



AD-Entreprise

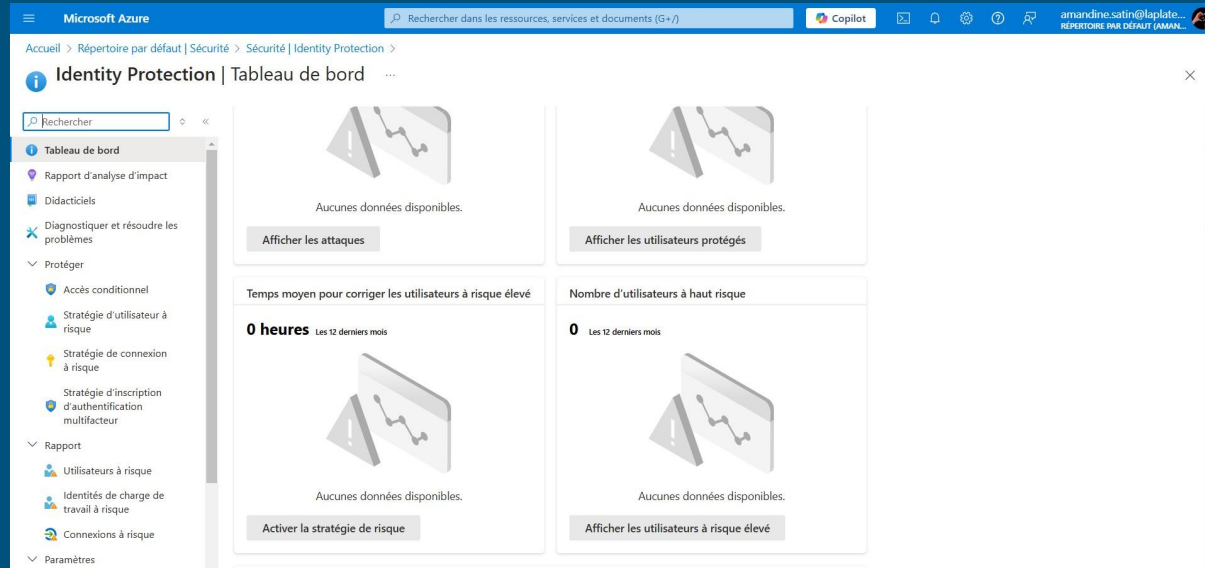




Sécurité Avancée et Politiques de Sécurité

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

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



on peut créer une stratégie à partir de modèles

Accueil > Répertoire par défaut | Sécurité > Sécurité | Identity Protection > Identity Protection | Tableau de bord

Créer une stratégie à partir de modèles

Fondation sécurisée Confiance Zéro Travail à distance Protéger l'administrateur Menace

☒ Exiger l'authentification multifactor pour les administrateurs

Exiger une authentification multifactor pour les comptes d'administration privilégiés afin de réduire le risque de compromission. Cette stratégie cible les mêmes rôles que les paramètres de sécurité par défaut.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☐ Exiger l'authentification multifactor pour tous les utilisateurs

Exiger une authentification multifactor pour tous les comptes d'utilisateur afin de réduire le risque de compromission.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☐ Sécurisation de l'inscription des informations de sécurité

Sécurisez quand et comment les utilisateurs s'inscrivent à l'authentification multifactor Azure AD et à la réinitialisation de mot de passe en libre-service.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☐ Exiger une authentification multifactor pour la gestion Azure

Exiger une authentification multifactor pour protéger l'accès privilégié à la gestion Azure.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☒ Exiger l'authentification multifactor pour les administrateurs

Exiger une authentification multifactor pour les comptes d'administration privilégiés afin de réduire le risque de compromission. Cette stratégie cible les mêmes rôles que les paramètres de sécurité par défaut.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☐ Exiger l'authentification multifactor pour tous les utilisateurs

Exiger une authentification multifactor pour tous les comptes d'utilisateur afin de réduire le risque de compromission.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☐ Sécurisation de l'inscription des informations de sécurité

Sécurisez quand et comment les utilisateurs s'inscrivent à l'authentification multifactor Azure AD et à la réinitialisation de mot de passe en libre-service.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☐ Exiger une authentification multifactor pour la gestion Azure

Exiger une authentification multifactor pour protéger l'accès privilégié à la gestion Azure.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

☐ Bloquer l'authentification héritée

Bloquez les points de terminaison d'authentification hérités qui peuvent être utilisés pour contourner l'authentification multifactor.

[En savoir plus](#)

[Afficher](#) [Télécharger le fichier JSON](#)

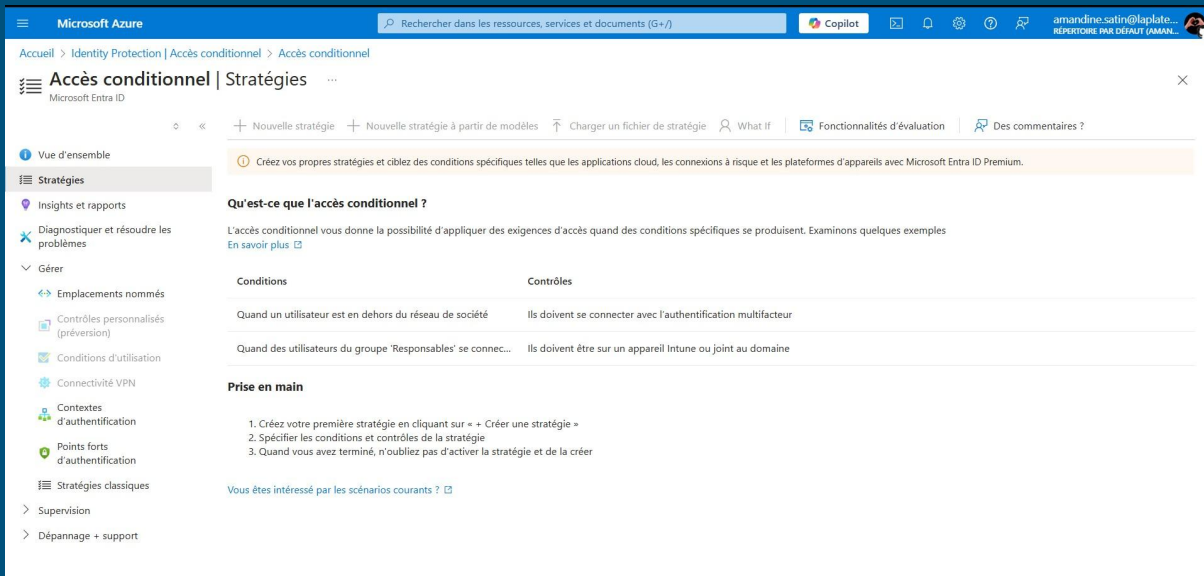
☐ Exiger un appareil ou une authentification multifactor Azure AD compatible ou hybride pour tous les utilisateurs

Protégez l'accès aux ressources de l'entreprise en demandant aux utilisateurs d'utiliser un appareil géré ou d'effectuer une authentification multifactor.

[En savoir plus](#)

Précédent Suivant

ou bien créer des stratégie conditionnelle



The screenshot displays the Microsoft Azure portal interface for Conditional Access Strategies. The top navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. The breadcrumb trail shows: Accueil > Identity Protection | Accès conditionnel > Accès conditionnel.

The main heading is "Accès conditionnel | Stratégies" with a sub-label "Microsoft Entra ID". Below this, there are several tabs: "Nouvelle stratégie", "Nouvelle stratégie à partir de modèles", "Charger un fichier de stratégie", "What If", "Fonctionnalités d'évaluation", and "Des commentaires?".

The left sidebar contains a navigation menu with the following items:

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

The main content area features a yellow tip: "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."

Below the tip, the section "Qu'est-ce que l'accès conditionnel ?" explains that Conditional Access allows applying requirements when specific conditions occur, with a link to "En savoir plus".

A table illustrates examples of conditions and controls:

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

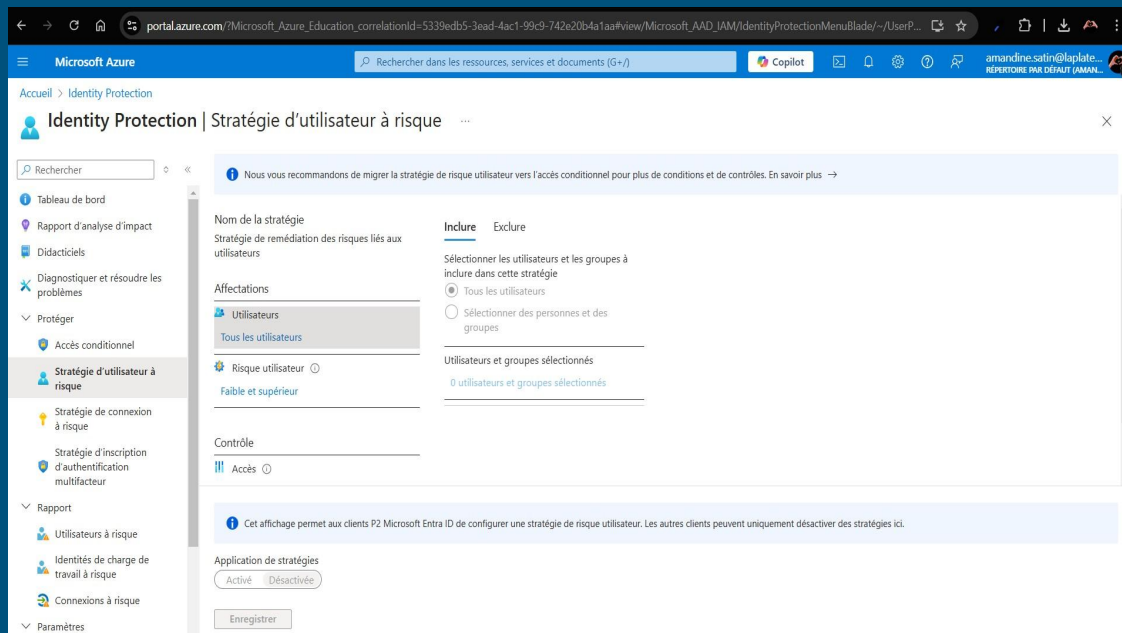
The "Prise en main" (Getting started) section provides a three-step guide:

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

At the bottom, there is a link: "Vous êtes intéressé par les scénarios courants ?".

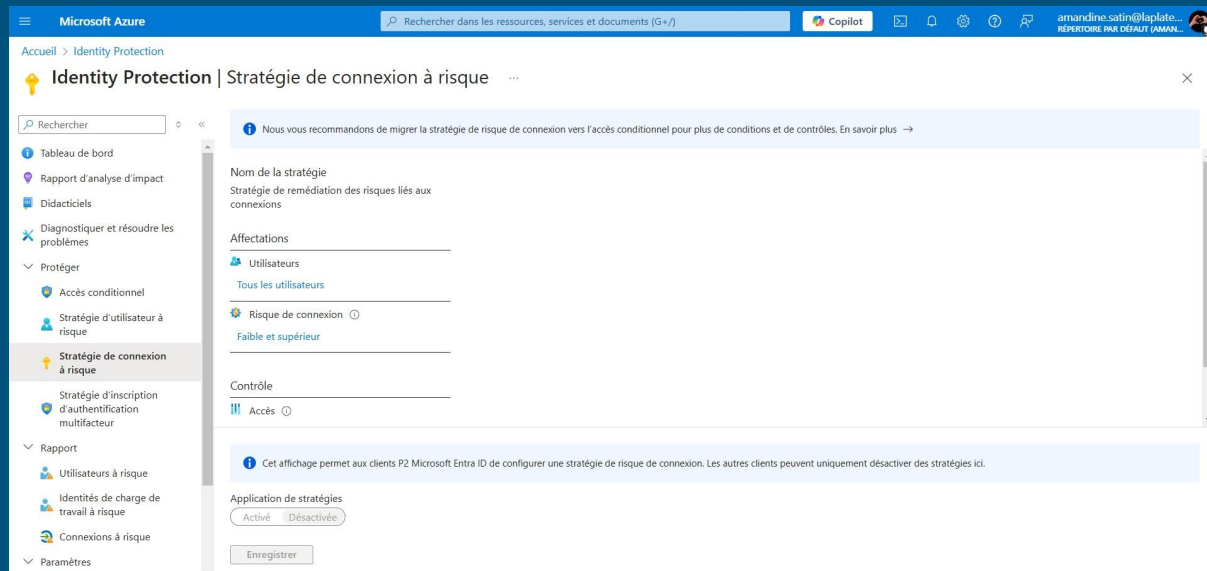
on peut gérer une stratégie d'utilisateur à risque

Cela permet d' **identifier rapidement des comportements inhabituels** et de **réagir avant qu'une compromission ne devienne un problème majeur**



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.



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

exiger la double authentification aux utilisateurs

The screenshot shows the Microsoft Azure portal interface for Identity Protection. The left sidebar contains navigation links: Tableau de bord, Rapport d'analyse d'impact, Didacticiels, Diagnostiquer et résoudre les problèmes, Protéger (with sub-links for Accès conditionnel, Stratégie d'utilisateur à risque, and Stratégie de connexion à risque), and Stratégie d'inscription d'authentification multifactor (selected). The main content area is titled 'Stratégie d'inscription d'authentification multifactor'. It includes a search bar, a 'Nom de la stratégie' field, and a 'Stratégie d'inscription d'authentification multifactor' section. Under 'Affectations', 'Utilisateurs' is selected, and 'Tous les utilisateurs' is chosen. The 'Contrôle' section has 'Exiger l'inscription de l'authentification multifactor Microsoft Entra ID' checked. A table shows 'Utilisateurs et groupes sélectionnés' with 0 users and groups. At the bottom, there are informational messages and an 'Application de stratégies' section with 'Activé' and 'Désactivée' buttons, and an 'Enregistrer' button.

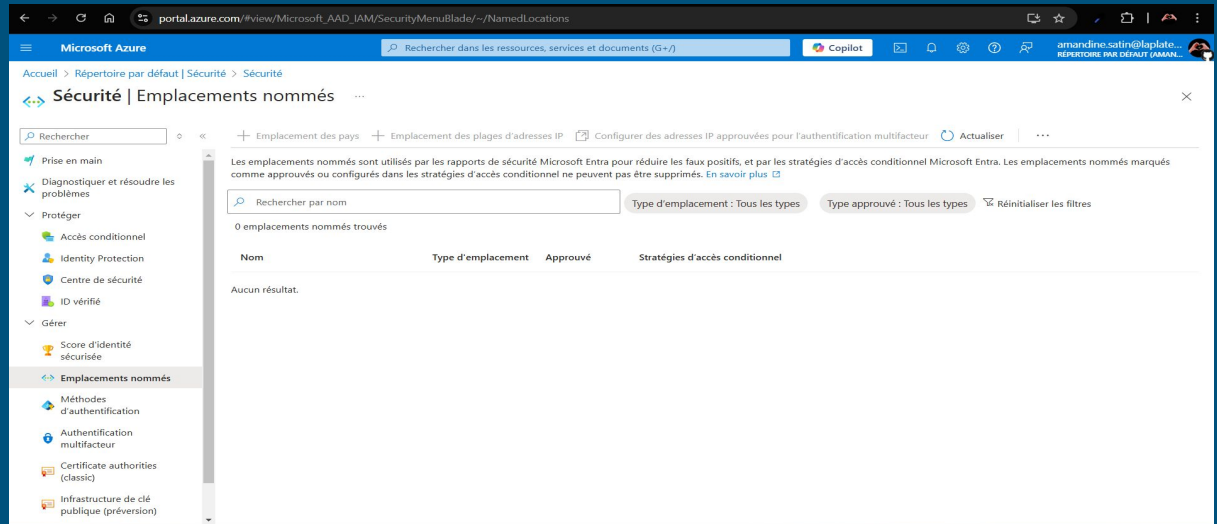
The screenshot shows the Microsoft Azure portal interface for 'Authentification multifactor par utilisateur'. The top navigation bar includes 'Microsoft Azure', a search bar, and a user profile. The main content area is titled 'Authentification multifactor par utilisateur'. It includes a 'Bulk update' button and a 'Des commentaires ?' link. The 'Users' tab is selected, showing a list of users with columns for 'Nom', 'UPN', and 'Statut'. The 'Statut' column shows 'Disabled' for all users. A 'Rechercher' bar and a 'Statut : Tout' dropdown are present. A table lists the following users:

Nom	UPN	Statut
amandine satin	amandine.satin_laplatforme.io#EXT#@amandinesatinlapl	Disabled
Jean-Luc Picard	jeanluc.picard@amandinesatinlaplatforme.onmicrosoft.co	Disabled
Rick	rick.sanchez@amandinesatinlaplatforme.onmicrosoft.com	Disabled
Morty	Morty.smith@amandinesatinlaplatforme.onmicrosoft.com	Disabled
Dexter	Dexter.reto@amandinesatinlaplatforme.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.

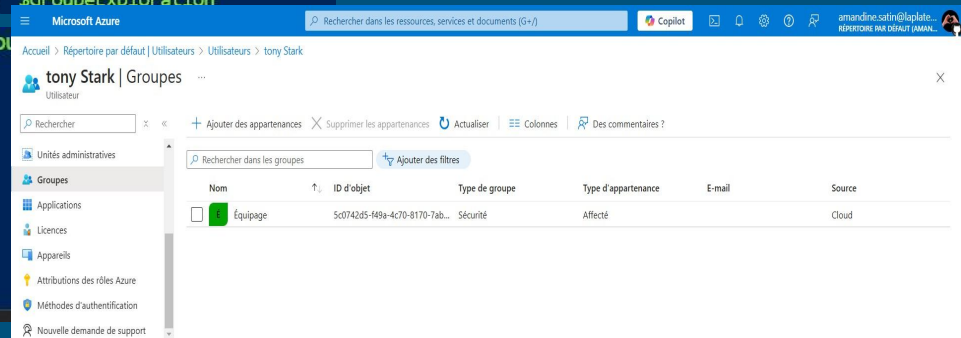
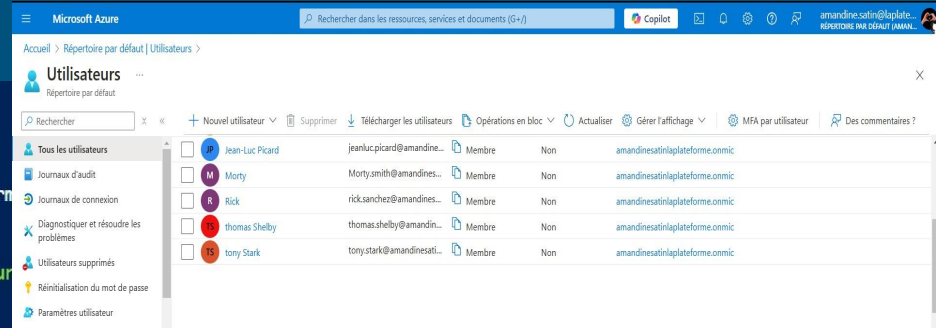
script ajout nouvel recrue dans groupe equipage

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

ObjectId                               DisplayName UserPrincipalName
-----
2addbc87-0fd2-45ea-af4a-57f91dc65d38 tony Stark  tony.stark@amandinesatinlaplateforme.com

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'"

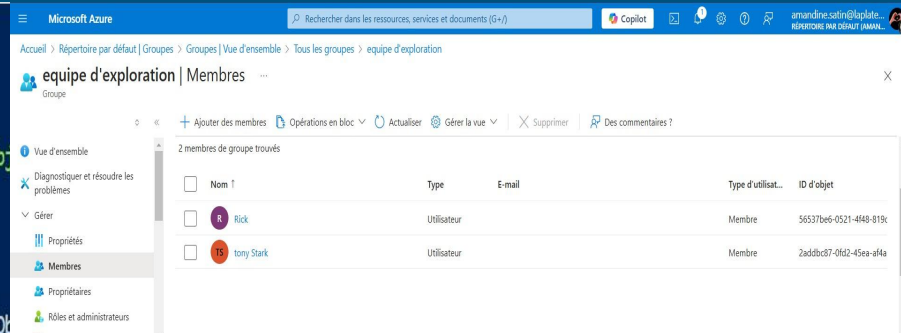
PS /home/amandine> Write-Host "$NomUtilisateur ajouté au groupe $GroupeExploration"
tony.stark ajouté au groupe class Group {
  DeletionTimestamp:
  ObjectId: 5c0742d5-f49a-4c70-8170-7ab957627612
  ObjectType: Group
  Description:
  DirSyncEnabled:
  DisplayName: Équipage
  LastDirSyncTime:
```



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

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



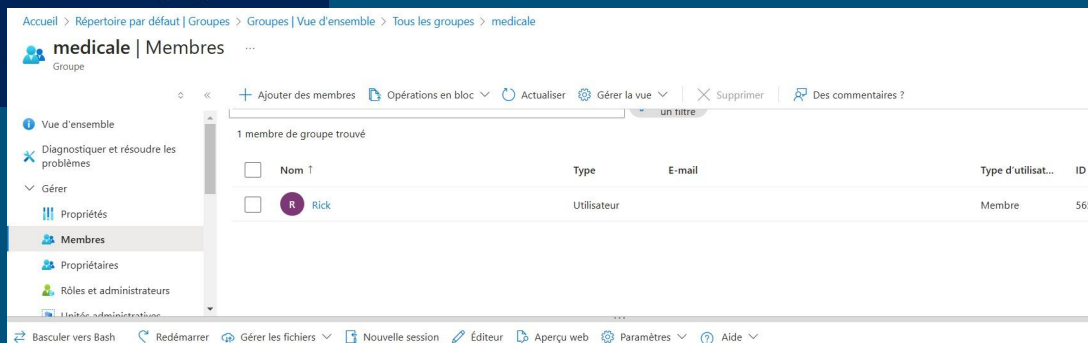
Microsoft Azure

Accueil > Répertoire par défaut > Groupes > Groupes > Vue d'ensemble > Tous les groupes > equipe d'exploration

equipe d'exploration | Membres

2 membres de groupe trouvés

Nom ↑	Type	E-mail	Type d'utilis...	ID d'objet
<input type="checkbox"/> Rick	Utilisateur		Membre	56537b65-0521-4848-819c
<input type="checkbox"/> Tony Stark	Utilisateur		Membre	2addbc37-0fd2-45ea-af4a



Microsoft Azure

Accueil > Répertoire par défaut > Groupes > Groupes > Vue d'ensemble > Tous les groupes > medicale

medicale | Membres

1 membre de groupe trouvé

Nom ↑	Type	E-mail	Type d'utilis...	ID
<input type="checkbox"/> Rick	Utilisateur		Membre	565

supprimer utilisateur des équipe 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> # 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 two side-by-side views of the Microsoft Azure portal, specifically the 'Membres' (Members) page for two different groups.

Left Panel: 'equipe d'exploration' | Membres

- Navigation: Accueil > Répertoire par défaut | Groupes > Groupes | Vue d'ensemble > Tous les groupes > equipe d'exploration
- Group: equipe d'exploration
- Actions: + Ajouter des membres, Opérations en bloc, Actualiser
- Members List: 1 membre de groupe trouvé. A table with columns 'Nom' and 'Type'. One member is listed: 'tony Stark' with a red 'TS' icon.
- Left Sidebar: Vue d'ensemble, Diagnostiquer et résoudre les problèmes, Gérer, Propriétés, Membres (selected), Propriétaires, Rôles et administrateurs.

Right Panel: 'medicale' | Membres

- Navigation: Accueil > Répertoire par défaut | Groupes > Groupes | Vue d'ensemble > Tous les groupes > medicale
- Group: medicale
- Actions: + Ajouter des membres, Opérations en bloc, Actualiser, Gérer la vue, Supprimer, Des commentaires?
- Members List: 0 membres de groupe trouvés. A table with columns 'Nom', 'Type', 'E-mail', 'Type d'utilisat...', and 'ID d'objet'. The message 'Aucun membre n'a été trouvé' is displayed.
- Left Sidebar: Vue d'ensemble, Diagnostiquer et résoudre les problèmes, Gérer, Propriétés, Membres (selected), Propriétaires, Rôles et administrateurs.



Intégration et Sécurisation des Applications

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

The screenshot shows the Microsoft Azure portal interface for managing Microsoft Entra applications. The main view is the 'Parcourir la galerie Microsoft Entra' (Browse Microsoft Entra gallery) page, which displays a search for 'saas' and lists several SaaS applications. A detailed view of the 'HPE SaaS' application is shown on the right.

Microsoft Azure

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.

saas

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

SSO fédéré | Approvisionnement

Affichage de 22 sur 22 résultats

Logo	Nom	Éditeur	Provisionnement
	HPE SaaS	Hewlett Packard Enterprise Development LP	Le provisionnement automatique n'est pas pris en charge
	Oifoo SAAS	Oifoo	
	MIC SAAS Portal	MIC Datenverarbeitung GmbH	
	Broadcom DX SaaS	Broadcom	
	Kaseya Kaseya SaaS	Kaseya Int'l Ltd.	
	Adoddle cSaas Platform	Aste Solutions Ltd	

HPE SaaS

Des commentaires ?

Logo

Nom *

HPE SaaS

Éditeur

Hewlett Packard Enterprise Development LP

Provisionnement

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

The screenshot displays the Microsoft Azure portal interface for configuring Single Sign-On (SSO) for HPE SaaS. The page is titled "HPE SaaS | Authentification basée sur SAML" and is categorized as an "Application d'entreprise".

The left sidebar shows the navigation menu with options like "Vue d'ensemble", "Plan de déploiement", "Diagnostic et résoudre les problèmes", "Gérer", "Propriétés", "Rôles et administrateurs", "Utilisateurs et groupes", "Authentification unique", "Approvisionnement", "Libre-service", "Attributs de sécurité personnalisés", "Sécurité", "Activité", and "Dépannage + support".

The main content area is divided into three numbered sections:

- 1. Configuration SAML de base**: This section contains a table with the following configuration details:

Identificateur (ID d'entité)	https://saas.hpe.com
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)	desazute
URL de déconnexion (facultatif)	Facultatif
- 2. Attributs et revendications**: This section contains a table with the following configuration details:

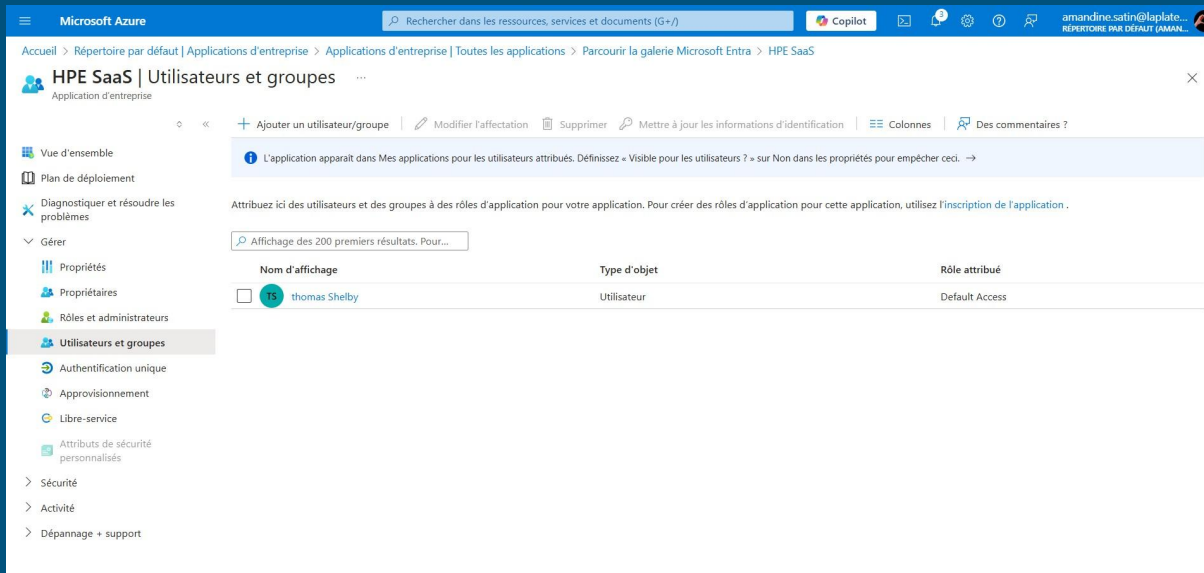
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Identificateur unique de l'utilisateur	user.userprincipalname
- 3. Certificats SAML**: This section contains a table with the following configuration details:

Certificat de signature de jetons	
Statut	Actif
Empreinte numérique	6CAA86F8364E7D387865F23E067557265F3D3851
Expiration	15/11/2027 07:13:49
E-mail de notification	amandine.satin@laplateforme.io

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

intégration utilisateurs/gROUPES dans l'application



The screenshot shows the Microsoft Azure portal interface for managing application users and groups. The breadcrumb trail indicates the path: Accueil > Répertoire par défaut | Applications d'entreprise > Applications d'entreprise | Toutes les applications > Parcourir la galerie Microsoft Entra > HPE SaaS.

The main heading is **HPE SaaS | Utilisateurs et groupes**, with a sub-label 'Application d'entreprise'.

Navigation links include: Ajouter un utilisateur/groupe, Modifier l'affectation, Supprimer, Mettre à jour les informations d'identification, Colonnes, and Des commentaires ?.

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

Instructions: 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 .

A search bar shows: Affichage des 200 premiers résultats. Pour...

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

The left sidebar contains the following menu items: Vue d'ensemble, Plan de déploiement, Diagnostiquer et résoudre les problèmes, Gérer (expanded), Propriétés, Propriétés, Rôles et administrateurs, **Utilisateurs et groupes** (selected), Authentification unique, Approvisionnement, Libre-service, Attributs de sécurité personnalisés, Sécurité, Activité, and Dépannage + support.

créer une application personnalisé

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Parcourir la galerie Microsoft Entra' (Browse the Microsoft Entra gallery) page. On the right, a modal dialog titled 'Créer votre propre application' (Create your own application) is open. The dialog contains the following elements:

- Header:** 'Créer votre propre application' with a close button (X).
- Section: Des commentaires ? (Comments?)**
 - Text: '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.'
- Form:** 'Quel est le nom de votre application ?' (What is the name of your application?) with a text input field containing 'Gestion des Réparations' and a checkmark icon.
- Section: Que voulez-vous faire avec votre application ? (What do you want to do with your 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).
- Footer:** A blue 'Créer' (Create) button.

The background page shows the 'Microsoft Azure' header with a search bar and a user profile. The main content area includes a breadcrumb trail: 'Accueil > Répertoire par défaut > Applications d'entreprise > Applications d'entreprise > Toutes les applications >'. Below this is the title 'Parcourir la galerie Microsoft Entra' and a link to 'Créer votre propre application'. A search bar and filter tabs for 'Authentification unique : Tout', 'Gestion du compte utilisateur : All', and 'Catégories : Tout' are present. The 'Plateformes cloud' (Cloud platforms) section displays three cards: 'Amazon Web Services (AWS)', 'Google Cloud Platform', and 'Oracle'. The 'Applications locales' (Local applications) section is partially visible at the bottom.

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
- Diagnostic 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

Nom

GD 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

Permettre aux 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](#)

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

Accueil > Gestion des Réparations

Gestion des Réparations | Authentification basée sur SAML

Application d'entreprise

Charger le fichier de métadonnées Modifier le mode d'authentification unique Test cette application Des commentaires ?

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

Identificateur (ID d'entité) <https://repair.management>

URL de réponse (URL Assertion Consumer Service) <https://repair.management/vice>

URL de connexion *Facultatif*

État du relais (facultatif) *Facultatif*

URL de déconnexion (facultatif) *Facultatif*

2 Attributs et revendications

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Identificateur unique de l'utilisateur	user.userprincipalname

Accueil > Gestion des Réparations

Gestion des Réparations | 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
- Diagnostic et résoudre les problèmes
- Gérer
 - Propriétés
 - Propriétaires
 - Rôles et administrateurs
 - Utilisateurs et groupes**
 - Authentification unique
 - Approvisionnement

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 pour les documents contenant des informations internes importantes, et configurer cette étiquette pour que les fichiers soient automatiquement chiffrés lorsqu'ils sont marqués ainsi

Microsoft Entra admin center

Home > Groups > All groups >

New Group

Got feedback?

Group type: Microsoft 365

Group name: *

Group email address: *

Group description: *

Membership type: *

Sensitivity label: *

Owners: No owners selected

Members: No members selected

Create

une étiquette de sensibilité

Classer les informations : Elles permettent de catégoriser les données en fonction de leur niveau de sensibilité (par exemple, "Public", "Confidentiel", "Strictement confidentiel").

Protéger les informations : Les étiquettes peuvent être liées à des règles de protection des données, telles que le chiffrement des fichiers ou l'application de restrictions d'accès (empêcher l'envoi par e-mail à des personnes externes, par exemple).

Contrôler l'accès : Elles permettent de définir qui peut accéder aux informations sensibles, et de restreindre ou autoriser des actions spécifiques sur ces informations, en fonction de la catégorie 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: [Empty]

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

Group writeback state: No writeback

