conditional access, a 'Nom de la stratégie' field with the value 'Stratégie de remédiation des risques liés aux connexions', an 'Affectations' section with 'Utilisateurs' and 'Tous les utilisateurs' selected, a 'Contrôle' section with 'Accès' selected, and an 'Application de stratégies' section with 'Activé' selected. A 'Enregistrer' button is at the bottom.

Activez MFA pour tous les officiers supérieurs afin de sécuriser l'accès aux données sensibles de Starfleet.

exiger la double authentification aux utilisateurs

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

amandine.satin@laplate...
RÉPERTOIRE PAR DÉFAUT (AMANDINE SATIN)

Accueil > Identity Protection

Identity Protection | Stratégie d'inscription d'authentification multifacteur

Rechercher

Tableau de bord

Rapport d'analyse d'impact

Didacticiels

Diagnostic et résoudre les problèmes

Protéger

- Accès conditionnel
- Stratégie d'utilisateur à risque
- Stratégie de connexion à risque
- Stratégie d'inscription d'authentification multifacteur**

Rapport

- Utilisateurs à risque
- Identités de charge de travail à risque
- Connexions à risque

Paramètres

Nom de la stratégie

Stratégie d'inscription d'authentification multifacteur

Affectations

- Utilisateurs
- Tous les utilisateurs

Contrôle

- ☒ Exiger l'inscription de l'authentification multifacteur Microsoft Entra ID

Inclure Exclure

Sélectionner les utilisateurs et les groupes à inclure dans cette stratégie

- ☒ Tous les utilisateurs
- ☐ Sélectionner des personnes et des groupes

Utilisateurs et groupes sélectionnés

0 utilisateurs et groupes sélectionnés

La stratégie d'inscription d'authentification multifacteur affecte uniquement l'authentification multifacteur Azure basée sur le cloud. Si vous disposez d'un serveur d'authentification multifacteur, il n'est pas affecté.

Cet affichage permet aux clients P2 Microsoft Entra ID de configurer une stratégie d'inscription d'authentification multifacteur. Les autres clients peuvent uniquement désactiver les stratégies ici.

Application de stratégies

Activé Désactivée

Enregistrer

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

amandine.satin@laplate...
RÉPERTOIRE PAR DÉFAUT (AMANDINE SATIN)

Accueil > Répertoire par défaut | Utilisateurs > Utilisateurs

Authentification multifacteur par utilisateur

Bulk update

Des commentaires ?

Users

Service settings

Utilisez l'authentification multifacteur (MFA) pour protéger vos utilisateurs et vos données. Notre approche recommandée pour appliquer l'authentification multifacteur consiste à utiliser des stratégies d'accès conditionnel adaptatives. En savoir plus

Avant de commencer, consultez le guide de déploiement de l'authentification multifacteur.

✓ Activer MFA

○ Désactiver MFA

🛡️ Appliquer MFA

⚙️ Paramètres de MFA utilisateur

Rechercher

Statut : Tout

Afficher : Connecter les utilisateurs autorisés

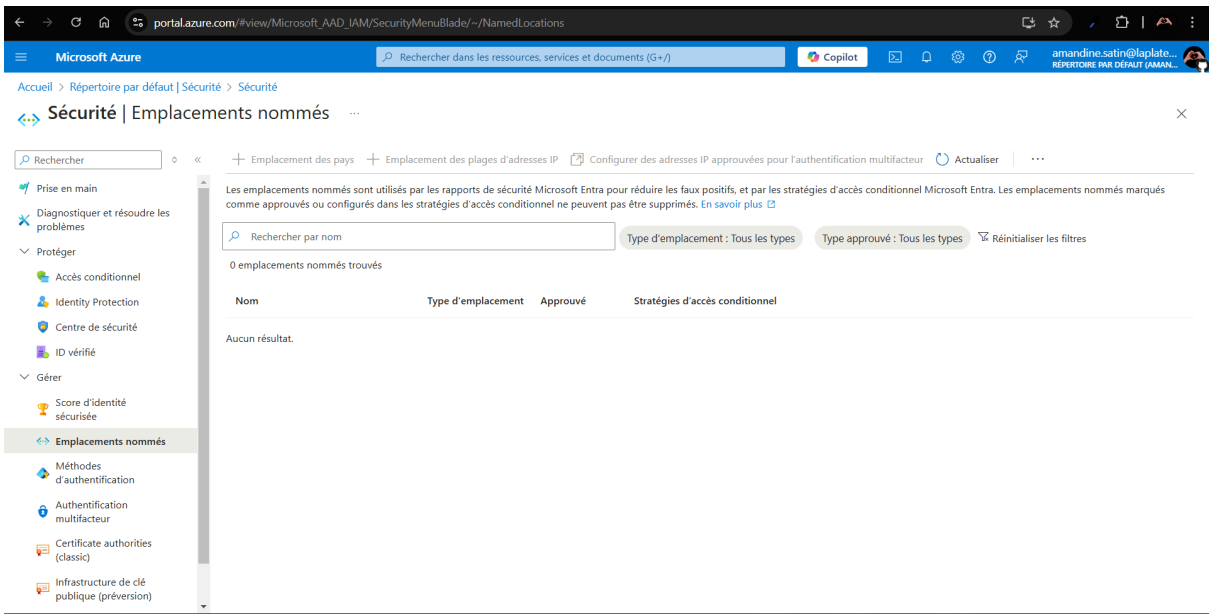
🗕 Réinitialiser les filtres

<input type="checkbox"/>	Nom	UPN	Statut
<input type="checkbox"/>	amandine satin	amandine.satin_laplateforme.io#EXT#@amandinesatinlaplateforme.onmicrosoft.com	Disabled
<input type="checkbox"/>	Jean-Luc Picard	jeanluc.picard@amandinesatinlaplateforme.onmicrosoft.com	Disabled
<input type="checkbox"/>	Rick	rick.sanchez@amandinesatinlaplateforme.onmicrosoft.com	Disabled
<input type="checkbox"/>	Morty	Morty.smith@amandinesatinlaplateforme.onmicrosoft.com	Disabled
<input type="checkbox"/>	Dexter	Dexter.reto@amandinesatinlaplateforme.onmicrosoft.com	Disabled

Créez des politiques d'accès pour restreindre les connexions depuis des emplacements non autorisés comme des planètes non sécurisées ou des vaisseaux inconnus.

Les **emplacements nommés** (ou **Named Locations**) sont une fonctionnalité qui permet de définir des zones géographiques spécifiques ou des plages d'adresses IP afin de les utiliser dans des **politiques d'accès conditionnel** . Ils servent à **renforcer la sécurité et à contrôler les accès** en se basant sur des critères de localisation.

On peut créer des **politiques d'accès conditionnel** qui bloquent ou restreignent les connexions en fonction de l'emplacement géographique. ou de l'adresse IP.



Automatisation avec PowerShell

Créez des scripts pour automatiser la gestion des utilisateurs, , ajouter des nouvelles recrues de Starfleet ou des transferts d'autres vaisseaux.

script ajout nouvel recrue dans groupe equipage

```
>> -Department "Membre d'équipage"

ObjectID                               DisplayName UserPrincipalName                UserType
-----
2addbc87-0fd2-45ea-af4a-57f91dc65d38 tony Stark  tony.stark@amandinesatinlaplateforme.onmicrosoft.com Member

PS /home/amandine>
PS /home/amandine> Write-Host "Nouvelle recrue ajoutée avec succès : $NomUtilisateur"
Nouvelle recrue ajoutée avec succès : tony.stark
PS /home/amandine>
PS /home/amandine> # Ajouter l'utilisateur au groupe "Équipe d'exploration"
PS /home/amandine> $groupeExploration = Get-AzureADGroup -Filter "DisplayName eq '$GroupeExploration'"

PS /home/amandine> Write-Host "$NomUtilisateur ajouté au groupe $GroupeEquipe"
tony.stark ajouté au groupe class Group {
  DeletionTimestamp:
  ObjectId: 5c0742d5-f49a-4c70-8170-7ab957627612
  ObjectType: Group
  Description:
  DirSyncEnabled:
  DisplayName: Équipage
  LastDirSyncTime:
```

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

amandine.satin@laplate...
RÉPERTOIRE PAR DÉFAUT (AMAND...)

Accueil > Répertoire par défaut | Utilisateurs >

Utilisateurs
Répertoire par défaut

Rechercher

+ Nouvel utilisateur

Supprimer

Télécharger les utilisateurs

Opérations en bloc

Actualiser

Gérer l'affichage

MFA par utilisateur

Des commentaires ?

Tous les utilisateurs

Journaux d'audit

Journaux de connexion

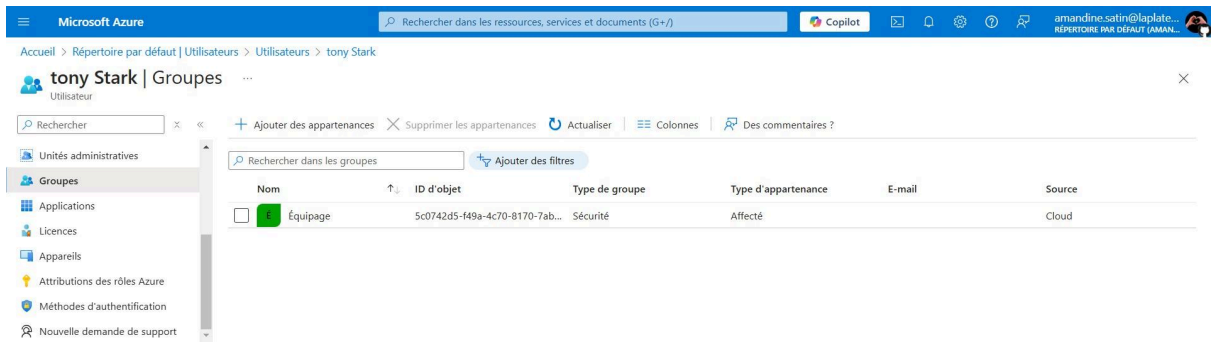
Diagnostiquer et résoudre les problèmes

Utilisateurs supprimés

Réinitialisation du mot de passe

Paramètres utilisateur

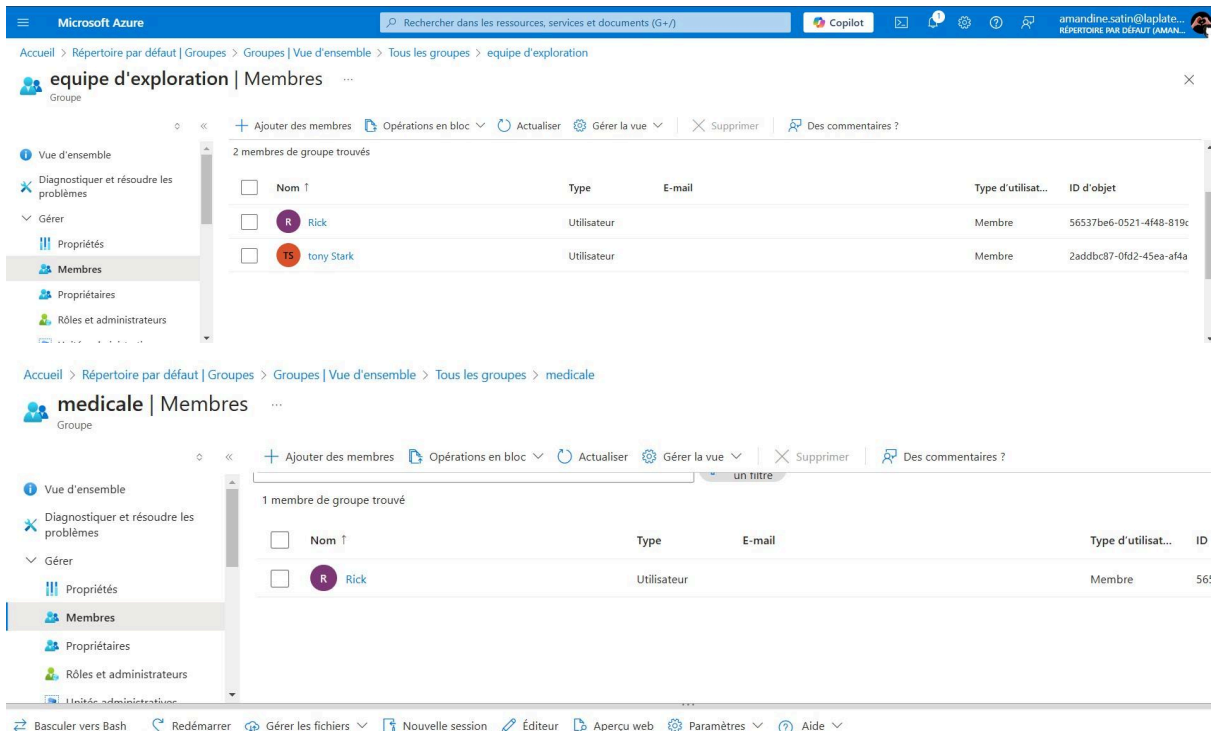
<input type="checkbox"/>	Jean-Luc Picard	jeanluc.picard@amandine...	Membre	Non	amandinesatinlaplateforme.onmic
<input type="checkbox"/>	Morty	Morty.smith@amandines...	Membre	Non	amandinesatinlaplateforme.onmic
<input type="checkbox"/>	Rick	rick.sanchez@amandines...	Membre	Non	amandinesatinlaplateforme.onmic
<input type="checkbox"/>	thomas Shelby	thomas.shelby@amandin...	Membre	Non	amandinesatinlaplateforme.onmic
<input type="checkbox"/>	tony Stark	tony.stark@amandinesati...	Membre	Non	amandinesatinlaplateforme.onmic



Gérez les groupes, comme les équipes d'exploration et les équipes médicales, en automatisant l'ajout et la suppression des membres.

script ajout d'un utilisateur dans equipe exploration et médical

```
PS /home/amandine> # Récupérer l'utilisateur Rick Sanchez
PS /home/amandine> $UtilisateurObj = Get-AzureADUser -ObjectId $EmailUtilisateur
PS /home/amandine>
PS /home/amandine> # Ajouter Rick Sanchez au groupe "equipe d'exploration"
PS /home/amandine> Add-AzureADGroupMember -ObjectId $GroupeExplorationObjectId -RefObjectId $UtilisateurObj.ObjectId
PS /home/amandine> Write-Host "$EmailUtilisateur ajouté au groupe 'equipe d'exploration'."
rick.sanchez@amandinesatinlaplateforme.onmicrosoft.com ajouté au groupe 'equipe d'exploration'.
PS /home/amandine>
PS /home/amandine> # Ajouter Rick Sanchez au groupe "medicale"
PS /home/amandine> Add-AzureADGroupMember -ObjectId $GroupeMedicaleObjectId -RefObjectId $UtilisateurObj.ObjectId
PS /home/amandine> Write-Host "$EmailUtilisateur ajouté au groupe 'medicale'."
rick.sanchez@amandinesatinlaplateforme.onmicrosoft.com ajouté au groupe 'medicale'.
PS /home/amandine> []
```



supprimer utilisateur des equipe exploration et medical

```
PS /home/amandine> # Récupérer l'utilisateur Rick Sanchez
PS /home/amandine> $UtilisateurObj = Get-AzureADUser -ObjectId $EmailUtilisateur
PS /home/amandine>
PS /home/amandine> # Supprimer Rick Sanchez du groupe "equipe d'exploration"
PS /home/amandine> Remove-AzureADGroupMember -ObjectId $GroupeExplorationObjectId -MemberId $UtilisateurObj.ObjectId
PS /home/amandine> Write-Host "$EmailUtilisateur supprimé du groupe 'equipe d'exploration'."
rick.sanchez@amandinesatinlaplateforme.onmicrosoft.com supprimé du groupe 'equipe d'exploration'.
PS /home/amandine>
PS /home/amandine> # Supprimer Rick Sanchez du groupe "medicale"
PS /home/amandine> Remove-AzureADGroupMember -ObjectId $GroupeMedicaleObjectId -MemberId $UtilisateurObj.ObjectId
PS /home/amandine> Write-Host "$EmailUtilisateur supprimé du groupe 'medicale'."
rick.sanchez@amandinesatinlaplateforme.onmicrosoft.com supprimé du groupe 'medicale'.
PS /home/amandine> []
```

The screenshot displays the Microsoft Azure portal interface for managing groups and their members. The top navigation bar shows the user 'amandine.satin@laplateforme.onmicrosoft.com' and the 'Microsoft Azure' logo. The main content area is divided into two sections, each showing the 'Membres' (Members) tab for a specific group.

Group: equipe d'exploration

The 'Membres' tab shows a list of group members. The search bar indicates '1 membre de groupe trouvé'. The table below lists the members:

Nom	Type	E-mail	Type d'utilisat...	ID d'objet
TS tony Stark	Utilisateur		Membre	2adddbc87-0fd2-45ea-af4a

Group: medicale

The 'Membres' tab shows a list of group members. The search bar indicates '0 membres de groupe trouvés'. The table below shows no results:

Nom	Type	E-mail	Type d'utilisat...	ID d'objet
Aucun membre n'a été trouvé				

Intégration et Sécurisation des Applications

integration application saas
pour gérer l'authentification, l'accès, et la sécurité

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

amandine.satin@laplate...
REPERTOIRE PAR DEFAUT (AMAN...

Accueil > Répertoire par défaut | Applications d'entreprise > Applications d'entreprise | Toutes les applications >

Parcourir la galerie Microsoft Entra

+ Créer votre propre application

Des commentaires ?

La galerie d'applications Microsoft Entra est un catalogue de milliers d'applications qui facilitent le déploiement et la configuration de l'authentification unique (SSO) à partir de la galerie d'applications, vous tirez parti des modèles prédéfinis pour connecter vos utilisateurs de manière plus sécurisée à leurs applications. Parcourez et développez dans la galerie Microsoft Entra pour que d'autres organisations puissent la découvrir et l'utiliser, vous pouvez créer une demande à l'aide du processus

saas

Authentification unique : Tout

Gestion du compte utilisateur : All

Catégories : Tout

SSO fédéré

Approvisionnement

Affichage de 22 sur 22 résultats

HPE SaaS

Hewlett Packard Enterprise Development LP

Olfeo SAAS

Olfeo

MIC SAAS Portal

MIC Datenverarbeitung GmbH

Broadcom DX SaaS

Broadcom

Kaseya Kaseya SaaS

Kaseya Int'l Ltd.

Adoddle cSaas Platform

Aste Solutions Ltd

Des commentaires ?

Logo

Nom *

HPE SaaS

Éditeur

Hewlett Packard Enterprise Development LP

Approvisionnement

Le provisionnement automatique n'est pas pris en charge

Mode d'authentification unique

URL

https://saas.hpe.com/

Authentification basée sur SAML

Authentification liée

Lire notre tutoriel pas à pas sur l'intégration de HPE SaaS

For over a decade, HPE has been leveraging the cloud to deliver industry leading and award winning HPE software solutions. Our SaaS products empower IT professionals to adapt to rapid change, utilize resources more efficiently and deliver greater business value to their organization.

Créer

configuration sso choisir le mode SAML

Le **SAML** (Security Assertion Markup Language) est un protocole standard de gestion des identités et des accès qui permet à des applications (services tiers) de s'authentifier en utilisant un fournisseur d'identité (Identity Provider, IdP). Dans le contexte de **Azure Active Directory (Azure AD)**, SAML est souvent utilisé pour la gestion de l'authentification unique (SSO - Single Sign-On) avec des applications externes ou internes.

Processus d'authentification avec SAML :

1. **L'utilisateur demande l'accès à l'application (SP) :**
 - L'utilisateur tente de se connecter à une application qui utilise SAML pour l'authentification.
2. **Redirection vers Azure AD (IdP) :**
 - L'application (SP) redirige l'utilisateur vers Azure AD pour authentification.
 - Azure AD vérifie l'identité de l'utilisateur, souvent en utilisant les informations d'un annuaire ou d'un mécanisme d'authentification secondaire.
3. **Azure AD génère une assertion SAML :**
 - Une fois que l'utilisateur est authentifié, Azure AD génère une **assertion SAML**, qui contient des informations sur l'utilisateur (comme le nom d'utilisateur, le groupe, etc.) et la valide pour l'application.
4. **L'utilisateur est renvoyé à l'application (SP) avec l'assertion SAML :**
 - L'application vérifie l'assertion SAML reçue et accorde l'accès à l'utilisateur, sans avoir besoin d'un mot de passe ou d'une autre forme d'authentification.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/J)

Copilot

amandine.satin@laplateforme.io

Accueil > Répertoire par défaut | Applications d'entreprise > Applications d'entreprise | Toutes les applications > Parcourir la galerie Microsoft Entra > HPE SaaS

HPE SaaS | 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
- Libre-service
- Attributs de sécurité personnalisés

Sécurité

Activité

Dépannage + support

L'authentification unique (SSO) apporte sécurité et confort aux utilisateurs qui se connectent à des applications dans Microsoft Entra ID. En effet, un utilisateur de votre organisation peut se connecter à toutes les applications qu'il utilise avec un seul compte. Une fois l'utilisateur connecté à une application, ces informations d'identification sont utilisées pour toutes les autres applications auxquelles il veut accéder. [En savoir plus.](#)

Sélectionner une méthode d'authentification unique

[Aidez-moi à choisir](#)

Désactivé

L'authentification unique n'est pas activée. L'utilisateur ne pourra pas lancer l'application à partir de Mes applications.

SAML

Authentification enrichie et sécurisée aux applications à l'aide du protocole SAML (Security Assertion Markup Language).

Lié

Ajoutez un lien à une application dans Mes applications et/ou le lanceur d'applications Office 365.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/J)

Copilot

thomas.shelby@amandine.io

Accueil > HPE SaaS

HPE SaaS | Authentification basée sur SAML

Application d'entreprise

Charger le fichier de métadonnées

Modifier le mode d'authentification unique

Test cette application

Des commentaires ?

1 Configuration SAML de base

Identificateur (ID d'entité) [https://saas.hpe.com](#) [Modifier](#)

URL de réponse (URL Assertion Consumer Service) [https://reponse.saas.hpe.com/SP/ACS.saml2](#)

URL de connexion [https://login.saas.hpe.com/msg](#)

État du relais (facultatif) [desazure](#)

URL de déconnexion (facultatif) [Facultatif](#)

2 Attributs et revendications

givenname [user.givenname](#) [Modifier](#)

surname [user.surname](#)

emailaddress [user.mail](#)

name [user.userprincipalname](#)

Identificateur unique de l'utilisateur [user.userprincipalname](#)

3 Certificats SAML

Certificat de signature de jetons [Modifier](#)

Statut [Actif](#)

Empreinte numérique [6CAA86F8364E7D387865F23E067557265F3D3851](#)

Expiration [15/11/2027 07:13:49](#)

E-mail de notification [amandine.satin@laplateforme.io](#)

intégration utilisateurs/groupe dans l'application

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

amandine.satin@laplate...
RÉPERTOIRE PAR DÉFAUT (AMAN...)

Accueil > Répertoire par défaut > Applications d'entreprise > Applications d'entreprise | Toutes les applications > Parcourir la galerie Microsoft Entra > HPE SaaS

HPE SaaS | Utilisateurs et groupes

Application d'entreprise

+ Ajouter un utilisateur/groupe | Modifier l'affectation | Supprimer | Mettre à jour les informations d'identification | Colonnes | Des commentaires ?

Vue d'ensemble

Plan de déploiement

Diagnostiquer et résoudre les problèmes

Gérer

- Propriétés
- Propriétaires
- Rôles et administrateurs
- Utilisateurs et groupes**
- Authentification unique
- Approvisionnement
- Libre-service
- Attributs de sécurité personnalisés

Sécurité

Activité

Dépannage + support

L'application apparaît dans Mes applications pour les utilisateurs attribués. Définissez « Visible pour les utilisateurs ? » sur Non dans les propriétés pour empêcher ceci. →

Attribuez ici des utilisateurs et des groupes à des rôles d'application pour votre application. Pour créer des rôles d'application pour cette application, utilisez l'inscription de l'application.

Affichage des 200 premiers résultats. Pour...

Nom d'affichage	Type d'objet	Rôle attribué
<input type="checkbox"/> 15 thomas Shelby	Utilisateur	Default Access

créer une application personnalisé

portal.azure.com/#view/Microsoft_AAD_IAM/AppGalleryBladeV2

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

amandine.satin@laplate...
RÉPERTOIRE PAR DÉFAUT (AMAN...)

Accueil > Répertoire par défaut > Applications d'entreprise > Applications d'entreprise | Toutes les applications >

Parcourir la galerie Microsoft Entra

+ Créer votre propre application | Des commentaires ?


La galerie d'applications Microsoft Entra est un catalogue de milliers d'applications qui facilitent le déploiement et la configuration de l'authentification unique (SSO). À partir de la galerie d'applications, vous tirez parti des modèles prédéfinis pour connecter vos utilisateurs de manière plus sécurisée à leurs applications. Parcourez la galerie d'applications Microsoft Entra pour que d'autres organisations puissent la découvrir et l'utiliser, vous pouvez créer une demande à l'aide du processus de demande d'application.

Rechercher dans l'application


Authentification unique : **Tout** | Gestion du compte utilisateur : **All** | Catégories : **Tout**

Plateformes cloud


Amazon Web Services (AWS)



Google Cloud Platform



Oracle



Applications locales

Ajouter une application locale

Configurez le proxy d'application Microsoft Entra 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.

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 ?

Gestion des Réparations ✓

Que voulez-vous faire avec votre application ?

- ☐ Configurer le proxy d'application pour un accès à distance sécurisé à une application locale
- ☐ Inscrire une application à intégrer à Microsoft Entra ID (application que vous développez)
- ☒ Intégrer une autre application que vous ne trouvez pas dans la galerie (non galerie)

Créer

Accueil > Répertoire par défaut | Applications d'entreprise > Applications d'entreprise | Toutes les applications > Parcourir la galerie Microsoft Entra >

Gestion des Réparations | Vue d'ensemble

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

Sécurité

Accès conditionnel

Autorisations

Propriétés

GD

Nom

Gestion des Réparations

ID d'application

481d78b9-25a8-42c5-a587-...

ID d'objet

01a59d7b-d367-401c-9e34...

Getting Started

1. Attribuer des utilisateurs et des groupes

Fournir à des utilisateurs et groupes spécifiques un accès aux applications

Attribuer des utilisateurs et des groupes

2. Configurer l'authentification unique

Permettre aux utilisateurs de se connecter à leur application à l'aide de leurs informations d'identification Microsoft Entra

Prise en main

3. Provisionner des comptes d'utilisateurs

Créer et supprimer automatiquement des comptes d'utilisateurs dans l'application

Prise en main

4. Accès conditionnel

Sécuriser l'accès à cette application avec une stratégie d'accès personnalisable.

5. Libre-service

Permettre aux utilisateurs de demander l'accès à l'application à l'aide de leurs informations d'identification Microsoft Entra

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

Copilot

Accueil > Gestion des Réparations

Gestion des Réparations | Authentification basée sur SAML

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

Sécurité

Accès conditionnel

Autorisations

Configurer l'authentification unique avec SAML

Une implémentation SSO basée sur les protocoles de fédération améliore la sécurité, la fiabilité et l'expérience de l'utilisateur final. Elle est également plus facile à implémenter. Choisissez l'authentification unique SAML chaque fois que cela est possible pour les applications existantes qui n'utilisent pas OpenID Connect ou OAuth. [En savoir plus.](#)

Lire le [guide de configuration](#) pour l'intégration de Gestion des Réparations.

1

Configuration SAML de base

Modifier

Identificateur (ID d'entité)
URL de réponse (URL Assertion Consumer Service)
URL de connexion
État du relais (facultatif)
URL de déconnexion (facultatif)

https://repair.management

https://repair.management

Facultatif

Facultatif

Facultatif

2

Attributs et revendications

Modifier

givenname
surname
emailaddress
name
Identificateur unique de l'utilisateur

user.givenname

user.surname

user.mail

user.userprincipalname

user.userprincipalname

Accueil > Gestion des Réparations

Gestion des Réparations | Utilisateurs et groupes

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

+ Ajouter un utilisateur/groupe

Modifier l'affectation

Supprimer

Mettre à jour les informations d'identification

Colonnes

Des commentaires ?

L'application apparaît dans Mes applications pour les utilisateurs attribués. Définissez « Visible pour les utilisateurs ? » sur Non dans les propriétés pour empêcher ceci. →

Attribuez ici des utilisateurs et des groupes à des rôles d'application pour votre application. Pour créer des rôles d'application pour cette application, utilisez l'inscription de l'application.

Affichage des 200 premiers résultats. Pour...

Nom d'affichage	Type d'objet	Rôle attribué
<input type="checkbox"/> Rick	Utilisateur	User

création de rôle pour l'application

Create app role ×

Display name * ⓘ

Survey Writer ✓

Allowed member types * ⓘ

☒ Users/Groups

☐ Applications

☐ Both (Users/Groups + Applications)

Value * ⓘ

Survey.Create ✓

Description * ⓘ

Writers can create surveys. ✓

Do you want to enable this app role? ⓘ

☒

Champ	Description	Exemple
Nom complet	Nom d'affichage du rôle d'application qui apparaît lors du consentement de l'administrateur et de l'affectation de l'application. Cette valeur peut contenir des espaces.	Survey Writer
Types de membres autorisés	<p>Spécifie si ce rôle d'application peut être attribué aux utilisateurs, aux applications ou aux deux.</p> <p>Lorsqu'ils sont disponibles pour <code>applications</code>, les rôles d'application s'affichent en tant que permissions d'application sous la section Gérer > Autorisations d'API > Ajouter une autorisation > Mes API > Choisir une API > Permissions d'application lors de l'inscription d'une application.</p>	Users/Groups
Valeur	Spécifie la valeur de la revendication des rôles que l'application doit attendre dans le jeton. La valeur doit correspondre exactement à la chaîne référencée dans le code de l'application. La valeur ne peut pas contenir d'espaces.	Survey.Create
Description	Description plus détaillée du rôle d'application affiché pendant les expériences d'affectation et de consentement des applications d'administration.	Writers can create surveys.

Surveillance et Réponse aux Incidents

une étiquette de confidentialité

Microsoft Entra admin center

Home > Groups > All groups > New Group

Got feedback?

Group type: Microsoft 365

Group name: Enter the name of the group

Group email address: Enter the local part of the email address @microsoft.com

Group description: Enter a description for the group

Membership type: Assigned

Sensitivity label: Confidential/Internal only

Owners: No owners selected

Members: No members selected

Create

une étiquette de sensibilité

Home > Groups > All groups > 'A' Project Team

'A' Project Team | Properties

Group

Save Discard Got feedback?

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Applications

Azure role assignments

Activity

Privileged Identity Management

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

New support request

General settings

Group name: 'A' Project Team

Group description: DP Re-do V-Team

Group type: Microsoft 365

Membership type: Assigned

Sensitivity label: Confidential/Internal only Remove

Object Id

Microsoft Entra roles can be assigned to the group: Yes No

Group writeback state: No writeback

journaux de connexion

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

amandine.satin@laplate...

RÉPERTOIRE PAR DÉFAUT

Accueil > Répertoire par défaut

Répertoire par défaut | Journaux de connexion

personnalisés

Mobilité (GPM et WIP)

Réinitialisation du mot de passe

Paramètres utilisateur

Propriétés

Sécurité

Supervision

Journaux de connexion

Journaux d'audit

Provisionner des journaux

Intégrité

Log Analytics

Paramètres de diagnostic

Classeurs

Utilisation et insights

Résultats de l'opération

Télécharger

Exporter les paramètres de données

Dépanner

Actualiser

Colonnes

Des commentaires ?

Vous souhaitez revenir à l'expérience de connexion par défaut ? Cliquez ici pour quitter la préversion. →

Date : Dernières 24 heures

Afficher les dates au format : Local

Ajouter des filtres

Connexions utilisateur (interactives)

Connexions utilisateur (non interactives)

Connexions du principal de service

Connexions d'identités managées

Date	ID de requête	Utilisateur	Application	Statut	Adresse IP	Emplacement	Accès condition...	Exigence d'auth
15/11/2024 08:10:13	587e00cc-5c2a-4f46...	amandine satin	Azure Portal	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification
15/11/2024 07:54:16	18b821d1-dd43-441...	thomas Shelby	My Apps	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification
15/11/2024 07:53:57	5eb6d4e0-5210-4dd...	thomas Shelby	Azure Portal	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification
15/11/2024 07:53:48	959fbc63-5d4b-420...	thomas Shelby	Azure Portal	Interrompu	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification
15/11/2024 07:52:18	959fbc63-5d4b-420...	thomas Shelby	Azure Portal	Interrompu	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification
15/11/2024 07:47:29	08843fd8-666e-42a2...	amandine satin	Azure Portal	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification
15/11/2024 07:14:20	581c7909-c04c-41a8...	amandine satin	My Apps	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification
15/11/2024 07:01:44	655c5e5c-88ee-45b...	amandine satin	Azure Portal	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué	Authentification