


# AD Entreprise

## Sécurité avancée et Politiques de sécurité



### Protection de l'identité

Affichez les utilisateurs à risque, les identités de charge de travail à risque et les connexions à risque dans votre locataire.

Identity Protection | Stratégie d'utilisateur à risque

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 multifactor

Rapport

Paramètres

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

Nom de la stratégie

Stratégie de remédiation des risques liés aux utilisateurs

Affectations

Utilisateurs

Tous les utilisateurs

Risque utilisateur

Faible et supérieur

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

Identity Protection | Stratégie de connexion à risque

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 multifactor

Rapport

Utilisateurs à risque

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 →

Nom de la stratégie

Stratégie de remédiation des risques liés aux connexions

Affectations

Utilisateurs

Tous les utilisateurs

Risque de connexion

Faible et supérieur

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.

Application de stratégies

Activé Désactivée

Enregistrer

Identity Protection | Stratégie d'inscription d'authentification multifactor

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 multifactor**

Rapport

Paramètres

Dépannage + support

Nom de la stratégie

Stratégie d'inscription d'authentification multifactor

Affectations

Utilisateurs

Tous les utilisateurs

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

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

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

Application de stratégies

Activé Désactivée

Enregistrer

Cette partie est payante

# Automatisation avec PowerShell

## I/ Utilisateurs

### 1. Script : Ajouter une nouvelle recrue dans Entra ID

```
# Connexion à Entra ID (Azure AD)
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"

# Informations sur la nouvelle recrue
$recrueDetails = @{
    accountEnabled = $true
    displayName = "Nouvelle Recrue"
    mailNickname = "nrecrue"
    userPrincipalName = "nouvelle.recrue@starfleet.com"
    passwordProfile = @{
        forceChangePasswordNextSignIn = $true
        password = "StarfleetP@ss123"
    }
    jobTitle = "Cadet"
    department = "Équipe Exploration"
}

# Création de la recrue dans Entra ID
$newRecrue = New-MgUser -BodyParameter $recrueDetails
Write-Output "Recrue créée avec ID : $($newRecrue.Id)"

# Ajout de la recrue dans le groupe "Équipe Exploration"
$groupName = "Equipe Exploration"
$groupId = (Get-MgGroup -Filter "displayName eq '$groupName'").Id

if ($null -ne $groupId) {
    Add-MgGroupMember -GroupId $groupId -DirectoryObjectId $newRecrue.Id
    Write-Output "Recrue ajoutée au groupe '$groupName'"
} else {
    Write-Output "Erreur : Le groupe '$groupName' n'a pas été trouvé."
}
```

## 2. Script : Transférer un utilisateur d'un vaisseau (ou groupe) à un autre

```
# Connexion à Entra ID (Azure AD)
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"

# Paramètres du transfert
$userPrincipalName = "utilisateur.transfere@starfleet.com"
$ancienGroupe = "Vaisseau A"
$nouveauGroupe = "Vaisseau B"

# Récupération de l'utilisateur à transférer
$userId = (Get-MgUser -Filter "userPrincipalName eq '$userPrincipalName').Id

if ($null -ne $userId) {
    # Retrait de l'utilisateur de l'ancien groupe
    $ancienGroupId = (Get-MgGroup -Filter "displayName eq '$ancienGroupe').Id
    if ($null -ne $ancienGroupId) {
        Remove-MgGroupMember -GroupId $ancienGroupId -DirectoryObjectId $userId
        Write-Output "Utilisateur retiré du groupe '$ancienGroupe'"
    } else {
        Write-Output "Erreur : Le groupe '$ancienGroupe' n'a pas été trouvé."
    }
}

# Ajout de l'utilisateur dans le nouveau groupe
$nouveauGroupId = (Get-MgGroup -Filter "displayName eq '$nouveauGroupe').Id
if ($null -ne $nouveauGroupId) {
    Add-MgGroupMember -GroupId $nouveauGroupId -DirectoryObjectId $userId
    Write-Output "Utilisateur ajouté au groupe '$nouveauGroupe'"
} else {
    Write-Output "Erreur : Le groupe '$nouveauGroupe' n'a pas été trouvé."
}
} else {
    Write-Output "Erreur : L'utilisateur avec UPN '$userPrincipalName' n'a pas été trouvé."
}
```

### ***3. Script : Mettre à jour les informations d'un utilisateur transféré***

```
# Connexion à Entra ID (Azure AD)
Connect-MgGraph -Scopes "User.ReadWrite.All"

# Paramètres de mise à jour
$userPrincipalName = "utilisateur.transfere@starfleet.com"

# Nouveaux détails de l'utilisateur après transfert
$updatedUserDetails = @{
    jobTitle = "Officier Scientifique"
    department = "Recherche Intergalactique"
}

# Mise à jour des informations de l'utilisateur
Set-MgUser -UserId $userPrincipalName -JobTitle $updatedUserDetails.jobTitle
-Department $updatedUserDetails.department
Write-Output "Informations de l'utilisateur mises à jour : Titre =
$( $updatedUserDetails.jobTitle), Département = $( $updatedUserDetails.department)"
```

## II/ Groupes

### 1. Script : Ajouter un utilisateur à un groupe spécifique

```
# Connexion à Entra ID (Azure AD) avec les permissions nécessaires
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"

# Paramètres pour l'ajout
$userPrincipalName = "nouveau.membre@starfleet.com" # UPN de l'utilisateur
$groupName = "Equipe Exploration" # Nom du groupe cible

# Récupération de l'utilisateur
$userId = (Get-MgUser -Filter "userPrincipalName eq '$userPrincipalName').Id

if ($null -ne $userId) {
    # Récupération de l'ID du groupe cible
    $groupId = (Get-MgGroup -Filter "displayName eq '$groupName').Id

    if ($null -ne $groupId) {
        # Ajout de l'utilisateur au groupe
        Add-MgGroupMember -GroupId $groupId -DirectoryObjectId $userId
        Write-Output "Utilisateur ajouté au groupe '$groupName'."
    } else {
        Write-Output "Erreur : Le groupe '$groupName' n'a pas été trouvé."
    }
} else {
    Write-Output "Erreur : L'utilisateur avec UPN '$userPrincipalName' n'a pas été trouvé."
}
```

## 2. Script : Supprimer un utilisateur d'un groupe spécifique

```
# Connexion à Entra ID (Azure AD)
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"

# Paramètres pour la suppression
$userPrincipalName = "ancien.membre@starfleet.com" # UPN de l'utilisateur
$groupName = "Equipe Exploration" # Nom du groupe cible

# Récupération de l'utilisateur
$userId = (Get-MgUser -Filter "userPrincipalName eq '$userPrincipalName').Id

if ($null -ne $userId) {
    # Récupération de l'ID du groupe cible
    $groupId = (Get-MgGroup -Filter "displayName eq '$groupName').Id

    if ($null -ne $groupId) {
        # Suppression de l'utilisateur du groupe
        Remove-MgGroupMember -GroupId $groupId -DirectoryObjectId $userId
        Write-Output "Utilisateur retiré du groupe '$groupName'."
    } else {
        Write-Output "Erreur : Le groupe '$groupName' n'a pas été trouvé."
    }
} else {
    Write-Output "Erreur : L'utilisateur avec UPN '$userPrincipalName' n'a pas été trouvé."
}
```

### ***3. Script : Ajout de plusieurs utilisateurs dans des groupes en fonction de leur rôle***

```
# Connexion à Entra ID (Azure AD)
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"

# Définir les critères pour l'équipe médicale
$department = "Médical"          # Département ou titre cible
$groupName = "Equipe Médicale"   # Nom du groupe cible

# Récupération de l'ID du groupe cible
$groupId = (Get-MgGroup -Filter "displayName eq '$groupName'").Id

if ($null -ne $groupId) {
    # Recherche des utilisateurs dans Entra ID selon les critères
    $users = Get-MgUser -Filter "department eq '$department'"

    # Ajout de chaque utilisateur dans le groupe
    foreach ($user in $users) {
        Add-MgGroupMember -GroupId $groupId -DirectoryObjectId $user.Id
        Write-Output "Utilisateur $($user.DisplayName) ajouté au groupe '$groupName'."
    }
} else {
    Write-Output "Erreur : Le groupe '$groupName' n'a pas été trouvé."
}
```

### III/ Politiques de sécurité

Création d'une politique de sécurité

**Accédez à Azure Active Directory > Sécurité > Accès conditionnel.**

**Créez une nouvelle politique** en cliquant sur « Nouvelle politique ».

**Définissez les utilisateurs et groupes cibles** : Sélectionnez les groupes spécifiques (par exemple, les équipes de mission sensible) pour appliquer la politique.

**Définissez les conditions d'accès** : Choisissez les conditions comme l'exigence de MFA, la localisation géographique, ou les appareils conformes.

**Définissez les contrôles de session** : Activez des contrôles supplémentaires si nécessaire (comme l'accès restreint aux applications sensibles).

#### *// Script PowerShell : Ajouter des utilisateurs à un groupe de mission sensible*

```
# Connexion à Entra ID (Azure AD)
```

```
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"
```

```
# Paramètres du groupe de mission sensible
```

```
$missionSensGroupName = "Mission Sensible"
```

```
$missionSensGroupId = (Get-MgGroup -Filter "displayName eq  
'$missionSensGroupName']").Id
```

```
if ($null -ne $missionSensGroupId) {
```

```
    # Liste des utilisateurs à ajouter au groupe de mission sensible
```

```
    $userPrincipalNames = @("membre1@starfleet.com", "membre2@starfleet.com",  
"membre3@starfleet.com")
```

```
    foreach ($upn in $userPrincipalNames) {
```

```
        $userId = (Get-MgUser -Filter "userPrincipalName eq '$upn']").Id
```

```
        if ($null -ne $userId) {
```

```
            Add-MgGroupMember -GroupId $missionSensGroupId -DirectoryObjectId $userId
```

```
            Write-Output "Utilisateur $upn ajouté au groupe de mission sensible."
```

```
        } else {
```

```
            Write-Output "Erreur : Utilisateur $upn non trouvé."
```

```
        }
```

```
    }
```

```
} else {
```

```
    Write-Output "Erreur : Le groupe de mission sensible n'a pas été trouvé."
```

```
}
```



### ***II/ Automatiser la Mise à Jour des Politiques de Sécurité avec Microsoft Graph API (Facultatif)***

```
# Connexion avec des autorisations d'administration
Connect-MgGraph -Scopes "Policy.ReadWrite.ConditionalAccess"

# Exemple de récupération des politiques d'accès conditionnel
$polices = Get-MgConditionalAccessPolicy
foreach ($policy in $polices) {
    Write-Output "Nom de la politique : $($policy.DisplayName)"
}

# Modification d'une politique d'accès conditionnel pour exiger MFA
$policyId = "<ID de la politique>"
Update-MgConditionalAccessPolicy -ConditionalAccessPolicyId $policyId -Conditions @{
    "clientAppTypes" = @("Browser") } -GrantControls @{ "builtInControls" = @("mfa") }
Write-Output "Politique mise à jour pour exiger MFA."
```

---

**Exécuter les scripts pour vérifier s'ils fonctionnent correctement**

# Intégration et Sécurisation des Applications

## I/ Intégration d'une application SaaS avec Entra ID

TAS | 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

📘 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"/>	DC Dylan Capron	Utilisateur	Default Access

EmpCenter | 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

✅ Attribution d'application réussie  
L'accès a été attribué à 1 utilisateur et 0 groupes

📘 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"/>	DC Dylan Capron	Utilisateur	Default Access

## Applications d'entreprise | Toutes les applications

- Vue d'ensemble
  - Vue d'ensemble
  - Diagnostiquer et résoudre les problèmes
- Gérer
  - Toutes les applications
  - Connecteurs de réseau privé
  - Paramètres utilisateur
  - Lanceur d'applications
  - Extensions d'authentification personnalisées

Affichez, filtrez et recherchez les applications de votre organisation qui sont configurées pour utiliser votre locataire Microsoft Entra comme fournisseur d'identité. La liste des applications conservées par votre organisation se trouve dans [inscriptions d'applications](#).

Rechercher par nom d'application ou par ... Type d'application == Applications d'entreprise ID d'application commence par Ajouter des filtres

2 applications trouvées

Nom	ID d'objet	ID d'application	URL de la page ...	Créé le	État d'expiration...	Date d'expiration...	URI d'identific
TAS	4e8b15bd-f025-493...	4c1beeea-6cdc-4835...	https://taseu.combta...	13/11/2024	-	-	4c1beeea-6cd
EmpCenter	8d8105c4-531c-477f...	34a9061c-f54c-4ffe...	https://*.empcenter...	13/11/2024	-	-	34a9061c-f54c

## II/ Ajouter une application personnalisée :

## Gestion des Réparations | Vue d'ensemble

- 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

### Propriétés

Nom GD Gestion des Réparations

ID d'application 56ab75b0-95bd-4fa7-b640-...

ID d'objet a83406fa-d59c-464d-9c71-...

### 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. Provisionner des comptes d'utilisateurs**  
Vous devez créer des comptes d'utilisateurs dans l'application  
[En savoir plus](#)

## Gestion des Réparations | Utilisateurs et groupes

- 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

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

L'application n'apparaît pas dans Mes applications pour les utilisateurs attribués. Définissez « Visible pour les utilisateurs ? » sur Oui dans les propriétés pour autoriser 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"/> DC Dylan Capron	Utilisateur	Default Access

Attribution à l'application réussie  
L'accès a été attribué à 1 utilisateur et 0 groupes

# Surveillance et Réponse aux Incidents

Default Directory | Journaux d'audit

Télécharger

Exporter les paramètres de données

Actualiser

Gérer la vue

Des commentaires ?

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 en bloc (préversion)

Dépannage + support

Annuaire

Sécurité personnalisée

Date ↓	Service	Catégorie	Activité	Statut	Motif du s
13/11/2024 14:00:41	Core Directory	UserManagement	Add app role assignmen...	Opération réussie	
13/11/2024 13:59:17	Core Directory	ApplicationManagement	Add service principal	Opération réussie	
13/11/2024 13:59:17	Core Directory	ApplicationManagement	Add application	Opération réussie	
13/11/2024 13:55:15	Core Directory	UserManagement	Add app role assignmen...	Opération réussie	
13/11/2024 13:46:56	Core Directory	ApplicationManagement	Update application	Opération réussie	
13/11/2024 13:46:56	Core Directory	ApplicationManagement	Update service principal	Opération réussie	
13/11/2024 13:46:55	Core Directory	ApplicationManagement	Add service principal	Opération réussie	
13/11/2024 13:46:55	Core Directory	ApplicationManagement	Add application	Opération réussie	
13/11/2024 13:35:42	Core Directory	UserManagement	Add app role assignmen...	Opération réussie	
13/11/2024 13:07:05	Core Directory	ApplicationManagement	Update application	Opération réussie	

## Créer un espace de travail Log Analytics

Grâce aux journaux Azure Monitor, vous pouvez facilement stocker, conserver et interroger les données collectées à partir de vos ressources supervisées dans Azure et d'autres environnements pour obtenir des insights intéressants. Un espace de travail Log Analytics est l'unité de stockage logique où vos données de journal sont collectées et stockées.

### Détails du projet

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement \* ⓘ

(Désactivé) Azure for Students

Groupe de ressources \* ⓘ

Créer nouveau

### Détails de l'instance

Nom \* ⓘ

Région \* ⓘ

East US