

Enterprise avec EntraID AD

EntraID AD est une solution d'annuaire **Active Directory (AD)** développée par **EntraID**, une organisation spécialisée dans les outils d'identité numérique.

Elle centralise la gestion des utilisateurs, des groupes et des droits d'accès au sein des systèmes informatiques, tout en assurant une sécurité renforcée et une conformité aux normes. Elle est particulièrement adaptée aux besoins des entreprises ou institutions qui recherchent une gestion simplifiée et unifiée de leurs identités numériques.

OBJECTIFS

- Sécurité avancées et politiques de sécurité :

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

Gestionnaire de sécurité Identity protection

- Pour gérer la sécurité Identity Protection:
- -Voir les attaques
- -Protection utilisateurs,
- -Activer une stratégie de risque
- -Afficher les utilisateur à risque élevé

stratégie de sécurité à partir de modèles :

Créer une stratégie à partir de modèles ...

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

☒ Exiger l'authentification multifacteur pour les administrateurs

Exiger une authentification multifacteur 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

☐ Sécurisation de l'inscription des informations de sécurité

Sécurisez quand et comment les utilisateurs s'authentifient avec l'authentification multifacteur Azure AD et le mot de passe en libre-service.

[En savoir plus](#)

 Afficher  Télécharger le fichier

☐ Exiger l'authentification multifacteur pour tous les utilisateurs

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

[En savoir plus](#)

 Afficher  Télécharger le fichier JSON

☐ Exiger une authentification multifacteur pour les administrateurs Azure

Exiger une authentification multifacteur pour les comptes privilégiés à la gestion Azure.

[En savoir plus](#)

 Afficher  Télécharger le fichier JS

stratégie conditionnelle

Microsoft Azure

Mettre à niveau

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

Copilot

laurent.fauveau@hotmail.com
RÉPERTOIRE PAR DÉFAUT

Accueil > Identity Protection | Accès conditionnel > Accès conditionnel

Accès conditionnel | Stratégies

Microsoft Entra ID

«

+ Nouvelle stratégie

+ Nouvelle stratégie à partir de modèles

↑ Charger un fichier de stratégie

What If

Fonctionnalités d'évaluation

Des commentaires ?

Vue d'ensemble

Stratégies

Insights et rapports

Diagnostiquer et résoudre les problèmes

Gérer

Supervision

Dépannage + support

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 multifacteur
Quand des utilisateurs du groupe 'Responsables' se connectent...	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. Spécifier 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 ?](#)

17/12/2024

5

stratégie d'utilisateur à risque

- 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 Identity Protection. The top navigation bar includes the Microsoft Azure logo, a 'Mettre à niveau' button, a search bar, and the user profile 'laurent.fauveau@hotmail.com'. The main header indicates the current path: 'Accueil > Identity Protection'. The page title is 'Identity Protection | Stratégie d'utilisateur à risque'. A search bar on the left contains 'Stratégie d'utilisateur à risque'. The left sidebar lists various security options under 'Protéger', 'Rapport', and 'Paramètres'. The main content area displays the configuration for the 'Stratégie d'utilisateur à risque' strategy, including its name, scope, and controls. A blue information banner at the top of the main content area recommends migrating to conditional access. Another blue information banner at the bottom explains that this feature is for Microsoft Entra ID clients. The 'Application de stratégies' section shows a toggle switch set to 'Activé' and an 'Enregistrer' button.

Microsoft Azure **Mettre à niveau** Rechercher dans les ressources, services et documents (G+/) Copilot laurent.fauveau@hotmail.com RÉPERTOIRE PAR DÉFAUT

Accueil > Identity Protection

Identity Protection | Stratégie d'utilisateur à risque

Stratégie d'utilisateur à risque

Nous vous recommandons de migrer la stratégie de risque utilisateur vers l'accès conditionnel pour plus de conditions et de contrôles. En savoir plus →

Protéger

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

Rapport

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

Paramètres

- Alertes Utilisateurs à risque détectés

Nom de la stratégie
Stratégie de remédiation des risques liés aux utilisateurs

Affectations

- Utilisateurs
Tous les utilisateurs
- Risque utilisateur
Faible et supérieur

Contrôle

- Accès

Cet affichage permet aux clients P2 Microsoft Entra ID de configurer une stratégie de risque utilisateur. Les autres clients peuvent uniquement désactiver des stratégies ici.

Application de stratégies

Activé Désactivée

Enregistrer

stratégie de connexion à risque

- Détecter et de répondre automatiquement aux connexions suspectes ou à risque.

The screenshot displays the Microsoft Azure portal interface for configuring a Risk Connection Strategy. The top navigation bar includes the Microsoft Azure logo, a 'Mettre à niveau' (Upgrade) button, a search bar, and the Copilot icon. The user profile 'laurent.fauveau@hotmail...' is visible in the top right corner.

The main content area is titled 'Identity Protection | Stratégie de connexion à risque'. A search bar at the top of the content area shows 'e de connexion à risque'. A blue informational banner at the top of the content area states: 'Nous vous recommandons de migrer la stratégie de risque de connexion vers l'accès conditionnel pour plus de conditions et de contrôles. En savoir plus →'.

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

- Tableau de bord
- Protéger
 - 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
 - Alertes Utilisateurs à risque détectés
- Dépannage + support
 - Nouvelle demande de support

The main configuration area for the 'Stratégie de connexion à risque' includes the following sections:

- Nom de la stratégie:** Stratégie de remédiation des risques liés aux connexions
- Affectations:**
 - Utilisateurs: Tous les utilisateurs
 - Risque de connexion: Faible et supérieur
- Contrôle:** Accès

A blue informational banner at the bottom of the configuration area states: 'Cet affichage permet aux clients P2 Microsoft Entra ID de configurer une stratégie de risque de connexion. Les autres clients peuvent uniquement désactiver des stratégies ici.'

The 'Application de stratégies' section at the bottom shows a toggle switch set to 'Activé' (Active), with a 'Désactivée' (Deactivated) option available. An 'Enregistrer' (Save) button is located at the bottom right of the configuration area.






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

Microsoft Azure

Mettre à niveau

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

Copilot



laurent.fauveau@hotma...
RÉPERTOIRE PAR DÉFAUT

Accueil > Identity Protection

Identity Protection | Stratégie d'inscription d'authentification multifacteur

Rechercher

Tableau de bord

Rapport d'analyse d'impact

Didacticiels

Diagnostiquer 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

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

double authentification aux utilisateurs

Microsoft Azure Mettre à niveau Rechercher dans les ressources, services et documents (G+) Copilot laurent.fauveau@hotmail.com RÉPERTOIRE PAR DÉFAUT













Accueil > **Utilisateurs** Répertoire par défaut

+ Nouvel utilisateur Supprimer Télécharger les utilisateurs Opérations en bloc Actualiser Gérer l'affichage MFA par utilisateur ...

Tous les utilisateurs Azure Active Directory s'appelle désormais Microsoft Entra ID

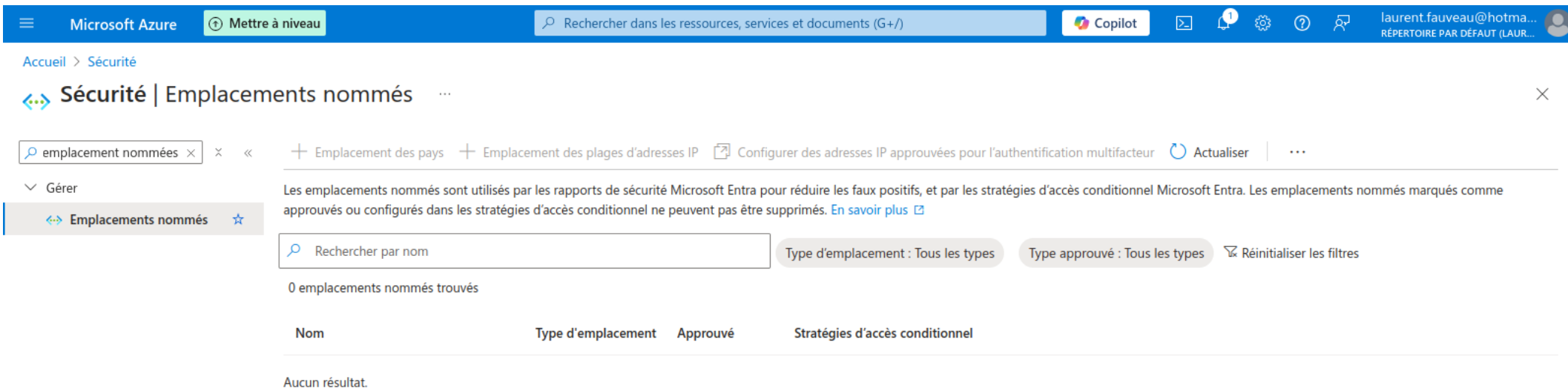
Ajouter un filtre

6 utilisateurs trouvés

<input type="checkbox"/>	Nom d'affichage ↑	Nom d'utilisateur principal ↑↓	Type d'utilisateur	Synchronisatio...	Identités	Nom de l'entreprise	Type de création
<input type="checkbox"/>	 Catherine Janeway	catherinejaneway@lauren...	 Membre	Non	laurentfauveauhotmail.onmicrosof		
<input type="checkbox"/>	 Deanna Troi	deannatoi@laurentfauvea...	 Membre	Non	laurentfauveauhotmail.onmicrosof		
<input type="checkbox"/>	 Geordi La forge	geordilaforge@laurentfau...	 Membre	Non	laurentfauveauhotmail.onmicrosof		
<input type="checkbox"/>	 Jean-Luc Picard	jeanlucpicard@laurentfau...	 Membre	Non	laurentfauveauhotmail.onmicrosof		
<input type="checkbox"/>	 laurent fauveau	laurent.fauveau_hotmail.c...	 Membre	Non	MicrosoftAccount		
<input type="checkbox"/>	 William Riker	williamriker@laurentfauve...	 Membre	Non	laurentfauveauhotmail.onmicrosof		

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

Named Locations sont une fonctionnalité qui permet de définir des zones géographiques spécifiques ou des plages d'adresses IP



Microsoft Azure

Mettre à niveau

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

Copilot

laurent.fauveau@hotmail.com
RÉPERTOIRE PAR DÉFAUT (LAUR...)

Accueil > Sécurité

Sécurité | Emplacements nommés

emplacement nommées

+ Emplacement des pays + Emplacement des plages d'adresses IP Configurer des adresses IP approuvées pour l'authentification multifacteur Actualiser

Gérer

Emplacements nommés

Rechercher par nom

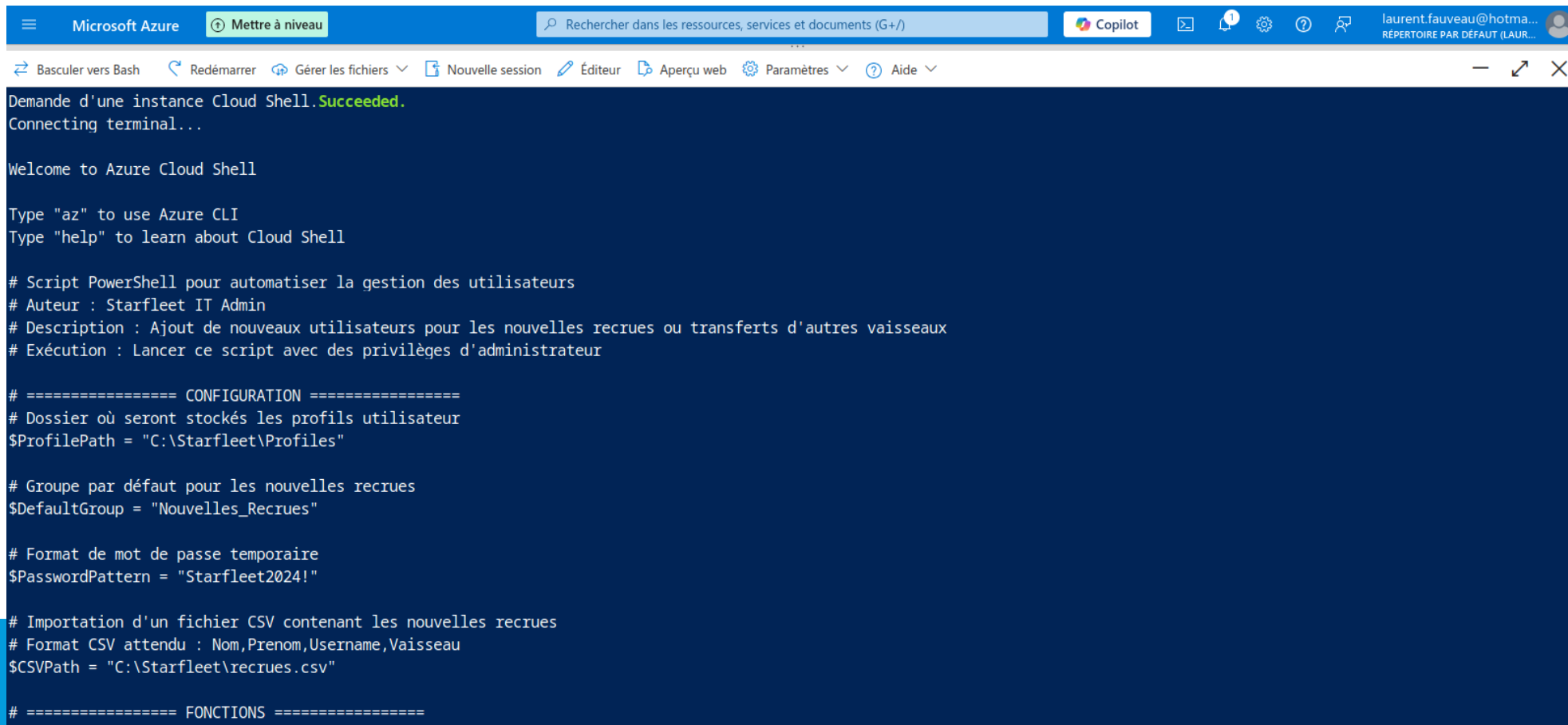
Type d'emplacement : Tous les types Type approuvé : Tous les types Réinitialiser les filtres

0 emplacements nommés trouvés

Nom	Type d'emplacement	Approuvé	Stratégies d'accès conditionnel
Aucun résultat.			

Automatisation avec PowerShell

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



The screenshot shows the Microsoft Azure Cloud Shell interface. The top bar includes the Microsoft Azure logo, a 'Mettre à niveau' button, a search bar, and various icons for Copilot, email, notifications, settings, and help. The user's email 'laurent.fauveau@hotmail.com' is visible in the top right. Below the top bar, there's a navigation bar with options like 'Basculer vers Bash', 'Redémarrer', 'Gérer les fichiers', 'Nouvelle session', 'Éditeur', 'Aperçu web', 'Paramètres', and 'Aide'. The main area displays the output of a PowerShell script. The script starts with a comment in French about automating user management, followed by a configuration section with variables for profile path, default group, password pattern, and CSV file path. The script is written in French and includes comments for each section.

```
Demande d'une instance Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

# Script PowerShell pour automatiser la gestion des utilisateurs
# Auteur : Starfleet IT Admin
# Description : Ajout de nouveaux utilisateurs pour les nouvelles recrues ou transferts d'autres vaisseaux
# Exécution : Lancer ce script avec des privilèges d'administrateur

# ===== CONFIGURATION =====
# Dossier où seront stockés les profils utilisateur
$ProfilePath = "C:\Starfleet\Profiles"

# Groupe par défaut pour les nouvelles recrues
$DefaultGroup = "Nouvelles_Recrues"

# Format de mot de passe temporaire
$PasswordPattern = "Starfleet2024!"

# Importation d'un fichier CSV contenant les nouvelles recrues
# Format CSV attendu : Nom,Prenom,Username,Vaisseau
$CSVPath = "C:\Starfleet\recrues.csv"

# ===== FONCTIONS =====
```

Script « Fonctions »

```
# ===== FONCTIONS =====

# Fonction pour vérifier si un utilisateur existe déjà
function Test-UserExists {
    param([string]$Username)
    $User = Get-ADUser -Filter {SamAccountName -eq $Username} -ErrorAction SilentlyContinue
    return $null -ne $User
}

# Fonction pour créer un nouvel utilisateur
function New-StarfleetUser {
    param(
        [string]$Nom,
        [string]$Prenom,
        [string]$Username,
        [string]$Vaisseau
    )

    # Vérification de l'existence
    if (Test-UserExists -Username $Username) {
        Write-Host "L'utilisateur $Username existe déjà. Passage à l'utilisateur suivant." -ForegroundColor Yellow
        return
    }
}
```

Scripts « Creation du Mot de passe »

```
# Création du mot de passe
```

```
MOTD: Azure Cloud Shell now includes Predictive IntelliSense! Learn more: https://aka.ms/CloudShell/IntelliSense
```

```
VERBOSE: Authenticating to Azure ...
```

```
VERBOSE: Building your Azure drive ...
```

```
PS /home/laurent> # Script PowerShell pour automatiser la gestion des utilisateurs# Auteur : Starfleet IT Admin# Description : Ajout de nouveaux utilisateurs pour les nouvelles recrues ou transferts d'autres vaisseaux# Exécution : Lancer ce script avec des privilèges d'administrateur# ===== CONFIGURATION =====# Dossier où seront stockés les profils utilisateurs$ProfilePath = "C:\Starfleet\Profiles"# Groupe par défaut pour les nouvelles recrues$DefaultGroup = "Nouvelles_Recrues"# Format de mot de passe temporaire$PasswordPattern = "Starfleet2024!"# Importation d'un fichier CSV contenant les nouvelles recrues# Format CSV attendu : Nom,Prenom,Username,Vaisseau$CSVPath = "C:\Starfleet\recrues.csv"# ===== FONCTIONS =====# Fonction pour vérifier si un utilisateur existe déjàfunction Test-UserExists {    param([string]$Username)    $User = Get-ADUser -Filter {SamAccountName -eq $Username} -ErrorAction SilentlyContinue    return $null -ne $User}# Fonction pour créer un nouvel utilisateurfunction New-StarfleetUser {    param([string]$Nom, [string]$Prenom, [string]$Username, [string]$Vaisseau)    # Vérification de l'existence    if (Test-UserExists -Username $Username) {        Write-Host "L'utilisateur $Username existe déjà. Passage à l'utilisateur suivant." -ForegroundColor Yellow        return    }    # Création du mot de passe
```

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

• Script PowerShell : Gestion des Groupes Starfleet

```
# Script PowerShell pour automatiser la gestion des groupes dans Active Directory
# Auteur : Starfleet IT Admin
# Description : Ajout ou suppression de membres dans les groupes AD (ex. : équipes
# Exécution : Lancer ce script avec des privilèges d'administrateur

# ===== CONFIGURATION =====

# Fichier CSV pour les membres à ajouter/supprimer
# Format CSV attendu : Action,Username,Groupe
# Action : "Ajouter" ou "Supprimer"
$CSVPath = "C:\Starfleet\groupes.csv"

# ===== FONCTIONS =====

# Fonction pour vérifier si un groupe existe
function Test-GroupExists {
    param([string]$GroupName)
    $Group = Get-ADGroup -Identity $GroupName -ErrorAction SilentlyContinue
```



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

- **Script PowerShell : Gestion des Groupes Starfleet (2)**

```
# Fonction pour vérifier si un utilisateur existe
function Test-UserExists {
    param([string]$Username)
    $User = Get-ADUser -Identity $Username -ErrorAction SilentlyContinue
    return $null -ne $User
}

# Fonction pour ajouter un membre au groupe
function Add-MemberToGroup {
    param(
        [string]$Username,
        [string]$GroupName
    )
}
```

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

- **Script PowerShell : Gestion des Groupes Starfleet (3)**

```
# Ajouter l'utilisateur au groupe
Add-ADGroupMember -Identity $GroupName -Members $Username -ErrorAction Silently
Write-Host "Utilisateur $Username ajouté au groupe $GroupName." -ForegroundColor
}

# Fonction pour supprimer un membre du groupe
function Remove-MemberFromGroup {
    param(
        [string]$Username,
        [string]$GroupName
    )

    # Vérifier si l'utilisateur et le groupe existent
    if (-not (Test-UserExists -Username $Username)) {
        Write-Host "Utilisateur $Username introuvable. Passage à l'action suivante."
        return
    }
    if (-not (Test-GroupExists -GroupName $GroupName)) {
```


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

- **Script PowerShell : Gestion des Groupes Starfleet (3)**

```
# Importation du fichier CSV
$Actions = Import-Csv -Path $CSVPath

# Traitement des actions
foreach ($Action in $Actions) {
    $Username = $Action.Username
    $GroupName = $Action.Groupe
    $Operation = $Action.Action

    switch ($Operation.ToLower()) {
        "ajouter" {
            Write-Host "Ajout de l'utilisateur $Username au groupe $GroupName..."
            Add-MemberToGroup -Username $Username -GroupName $GroupName
        }
        "supprimer" {
            Write-Host "Suppression de l'utilisateur $Username du groupe $GroupName"
            Remove-MemberFromGroup -Username $Username -GroupName $GroupName
        }
        default {
            Write-Host "Action '$Operation' non reconnue pour l'utilisateur $Username"
        }
    }
}

Write-Host "Traitement des groupes terminé !" -ForegroundColor Green
```



Intégration et Sécurisation des Applications

SAAS => SaaS d'applications d'entreprise pour automatiser la gestion des utilisateurs et des groupes

The screenshot displays the Microsoft Entra application gallery interface. At the top, the navigation bar includes 'Microsoft Azure', a 'Mettre à niveau' button, a search bar, and a 'Copilot' button. The main header shows 'Accueil > Applications d'entreprise | Toutes les applications >'. Below this, the section 'Parcourir la galerie Microsoft Entra' includes a '+ Créer votre propre application' link and a 'Des commentaires ?' link. A descriptive paragraph explains the gallery's purpose. A search bar contains the text 'saas'. Filter buttons for 'Authentification unique : Tout', 'Gestion du compte utilisateur : All', and 'Catégories : Tout' are visible. A section for 'Affichage de 22 sur 22 résultats' shows a grid of application cards. The first card is for 'HPE SaaS' by Hewlett Packard Enterprise Development LP, which is highlighted. Other cards include 'Olfeo SAAS', 'MIC SAAS Portal', 'Broadcom DX SaaS', 'Kaseya Kaseya SaaS', and 'Adoddle cSaas Platform'. A right-hand pane for 'HPE SaaS' provides details: 'Logo' (HPE SaaS), 'Éditeur' (Hewlett Packard Enterprise Development LP), 'Appvisionnement' (Le provisionnement automatique n'est pas pris en charge), 'Mode d'authentification unique' (https://saas.hpe.com/), and 'Authentification basée sur SAML'. A 'Créer' button is at the bottom right of the pane.

Microsoft Azure **Mettre à niveau** Rechercher dans les ressources, services et documents (G+/) Copilot laurent.fauveau@hotmail... RÉPERTOIRE PAR DÉFAUT (LAUR...)

Accueil > 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) et du provisionnement d'applications, vous tirez parti des modèles prédéfinis pour connecter vos utilisateurs de manière plus sécurisée à leurs applications. Parcourez ou créez votre propre application Microsoft Entra pour que d'autres organisations puissent la découvrir et l'utiliser, vous pouvez créer une demande à l'aide du processus décrit dans [cet article](#).

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

SSO fédéré Provisionnement

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
Asite Solutions Ltd

HPE SaaS

Des commentaires ?

Logo

Nom *

Éditeur Hewlett Packard Enterprise Development LP

Appvisionnement Le provisionnement automatique n'est pas pris en charge

Mode d'authentification unique <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

Microsoft Azure

Mettre à niveau

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

Copilot

laurent.fauveau@hotma...
RÉPERTOIRE PAR DÉFAUT (LAUR...

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

HPE SaaS | Vue d'ensemble

...

Application d'entreprise

Vue d'ensemble

Plan de déploiement

Diagnostiquer et résoudre les problèmes

Gérer

Sécurité

Activité

Dépannage + support

Propriétés

Nom

HPE SaaS

ID d'application

7b8b0980-d03a-433b-9f56- ...

ID d'objet

f3957ad4-f853-4a34-a9ca-3 ...

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

Vous devez créer des comptes d'utilisateurs dans l'application

En savoir plus

4. Accès conditionnel

Sécurisez 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

Processus d'authentification avec SAML :

Le processus d'authentification avec **SAML (Security Assertion Markup Language)** est une méthode couramment utilisée pour mettre en place une authentification unique (Single Sign-On, SSO). **SAML** est un protocole standard basé sur XML permettant aux utilisateurs d'accéder à plusieurs applications en utilisant une seule authentification,

- **Acteurs principaux dans le processus SAML**

Utilisateur : La personne qui souhaite accéder à une application.

Fournisseur d'identité (IdP - Identity Provider) : Le service qui authentifie l'utilisateur (ex : Okta, Microsoft Azure AD, Google Workspace).

Fournisseur de service (SP - Service Provider) : L'application ou le service auquel l'utilisateur souhaite accéder.

Assertions SAML : Messages XML échangés entre le SP et l'IdP, contenant les informations d'authentification et d'autorisation.

Diagramme du processus SAML

CSS

 Copier le code

```
Utilisateur → [SP] → Redirection → [IdP] → Authentification →  
[IdP génère Assertion SAML] → Redirection → [SP] → Validation → Accès accordé
```

intégration utilisateurs/groupes dans l'application

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



Diagnostic 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"/>	TS thomas Shelby	Utilisateur	Default Access

créer une application personnalisée

Microsoft Azure

Mettre à niveau

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

Copilot

laurent.fauveau@hotmail.com

RÉPERTOIRE PAR DÉFAUT (LAUR...)

Accueil >

Parcourir la galerie Microsoft Entra

+ Créer votre propre application

Des commentaires ?

crre

Authentification unique : **Tout**

Gestion du compte utilisateur : **All**

Catégories : **Tout**

Aucun résultat.

Ajouter crre comme nouvelle application

Créer

Créer votre propre application

Des commentaires ?

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

Quel est le nom de votre application ?

gestion des avaries et reparations

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 une application personnalisée

Microsoft Azure Mettre à niveau Rechercher dans les ressources, services et documents (G+/) Copilot laurent.fauveau@hotmail.com RÉPERTOIRE PAR DÉFAUT (LAUR...)

Accueil > Parcourir la galerie Microsoft Entra >

gestion des avaries et reparations | Vue d'ensemble

Application d'entreprise

- Vue d'ensemble
- Plan de déploiement
- Diagnostiquer et résoudre les problèmes
- Gérer
- Sécurité
- Activité
- Dépannage + support

Propriétés

Nom GD gestion des avaries et repara... Copier dans le Presse-papiers

ID d'application 66076c63-cec7-4d77-a1d6- ...

ID d'objet b71011a2-234a-433b-8341- ...

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**
Sécurisez 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

création de rôle pour l'application

Create app role

✕

Display name * ⓘ

Allowed member types * ⓘ
☒ Users/Groups
☐ Applications
☐ Both (Users/Groups + Applications)

Value * ⓘ

Description * ⓘ

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 applications, 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

Microsoft Azure

Mettre à niveau

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

Copilot

laurent.fauveau@hotmail.com
RÉPERTOIRE PAR DÉFAUT (LAUR...

Accueil >

Journaux d'audit

Télécharger

Actualiser

Colonnes

Des commentaires ?

Cette vue sera bientôt remplacée par une vue qui inclut des journaux d'attributs de sécurité personnalisés, un défilement infini et une réorganisation des colonnes. Essayez la nouvelle préversion des audits.

Date : 7 derniers jours

Afficher les dates au format : Local

Service : Tout

Catégorie : Tout

Activité : Tout

Ajouter des filtres

Date	Service	Catégorie	Activité	Statut	Motif d'état	Cible(s)	Initié par (actuel)
17/12/2024 09:11:00	Core Directory	ApplicationManage...	Update application	Success		gestion des avaries e...	AAD App Mana
17/12/2024 09:11:00	Core Directory	ApplicationManage...	Update service princi...	Success		gestion des avaries e...	AAD App Mana
17/12/2024 09:11:00	Core Directory	ApplicationManage...	Add service principal	Success		gestion des avaries e...	AAD App Mana
17/12/2024 09:10:59	Core Directory	ApplicationManage...	Add application	Success		gestion des avaries e...	AAD App Mana
17/12/2024 09:05:32	Core Directory	ApplicationManage...	Add service principal	Failure	Microsoft.Online.Wo...	Request Approvals R...	Microsoft Azure
17/12/2024 09:05:28	Core Directory	ApplicationManage...	Add service principal	Success		Request Approvals R...	Microsoft Azure
17/12/2024 08:59:43	Core Directory	ApplicationManage...	Add service principal	Success		Azure AD Applicatio...	Microsoft Azure
17/12/2024 08:48:37	Core Directory	ApplicationManage...	Update application	Success		HPE SaaS	AAD App Mana
17/12/2024 08:48:37	Core Directory	ApplicationManage...	Update service princi...	Success		HPE SaaS	AAD App Mana
17/12/2024 08:48:37	Core Directory	ApplicationManage...	Add service principal	Success		HPE SaaS	AAD App Mana
17/12/2024 08:48:37	Core Directory	ApplicationManage...	Add application	Success		HPE SaaS	AAD App Mana
17/12/2024 08:48:36	Core Directory	ApplicationManage...	Add service principal	Failure	Microsoft.Online.Wo...	AAD App Managem...	Microsoft Azure
17/12/2024 08:48:36	Core Directory	ApplicationManage...	Add service principal	Success		AAD App Managem...	Microsoft Azure

Notifications

Plus d'événements dans le journal d'activité →

Tout ignorer

Ajout de l'application

L'application gestion des avaries et reparations a été correctement ajoutée

il y a 10 minutes

Ajout de l'application

L'application HPE SaaS a été correctement ajoutée

il y a 32 minutes

109,92 € de crédit restant

L'abonnement « Azure subscription 1 » a un crédit restant de 109,92 €.

Effectuez une mise à niveau vers un abonnement assorti d'un paiement à l'utilisation.

il y a 58 minutes

journaux de connexion

Microsoft Azure

Mettre à niveau

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

Copilot

laurent.fauveau@hotmail.com
RÉPERTOIRE PAR DÉFAUT (LAUR...

Accueil >

Événements de connexion

Télécharger

Exporter les paramètres de données

Dépanner

Actualiser

Colonnes

Des commentaires ?

Date : Dernières 24 heures

Afficher les dates au format : Local

Ajouter des filtres

Connexions utilisateur (interactives)

Connexions utilisateur (non interactives)

Date	ID de requête	Utilisateur	Application	Statut	Adresse IP	Emplacement	Accès conditi
17/12/2024 08:22:45	dd032114-b428-473...	laurent fauveau	Azure Portal	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué
16/12/2024 12:46:20	bec850f6-b013-4777...	laurent fauveau	Azure Portal	Opération réussie	37.26.187.6	Marseille, Bouches-D...	Non appliqué

Notifications

Plus d'événements dans le journal d'activité →

Tout ignorer

Ajout de l'application

L'application gestion des avaries et reparations a été correctement ajoutée

il y a 5 minutes

Ajout de l'application

L'application HPE SaaS a été correctement ajoutée

il y a 27 minutes

109,92 € de crédit restant

L'abonnement « Azure subscription 1 » a un crédit restant de 109,92 €.

Effectuez une mise à niveau vers un abonnement assorti d'un paiement à l'utilisation.

il y a 53 minutes