

AD

ENTREPRISES

GACI Hanafi
DERRI Tara

INTRODUCTION

Ce projet nous demandais de mettre en place la

Sécurisation de l'Infrastructure de l'USS Enterprise avec Azure AD

Pour ce projet, nous avons été chargés de sécuriser et d'automatiser la gestion des identités des membres d'équipage de l'USS Enterprise en utilisant microsoft Entra ID. nous allons expliquer pas à pas comment procéder pour atteindre les objectifs demandés.

Sécurité Avancée et Politiques de Sécurité

Étape 1 : Préparation de l'environnement

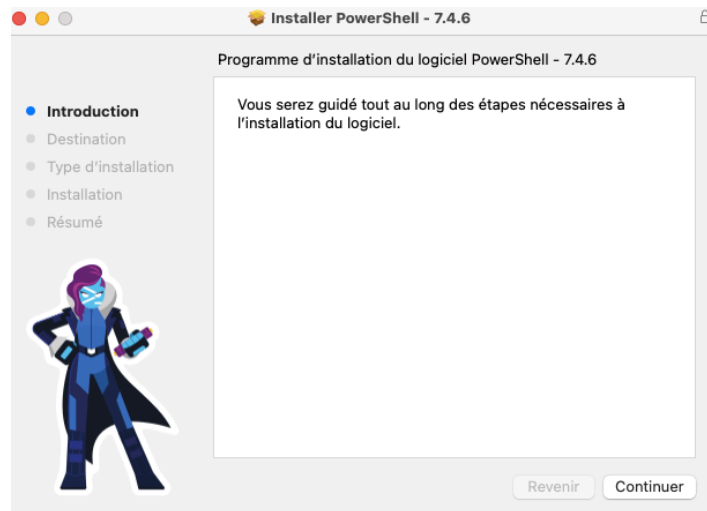
Création d'un compte Azure :

nous nous sommes rendus sur le [portail Azure](#) et créé un compte gratuit pour accéder à Azure AD.

Installation de PowerShell sur Mac :

Pour utiliser PowerShell sur macOS, on a installé via le téléchargement direct sur learn.microsoft.com avec la version PowerShell 7.4

processeurs x64 - [powershell-7.4.6-osx-x64.pkg](#) compatible avec notre MacBook



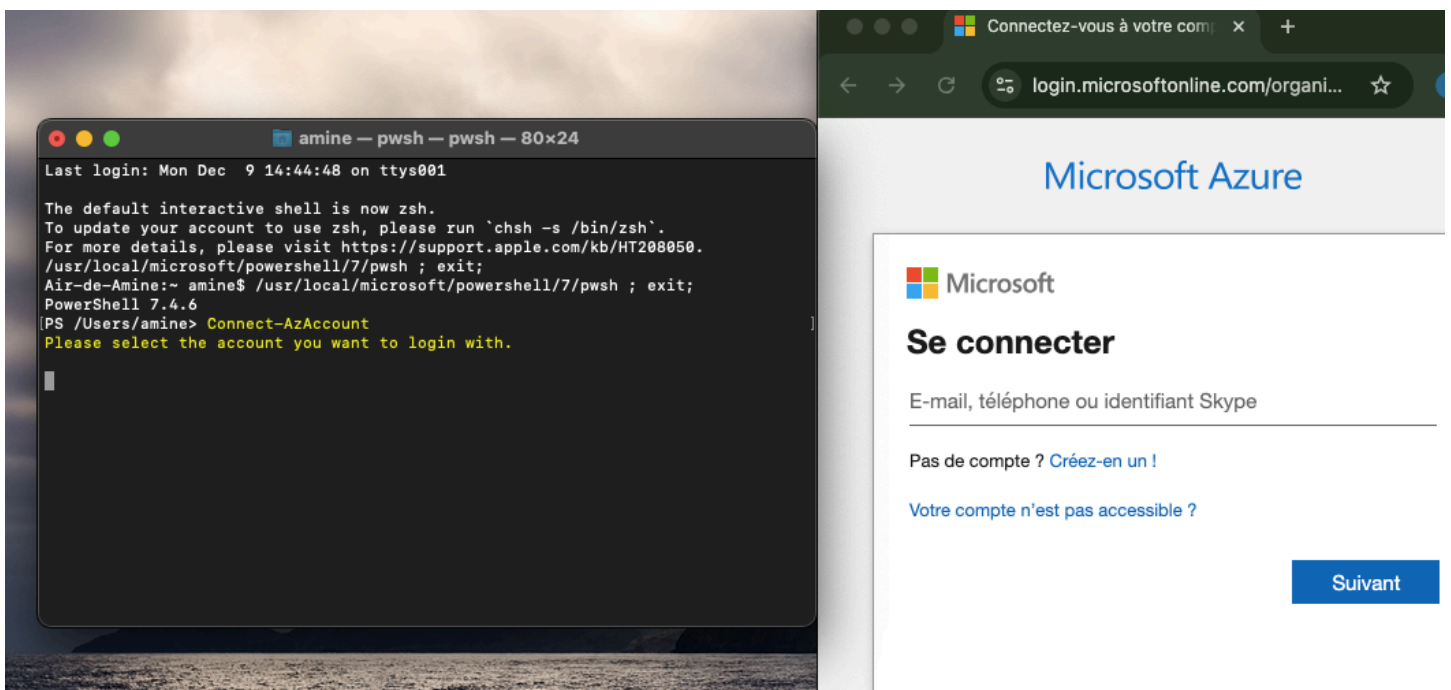
On a installé le module PowerShell qui nous permet de gérer Azure en exécutant :

```
Last login: Tue Dec 10 16:57:02 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
/usr/local/microsoft/powershell/7/pwsh ; exit;
Air-de-Amine:~ amine$ /usr/local/microsoft/powershell/7/pwsh ; exit;
PowerShell 7.4.6
PS /Users/amine> Install-Module -Name Az -AllowClobber -Scope CurrentUser

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from 'PSGallery'?
[[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
PS /Users/amine>
```

Ensuite, on se connecte au compte Azure avec :



```
[Announcements]
With the new Azure PowerShell login experience, you can select the subscription
you want to use more easily. Learn more about it and its configuration at https:
//go.microsoft.com/fwlink/?linkid=2271909.

If you encounter any problem, please open an issue at: https://aka.ms/azpsissue

Subscription name      Tenant
-----
Azure subscription 1  Répertoire par défaut

PS /Users/amine> █
```

Authentication complete. You can return to the application. Feel free to close this browser tab.

Étape 2 : Mise en place de la sécurité avancée

Étape 2 : Mise en place de la sécurité avancée

Pour renforcer la sécurité des identités dans Azure AD, nous avons activé l'authentification multifacteur (MFA) et créé des politiques d'accès conditionnel pour contrôler qui peut accéder à nos ressources. Voici les détails précis et de cette étape :

Étape 2 : Créer un groupe “Officiers Supérieurs”

Créer un nouveau groupe :

Cliquer sur **+ Nouveau groupe** en haut de l'écran.

Remplir les champs :

On a choisi en Type de groupe : **Sécurité**.

En nom : “Officiers Supérieurs”.

Sous **Appartenance au groupe**, on a choisis “Attribué pour ajouter manuellement les membres

puis on Clique sur **Créer** pour sauvegarder le groupe.

Nouveau groupe ...

 Des commentaires ?

Type de groupe * ⓘ

Sécurité

Nom du groupe * ⓘ

Officiers Supérieurs

Description du groupe ⓘ

Entrez une description pour le groupe

Type d'appartenance ⓘ

Affecté

Propriétaires

1 propriétaire sélectionné

Membres

Aucun membre sélectionné

Créer

1. Activer MFA pour les utilisateurs “officiers supérieurs”

Dans le menu , nous avons cliqué sur **Identités > Méthodes d’authentification**.

ensuite pour configurer la MFA :

Sous **Paramètres**, on a choisis **Méthodes d’authentification**.

on a Configuré les méthodes autorisées :

- **Les Application d’authentification** ici Microsoft Authenticator
- **et le SMS** comme alternative.

Sous **Politiques**, on a activé l’exigence d’authentification multifacteur pour les utilisateurs « officiers supérieurs » :

Dans **Utilisateurs ou groupes**, on a sélectionné le groupe contenant les officiers supérieurs et Activé l’application MFA.

Méthodes d'authentification | Stratégies

Répertoire par défaut – Sécurité dans Microsoft Entra ID

Rechercher

Ajouter une méthode externe (préversion)

Actualiser

Des commentaires ?

Gérer

Stratégies

Protection par mot de passe

Campagne d'inscription

Points forts d'authentification

Paramètres

Supervision

Stratégies de méthode d'authentification

Utilisez ces stratégies de méthodes d'authentification pour configurer les méthodes d'authentification que vos utilisateurs peuvent inscrire et utiliser. Si un utilisateur est dans l'étendue d'une méthode, il peut l'utiliser pour s'authentifier et pour la réinitialisation du mot de passe (certaines méthodes ne sont pas prises en charge dans certains scénarios). [En savoir plus](#)

Méthode	Cible	Activé
Intégré		
Clé d'accès (FIDO2)		Non
Microsoft Authenticator	1 groupe	Oui
SMS	1 groupe	Oui
Droit d'accès temporaire	Tous les utilisateurs	Oui
Jetons OATH matériels (préversion)		Non
Jetons OATH de logiciels tiers	Tous les utilisateurs	Oui
Appel vocal		Non
Mot de passe à usage unique par e-mail	Tous les utilisateurs	Oui
Authentification basée sur un certificat		Non

Paramètres Microsoft Authenticator

L'application Microsoft Authenticator est une méthode d'authentification phare, utilisable simplement via l'approbation de notification Push ou sans mot de passe. Le téléchargement de l'application est gratuit et disponible pour les appareils mobiles Android/iOS. [En savoir plus.](#)

Activer et cibler

Configurer

Activer

Inclure

Exclure

Cible

Tous les utilisateurs

Sélectionner des groupes

Ajouter des groupes

Nom	Type	Inscription	Mode d'authentification
Officiers Supérieurs	Groupe	Facultatif	N'importe lequel

Simulation détaillée des politiques d'accès conditionnel : Blocage depuis des emplacements non approuvés

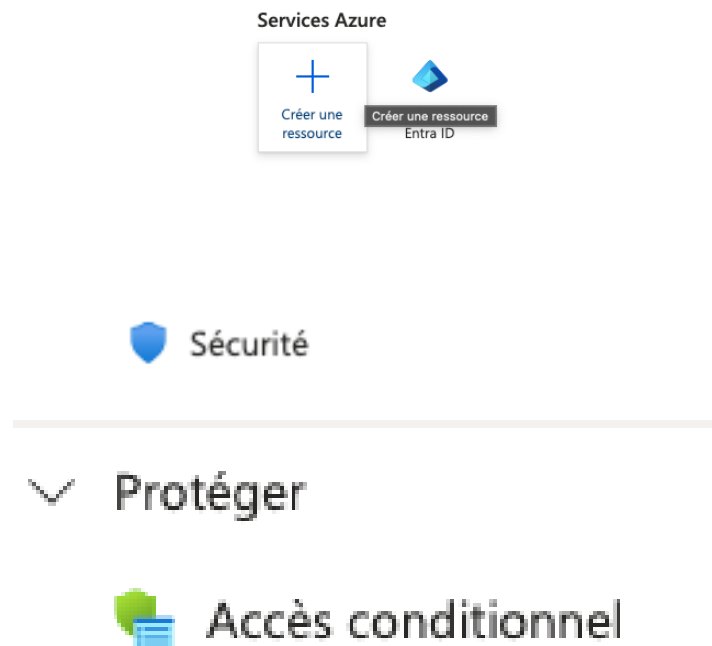
Bien que nous n'ayons pas accès à un abonnement Premium pour configurer directement des politiques d'accès conditionnel dans **Microsoft Entra ID**, voici un guide étape par étape détaillé pour expliquer comment nous aurions configuré cette politique si elle était disponible. en décrivant chaque action en détail

le but est donc de Créer une politique d'accès conditionnel permettant d'autoriser l'accès uniquement depuis des emplacements approuvés. D'exiger MFA pour toute tentative de connexion depuis des emplacements non approuvés et de bloquer complètement les connexions provenant de zones inconnues ou non définies.

1. Accéder à la configuration des politiques d'accès conditionnel

il faut commencer par Naviguer vers "Accès conditionnel" :

Dans le menu de gauche, cliquer sur Identités. et ensuite Sous Sécurité, cliquer sur Accès conditionnel.



1. Créer une nouvelle politique :

Cliquer sur **+ Nouvelle stratégie** en haut de l'écran.

Une nouvelle page s'ouvre pour configurer la politique.

Accès conditionnel | Vue d'ensemble ...

Microsoft Entra ID

◊ « + Créer une nouvelle stratégie + Créer une stratégie à partir de modèles |

Nous n'avons pas d'accès premium mais voici nos recherches sur comment procéder et comment mettre ca en place et créer une nouvelle stratégie :

Configurer la politique d'accès conditionnel:

Nommer la politique :

- Dans la section Nom, entrer un nom explicite, comme "Restreindre l'accès depuis des emplacements non approuvés" pour notre devoir

Définir les utilisateurs ou groupes affectés :

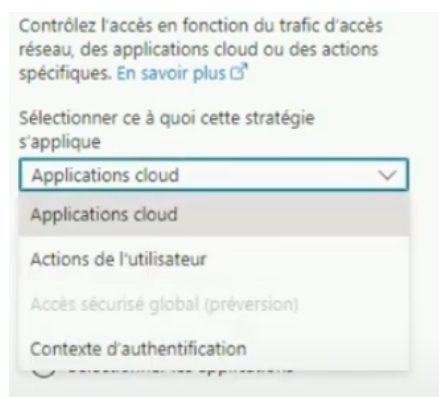
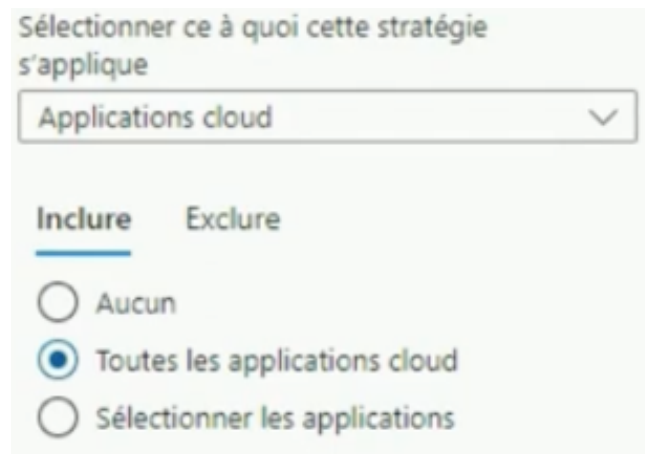
Sous Affectations, cliquez sur Utilisateurs ou groupes.

Sélectionnez Utilisateurs et groupes spécifiques, puis ajoutez le groupe Officiers Supérieurs (ou les utilisateurs spécifiques concernés).

Sélectionner les applications cloud :

Cliquer sur Applications ou actions cloud et Sélectionner Toutes les applications cloud si la

politique doit s'appliquer à toutes les applications.



Pour Configurer les conditions (emplacements) :

Cliquer sur Conditions, puis sur Emplacements.

Activer les emplacements en basculant le bouton sur Oui.



Configurer les emplacements :

Cliquer sur Configurer les emplacements > Nouveaux emplacements nommés.

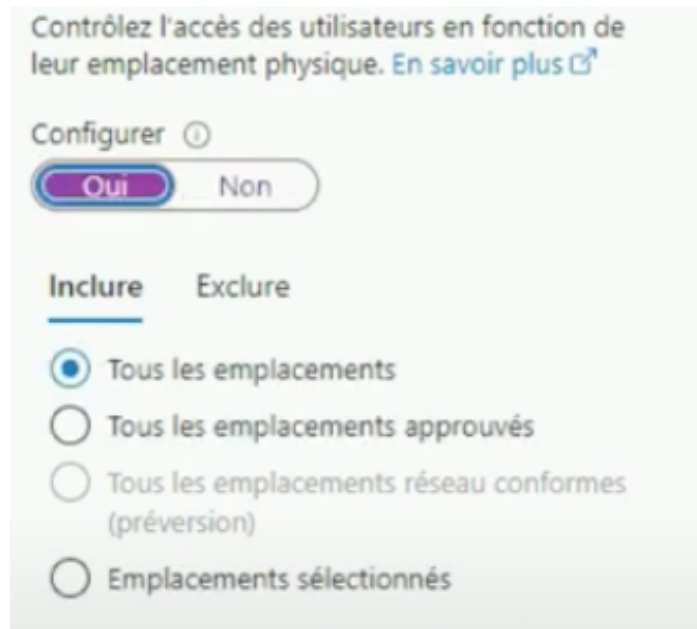
Ajouter un emplacement nommé Réseau USS Enterprise avec l'adresse IP du vaisseau.

Ajouter un autre emplacement nommé Stations approuvées avec les adresses IP des stations spatiales.

Dans la politique principale, sélectionner Tous les emplacements et choisir :

Autoriser uniquement les connexions depuis les emplacements approuvés.

Bloquer l'accès depuis tous les autres emplacements.



pour Configurer les contrôles d'accès :

Cliquer sur Contrôles d'accès > Accorder.

Sélectionner Exiger une authentification multifacteur (MFA) pour les connexions depuis des emplacements non approuvés.

Activer également l'option Bloquer l'accès pour les connexions depuis des zones inconnues.



Octroyer ×

Contrôlez l'application de l'accès pour bloquer ou accorder l'accès.
[En savoir plus](#)

☒ Bloquer l'accès
☐ Accorder l'accès

☒ Exiger une authentification multifacteur ⓘ

☐ Exiger la force de l'authentification ⓘ

☐ Exiger que l'appareil soit marqué comme conforme ⓘ

☐ Exiger un appareil avec jointure Microsoft Entra hybride ⓘ

☐ Demander une application cliente approuvée
[Voir la liste des applications clientes approuvées](#) ⓘ

☐ Exiger une stratégie de ⓘ

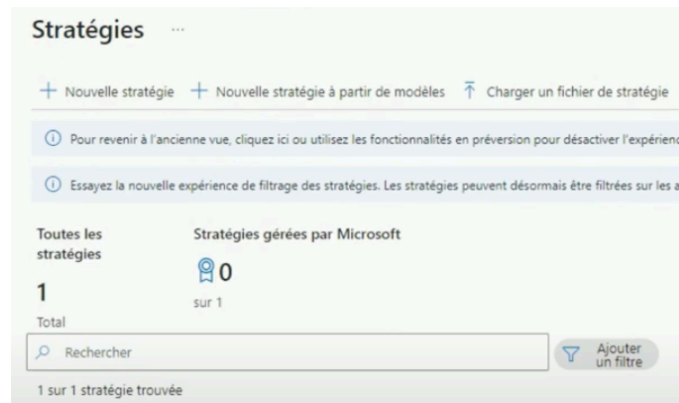
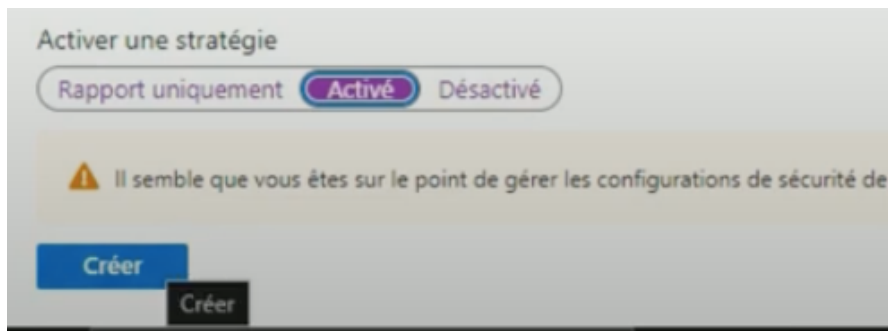
Sélectionner

MA

Pour Activer la politique :

Sous **Activer la politique**, choisir **Activé**.

Cliquer sur **Créer** pour finaliser la politique.



3. Tester la politique (simulation)

Si la politique était active, voici comment on testera son fonctionnement :

Test depuis un emplacement approuvé :

1. Configurer un terminal ou un appareil pour utiliser une adresse IP dans la plage approuvée (par exemple, 192.168.1.50).
2. Se connecter à une application cloud
3. Attendu : La connexion est autorisée sans demande MFA.

Test depuis un emplacement non approuvé :

1. Simuler une connexion depuis un emplacement non approuvé en utilisant un VPN avec une adresse IP externe (par exemple, 203.0.113.45).
2. se connecter avec le même compte.
3. Attendu : La connexion est autorisée uniquement après validation via MFA.

Test depuis une zone inconnue :

1. Configurer une connexion via un proxy ou VPN avec une adresse IP aléatoire (par exemple, 45.67.89.123).
2. Essayer de se connecter à l'application cloud.

3. Attendu : L'accès est bloqué avec un message indiquant que la connexion provient d'un emplacement non approuvé.

Automatisation avec PowerShell

nous avons créé des utilisateurs dans **Microsoft Entra ID** en utilisant **PowerShell** pour automatiser le processus. Voici une explication détaillée de chaque étape et des lignes de commande utilisées,

Nous avons préparé notre environnement PowerShell pour travailler avec Microsoft Entra ID et se connecter

```
[PS /Users/amine> connect-AzAccount
Please select the account you want to login with.

Retrieving subscriptions for the selection...

Subscription name      Tenant
-----
Azure subscription 1  Répertoire par défaut

PS /Users/amine> █
```

Cette commande nous permet de nous connecter à notre Microsoft Entra ID. Après l'exécution, nous avons entré nos identifiants de connexion pour nous authentifier.

Authentication complete. You can return to the application. Feel free to close this browser tab.

Création des utilisateurs

Nous avons créé plusieurs utilisateurs en une seule exécution grâce à un script PowerShell.

```

PS /Users/amine> $users = @(
>> @{ DisplayName = "James Kirk"; UserPrincipalName = "kirk@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString "TaraH@nafi123" -AsPlainText -Force); MailNickname = "kirk" },
>> @{ DisplayName = "Spock"; UserPrincipalName = "spock@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString "TaraH@nafi123" -AsPlainText -Force); MailNickname = "spock" },
>> @{ DisplayName = "Leonard McCoy"; UserPrincipalName = "mccoy@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString "TaraH@nafi123" -AsPlainText -Force); MailNickname = "mccoy"
>> }
PS /Users/amine>
PS /Users/amine> foreach ($user in $users) {
>>     New-AzADUser -DisplayName $user.DisplayName -UserPrincipalName $user.UserPrincipalName -Password $user.Password -MailNickname $user.MailNickname -Force
>>     Write-Host "Utilisateur $($user.DisplayName) créé avec succès !"
>> }

```

Nous avons créé un script contenant trois utilisateurs :

- **DisplayName** : Le nom complet de l'utilisateur
- **UserPrincipalName** : L'adresse e-mail utilisée comme identifiant principal pour nous c'est hanafigacilaplateforme.onmicrosoft.com
- **Password** : qui respecte les exigences de complexité des mots de passe configurées dans Microsoft Entra ID. et Converti en **SecureString** un format sécurisé pour les mots de passe
- **MailNickname** : Un surnom unique pour chaque utilisateur.
- **-Force** : Ignore les confirmations et crée directement l'utilisateur.
- **Write-Host** : Affiche un message confirmant la création de l'utilisateur.

voici le résultat :

```

PS /Users/amine> $users = @(
>> @{ DisplayName = "James Kirk"; UserPrincipalName = "kirk@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString "TaraH@nafi123" -AsPlainText -Force); MailNickname = "kirk" },
>> @{ DisplayName = "Spock"; UserPrincipalName = "spock@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString "TaraH@nafi123" -AsPlainText -Force); MailNickname = "spock" },
>> @{ DisplayName = "Leonard McCoy"; UserPrincipalName = "mccoy@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString "TaraH@nafi123" -AsPlainText -Force); MailNickname = "mccoy"
>> }
PS /Users/amine>
PS /Users/amine> foreach ($user in $users) {
>>     New-AzADUser -DisplayName $user.DisplayName -UserPrincipalName $user.UserPrincipalName -Password $user.Password -MailNickname $user.MailNickname -Force
>>     Write-Host "Utilisateur $($user.DisplayName) créé avec succès !"
>> }

```

```

AccountEnabled      :
AgeGroup            :
ApproximateLastSignInDateTime :
BusinessPhone       : {}
City                :
CompanyName          :
ComplianceExpirationDateTime :
ConsentProvidedForMinor :
Country             :
CreatedDateTime      :
CreationType         :
DeletedDateTime      :
Department          :
DeviceVersion        :
DisplayName           : James Kirk
EmployeeHireDate     :
EmployeeId           :
EmployeeOrgData      : {}
EmployeeType         :
ExternalUserState    :
ExternalUserStateChangeDateTime :
FaxNumber            :
GivenName            :
Id                   : 8461ac87-e141-44aa-960a-86e2a5786e9f
Identity             :
ImAddress            :
IsResourceAccount    :
JobTitle             :
LastPasswordChangeDateTime :
LegalAgeGroupClassification :
Mail                 :
MailNickname         :

```

```

Manager          : {
MobilePhone      :
OdataId         :
OdataType        : #microsoft.graph.user
OfficeLocation   :
OnPremisesImmutableId :
OnPremisesLastSyncDateTime :
OnPremisesSyncEnabled :
OperatingSystem  :
OperatingSystemVersion :
OtherMail        :
PasswordPolicy   :
PasswordProfile  : {
PhysicalId       :
PostalCode       :
PreferredLanguage :
ProxyAddress     :
ResourceGroupName :
ShowInAddressList :
SignInSessionsValidFromDateTime :
State            :
StreetAddress    :
Surname          :
TrustType        :
UsageLocation    :
UserPrincipalName : kirk@hanafigacilaplateforme.onmicrosoft.com
UserType         :
AdditionalProperties : {["@odata.context", https://graph.microsoft.com/v1.0/$metadata#users/$entity], [id, 8461ac87-e141-44aa-960a-86e2a5786e9f]}

```

Utilisateur James Kirk créé avec succès !

```

AccountEnabled   :
AgeGroup         :
ApproximateLastSignInDateTime :
BusinessPhone    : {}
City            :
CompanyName      :
ComplianceExpirationDateTime :
ConsentProvidedForMinor :
Country         :
CreatedDateTime  :
CreationType     :
DeletedDateTime  :
Department       :
DeviceVersion    :
DisplayName      : Spock
EmployeeHireDate :
EmployeeId       :
EmployeeOrgData  : {
EmployeeType     :
ExternalUserState :
ExternalUserStateChangeDateTime :
FaxNumber        :
GivenName        :
Id               : 7e84a59e-907d-4bed-801d-64e76870cfb6
Identity         :
ImAddress        :
IsResourceAccount :
JobTitle         :

```

```

JobTitle         :
LastPasswordChangeDateTime :
LegalAgeGroupClassification :
Mail            :
MailNickname    :
Manager         : {
MobilePhone      :
OdataId         :
OdataType        : #microsoft.graph.user
OfficeLocation   :
OnPremisesImmutableId :
OnPremisesLastSyncDateTime :
OnPremisesSyncEnabled :
OperatingSystem  :
OperatingSystemVersion :
OtherMail        :
PasswordPolicy   :
PasswordProfile  : {
PhysicalId       :
PostalCode       :
PreferredLanguage :
ProxyAddress     :
ResourceGroupName :
ShowInAddressList :
SignInSessionsValidFromDateTime :
State            :
StreetAddress    :
Surname          :
TrustType        :
UsageLocation    :
UserPrincipalName : spock@hanafigacilaplateforme.onmicrosoft.com
UserType         :
AdditionalProperties : {["@odata.context", https://graph.microsoft.com/v1.0/$metadata#users/$entity], [id, 7e84a59e-907d-4bed-801d-64e76870cfb6]}

```

Utilisateur Spock créé avec succès !

```

State           :
StreetAddress    :
Surname         :
TrustType       :
UsageLocation    :
UserPrincipalName : mccoy@hanafigacilaplateforme.onmicrosoft.com
UserType        :
AdditionalProperties : {["@odata.context", https://graph.microsoft.com/v1.0/$metadata#users/$entity], [id, 06f3ec5c-913e-4313-a718-ca615bda6fa1]}

```

Utilisateur Leonard McCoy créé avec succès !

PS /Users/amine> █

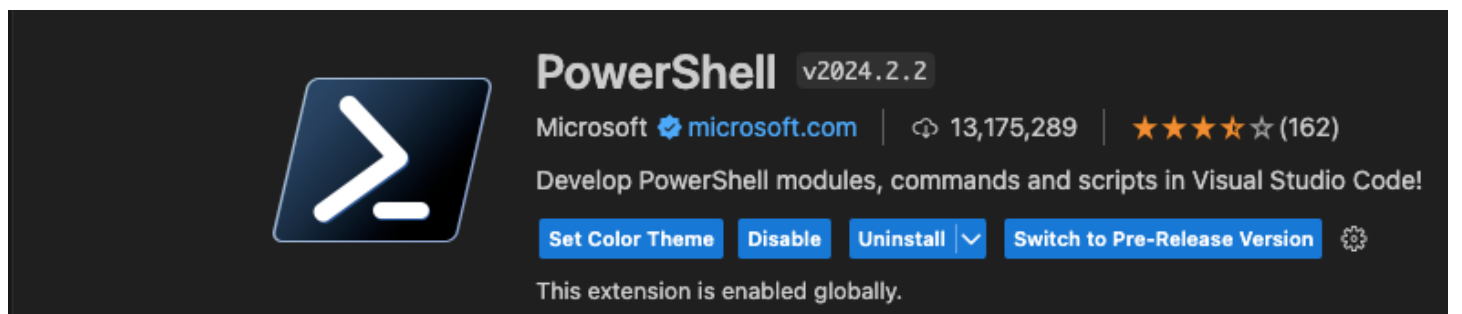
nous avons enregistré le fichier via VSCode pour sauvegarder toutes tes commandes PowerShell dans un fichier, que l'on pourra réutiliser et exécuter

nous avons autorisé l'exécution de fichiers PowerShell

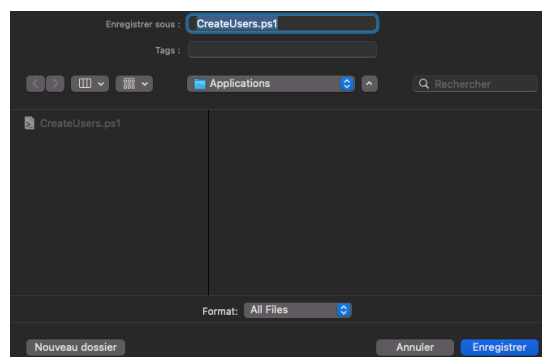
```
Air-de-Amine:~ amine$ chmod +x ~/Applications/CreateUsers.ps1
Air-de-Amine:~ amine$ ls -l ~/Applications/CreateUsers.ps1
-rwxr-xr-x  1 amine  staff   873 13 déc 19:13 /Users/amine/Applications/CreateUsers.ps1
Air-de-Amine:~ amine$
```

on crée le fichier sur Visual studio code

```
> CreateUsers.ps1 • Extension: PowerShell
Users > amine > Applications > > CreateUsers.ps1 > ...
1  $users = @(
2      @{ DisplayName = "James Kirk"; UserPrincipalName = "kirk@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString
3      @{ DisplayName = "Spock"; UserPrincipalName = "spock@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureString "Ta
4      @{ DisplayName = "Leonard McCoy"; UserPrincipalName = "mccoy@hanafigacilaplateforme.onmicrosoft.com"; Password = (ConvertTo-SecureSt
5  )
6
7  foreach ($user in $users) {
8      New-AzADUser -DisplayName $user.DisplayName -UserPrincipalName $user.UserPrincipalName -Password $user.Password -MailNickname $user.
9      Write-Host "Utilisateur $($user.DisplayName) créé avec succès !"
10 }
```



puis on l'a enregistré.



Les utilisateurs sont bien créés en vérifiant via le répertoire des utilisateurs Microsoft entra ID

Utilisateurs

Répertoire par défaut

Rechercher

Nouvel utilisateur

Supprimer

Télécharger les utilisateurs

Opérations en bloc

Actualiser

Gérer l'affichage

MFA par utilisateur

Tous les utilisateurs

Journaux d'audit

Journaux de connexion

Diagnostic et résoudre les problèmes

Utilisateurs supprimés

Réinitialisation du mot de passe

Paramètres utilisateur

Résultats de l'opération en bloc

Nouvelle demande de support

Azure Active Directory s'appelle désormais Microsoft Entra ID

Rechercher

Ajouter un filtre

4 utilisateurs trouvés

	Nom d'affichage ↑	Nom d'utilisateur principal ↑	Type d'utilisateur	Synchronisatio...	Identités	Nom de l'entreprise	Type d
<input type="checkbox"/>	HG hanafi gaci	hanafi.gaci_laplateforme.i...	Membre	Non	MicrosoftAccount		
<input type="checkbox"/>	JK James Kirk	kirk@hanafigacilaplatefor...	Membre	Non	hanafigacilaplateforme.onmicroso		
<input type="checkbox"/>	LM Leonard McCoy	mccoy@hanafigacilaplate...	Membre	Non	hanafigacilaplateforme.onmicroso		
<input type="checkbox"/>	S Spock	spock@hanafigacilaplatef...	Membre	Non	hanafigacilaplateforme.onmicroso		

Script pour gérer les groupes

on a d'abord Installé le module Microsoft.Graph puis on s'est connectés . (Accès aux données Microsoft)

```
PS /Users/amine> Install-Module Microsoft.Graph -Scope CurrentUser

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS /Users/amine>
```

Ajouter des utilisateurs à un groupe

nous avons exécuté ce script pour ajouter des utilisateurs aux groupes "equipe medicale" et "equipe dexploration".

```
PS /Users/amine> $groupName = "equipe medicale"
PS /Users/amine> $users = @(
>> "kirk@hanafigacilaplateforme.onmicrosoft.com",
>> "spock@hanafigacilaplateforme.onmicrosoft.com"
>> )
PS /Users/amine>
PS /Users/amine> $group = Get-AzADGroup -DisplayName $groupName
PS /Users/amine>
PS /Users/amine> if ($group) {
>> foreach ($userPrincipalName in $users) {
>>     $user = Get-AzADUser -UserPrincipalName $userPrincipalName
>>     if ($user) {
>>         Add-AzADGroupMember -TargetGroupId $group.Id -MemberId $user.Id
>>         Write-Host "Utilisateur $($user.DisplayName) ajouté au groupe $groupName avec succès !"
>>     } else {
>>         Write-Host "Utilisateur $userPrincipalName introuvable. Ajout ignoré."
>>     }
>> }
>> } else {
>>     Write-Host "Groupe $groupName introuvable."
>> }
```

Utilisateur James Kirk ajouté au groupe equipe medicale avec succès !

Utilisateur Spock ajouté au groupe equipe medicale avec succès

Membres

...

equipe medicale

Ajouter des membres

Opérations en bloc

Actualiser

Gérer la vue

Supprimer

Des commentaires ?

Membres directs

Tous les membres

Rechercher

Ajouter un filtre

2 membres de groupe trouvés

<input type="checkbox"/>	Nom ↑	Type	E-mail	Type d'utilisat...	ID d'objet	ID de l'appa
<input type="checkbox"/>	<div><div>JK</div>James Kirk</div>	Utilisateur		Membre	8461ac87-e141-44aa-960a-86e2a5786e9f	
<input type="checkbox"/>	<div><div>S</div>Spock</div>	Utilisateur		Membre	7e84a59e-907d-4bed-801d-64e76870cfb6	

```
PS /Users/amine> $groupName = "equipe dexploration"
PS /Users/amine> $users = @(
>> "mccoy@hanafigacilaplateforme.onmicrosoft.com",
>> "spock@hanafigacilaplateforme.onmicrosoft.com"
>> )
PS /Users/amine>
PS /Users/amine>
PS /Users/amine> $group = Get-AzADGroup -DisplayName $groupName
PS /Users/amine>
PS /Users/amine> if ($group) {
>>     foreach ($userPrincipalName in $users) {
>>         $user = Get-AzADUser -UserPrincipalName $userPrincipalName
>>         if ($user) {
>>             Add-AzADGroupMember -GroupId $group.Id -MemberId $user.Id
>>             Write-Host "Utilisateur $($user.DisplayName) ajouté au groupe $groupName avec succès !"
>>         } else {
>>             Write-Host "Utilisateur $userPrincipalName introuvable. Ajout ignoré."
>>         }
>>     }
>> } else {
>>     Write-Host "Groupe $groupName introuvable."
>> }
```

Utilisateur Leonard McCoy ajouté au groupe equipe dexploration avec succès !

Utilisateur Spock ajouté au groupe equipe dexploration avec succès !

equipe dexploration | Membres

...

Groupe

Ajouter des membres

Opérations en bloc

Actualiser

Gérer la vue

Supprimer

Des commentaires ?

Vue d'ensemble

Diagnostiquer et résoudre les problèmes

Gérer

Propriétés

Membres

Propriétaires

Rôles et administrateurs

Unités administratives

Appartenances aux groupes

Membres directs

Tous les membres

Rechercher

Ajouter un filtre

2 membres de groupe trouvés

<input type="checkbox"/>	Nom ↑	Type	E-mail	Type d'utilisat...	ID d'objet
<input type="checkbox"/>	<div><div>LM</div>Leonard McCoy</div>	Utilisateur		Membre	06f3ec5c-91
<input type="checkbox"/>	<div><div>S</div>Spock</div>	Utilisateur		Membre	7e84a59e-907d-4bed-801d-64e76870cfb6

Supprimer des utilisateurs d'un groupe

avec ce script on supprime automatiquement des utilisateurs spécifiques des groupes "equipe medicale" et "equipe dexploration".

```
PS /Users/amine> $groupName = "equipe dexploration"
PS /Users/amine> $users = @(
>>     "mccoy@hanafigacilaplateforme.onmicrosoft.com",
>>     "spock@hanafigacilaplateforme.onmicrosoft.com"
>> )
PS /Users/amine>
PS /Users/amine>
PS /Users/amine> $group = Get-AzADGroup -DisplayName $groupName
PS /Users/amine>
PS /Users/amine> if ($group) {
>>     foreach ($userPrincipalName in $users) {
>>         $user = Get-AzADUser -UserPrincipalName $userPrincipalName
>>         if ($user) {
>>             Remove-AzADGroupMember -TargetGroupId $group.Id -MemberId $user.Id -Force
>>             Write-Host "Utilisateur $($user.DisplayName) supprimé du groupe $groupName avec succès !"
>>         } else {
>>             Write-Host "Utilisateur $userPrincipalName introuvable. Suppression ignorée."
>>         }
>>     }
>> } else {
>>     Write-Host "Groupe $groupName introuvable."
>> }
```

Utilisateur Leonard McCoy supprimé du groupe equipe dexploration avec succès !

```
Utilisateur Spock supprimé du groupe equipe dexploration avec succès !
```

equipe depxloration | Membres

Groupe

Vue d'ensemble

Diagnostiquer et résoudre les problèmes

Gérer

Propriétés

Membres

Propriétaires

Rôles et administrateurs

+

Ajouter des membres

Opérations en bloc

Actualiser

Gérer la vue

X Supprimer

Des commentaires ?

Membres directs

Tous les membres

Rechercher
 Ajouter un filtre

0 membres de groupe trouvés

<input type="checkbox"/>	Nom ↑	Type	E-mail	Type d'utilisat...	ID d'objet
Aucun membre n'a été trouvé					

```
PS /Users/amine> $groupName = "equipe medicale"
PS /Users/amine> $users = @(
>>     "kirk@hanafigacilaplateforme.onmicrosoft.com",
>>     "spock@hanafigacilaplateforme.onmicrosoft.com"
>> )
PS /Users/amine>
PS /Users/amine>
PS /Users/amine> $group = Get-AzADGroup -DisplayName $groupName
PS /Users/amine>
PS /Users/amine> if ($group) {
>>     foreach ($userPrincipalName in $users) {
>>         $user = Get-AzADUser -UserPrincipalName $userPrincipalName
>>         if ($user) {
>>             Remove-AzADGroupMember -TargetGroupId $group.Id -MemberId $user.Id -Force
>>             Write-Host "Utilisateur $($user.DisplayName) supprimé du groupe $groupName avec succès !"
>>         } else {
>>             Write-Host "Utilisateur $userPrincipalName introuvable. Suppression ignorée."
>>         }
>>     }
>> } else {
>>     Write-Host "Groupe $groupName introuvable."
>> }
```

Utilisateur James Kirk supprimé du groupe equipe medicale avec succès !

Utilisateur Spock supprimé du groupe equipe medicale avec succès !

Membres ...

equipe medicale

+ Ajouter des membres Opérations en bloc Actualiser Gérer la vue Supprimer Des commentaires ?

Membres directs Tous les membres

Rechercher

Ajouter un filtre

0 membres de groupe trouvés

<input type="checkbox"/>	Nom ↑	Type	E-mail	Type d'utilisat...	ID d'objet	ID de l'app
--------------------------	-------	------	--------	--------------------	------------	-------------

Aucun membre n'a été trouvé

Déplacer les utilisateurs d'un groupe a un autre

```
PS /Users/amine>
PS /Users/amine> Function Move-AzureADMember {
>>     param (
>>         [string]$UserId, # ID de l'utilisateur
>>         [string]$SourceGroupId, # ID du groupe source
>>         [string]$DestinationGroupId # ID du groupe destination
>>     )
>>
>>     # Retirer l'utilisateur du groupe source
>>     Remove-MgGroupMember -GroupId $SourceGroupId -DirectoryObjectId $UserId
>>
>>     # Ajouter l'utilisateur au groupe destination
>>     Add-MgGroupMember -GroupId $DestinationGroupId -DirectoryObjectId $UserId
>>
>>     Write-Host "Utilisateur déplacé avec succès."
>> }
PS /Users/amine>
PS /Users/amine> # Déplacer plusieurs utilisateurs avec leurs informations
PS /Users/amine> $Utilisateur = "kirk1@hanafigacilaplateforme.onmicrosoft.com"
PS /Users/amine> $GroupeSource = "groupe medical"
PS /Users/amine> $GroupeDestination = "groupe dexploration"
PS /Users/amine>
PS /Users/amine> $UserId = (Get-MgUser -Filter "userPrincipalName eq '$Utilisateur']").Id
```

```
Utilisateur déplacé avec succès.
PS /Users/amine> █
```

Pour appliquer les politiques de sécurité pour les missions sensibles nous devons procéder comme pour précédemment dans le job 1 car nous n'avons pas les accès premium

Intégration et Sécurisation des Applications

Dans cette partie du projet, nous allons intégrer des applications SaaS et une application personnalisée avec Microsoft Entra ID pour un accès sécurisé. Nous allons aussi configurer le Single Sign-On (SSO) pour simplifier l'authentification des membres d'équipage, puis gérer les permissions d'accès pour une application personnalisée destinée à l'équipe d'ingénierie.

1. Intégrer des applications SaaS avec Microsoft Entra ID

- Trello : Remplace le “Centre de Commandement” pour la gestion des tâches et des projets.
- Microsoft Teams : Remplace le “Journal du Capitaine” pour la collaboration d'équipe et la gestion des communications.

nous avons navigué vers **Applications d'entreprise > + Nouvelle application**.



nous avons recherché **Trello** dans la **Galerie des Applications** et l'avons ajoutée

Parcourir la galerie Microsoft Entra

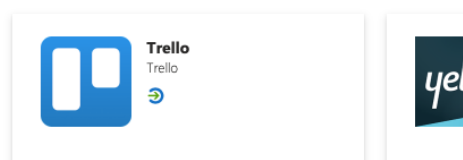
+ Créer votre propre application | Des commentaires ?

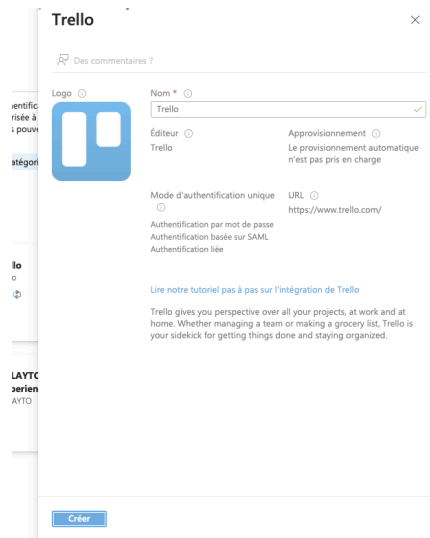
La galerie d'applications Microsoft Entra est un catalogue de milliers d'applications. À partir de la galerie d'applications, vous tirez parti des applications que vous avez développées dans la galerie Microsoft Entra.

trelo x Authentificat

SSO fédéré Appvisionnement

Affichage de 8 sur 8 résultats





Trello étant une application tierce, nous l'avons ajoutée manuellement depuis la galerie des applications SaaS.

Configurer le Single Sign-On (SSO) :

- Dans la page de configuration de Trello, nous avons accédé à l'onglet **Authentification unique**.


Trello | Authentification unique

Application d'entreprise

Vue d'ensemble

Plan de déploiement

Diagnostic et résoudre les

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](#).



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](#)

Sélectionner une méthode d'authentification unique [Aidez-moi à choisir](#)



- Nous avons choisi SAML comme méthode d'authentification, car SAML garantit un accès sécurisé à Trello, en utilisant les identifiants gérés par Entra ID.

Configuration SAML de base

- Nous avons configuré les paramètres suivants :
 - **URL SAML d'ACS** :: <https://trello.com/auth/saml/consume/starfleet>

Cette URL permet à Trello de recevoir et de traiter les informations d'identification des utilisateurs depuis Entra ID.

- **Identifiant (ID d'émetteur)** : <https://trello.com/auth/saml/metadata>

Cette URL est le point d'entrée principal où Microsoft Entra ID et Trello échangent des informations SAML.

Configuration SAML de base

>

[Enregistrer](#) | [Des commentaires ?](#)

Identificateur (ID d'entité) * ⓘ

ID unique qui identifie votre application à Microsoft Entra ID. Cette valeur doit être unique dans toutes les applications de votre locataire Microsoft Entra. L'identificateur par défaut sera l'audience de la réponse SAML pour l'authentification unique initiée par IDP.

Par défaut

 ✓[Ajouter un identificateur](#)**Modèles :** https://trello.com/auth/saml/metadata

URL de réponse (URL Assertion Consumer Service) * ⓘ

L'URL de réponse correspond à l'emplacement où l'application est supposée recevoir le jeton d'authentification. Cette URL est parfois appelée « Assertion Consumer Service » (ACS) dans SAML.

Index

Par défaut

 ✓[Ajouter une URL de réponse](#)**Modèles :** https://trello.com/auth/saml/consume/EXAMPLE

Enregistrer la configuration de

Des commentaires ? unique

La configuration de l'authentification unique a été enregistrée.



- Nous avons téléchargé le fichier de métadonnées SAML fourni par Entra ID et l'avons importé dans le tableau de bord administratif de Trello.

XML de métadonnées de fédération

[Télécharger](#)

Ce fichier contient des informations cryptographiques nécessaires pour établir une communication sécurisée entre Entra ID et Trello. Il inclut des détails comme l'URL d'authentification et le certificat public.

Dans les paramètres SSO de Trello :

- Nous avons recherché l'option pour **Importer les métadonnées SAML**

- on Téléverse le fichier qu'on a téléchargé depuis Entra ID.

tout ca afin que cela configure Trello pour qu'il reconnaisse Microsoft Entra ID comme fournisseur d'identité.

Voici ce que vous devez faire avant de configurer l'authentification unique SAML :

- ✔ Abonnez-vous à Atlassian Guard Standard de votre organisation. [Comprendre Atlassian Guard](#)
- ✔ Assurez-vous d'être administrateur d'une organisation Atlassian.
- ✔ Vérifiez un ou plusieurs de vos domaines dans votre organisation. [Comment vérifier un domaine](#)
- ✔ Ajoutez un répertoire de fournisseur d'identité à votre organisation. [Comment ajouter un fournisseur d'identité](#)
- ✔ Liez les domaines vérifiés à votre répertoire de fournisseur d'identité. [Comment lier des domaines](#)
- ✔ Vérifiez que votre produit Atlassian et votre fournisseur d'identité utilisent le protocole HTTPS pour communiquer et que l'URL de base de produit configurée est celle de HTTPS.

Voici ce que nous vous recommandons de faire avant de configurer l'authentification unique SAML :

- ✔ Assurez-vous que l'horloge sur votre serveur de fournisseur d'identité est synchronisée avec NTP. Les demandes d'authentification SAML ne sont valables que pour une durée limitée.
- ✔ Planifiez le temps d'arrêt pour configurer et tester votre configuration SAML.
- ✔ Créez une politique d'authentification pour tester votre configuration SAML . Ajoutez un utilisateur à la politique de test. Après avoir configuré SAML, vous pouvez activer l'authentification unique pour la politique de test.

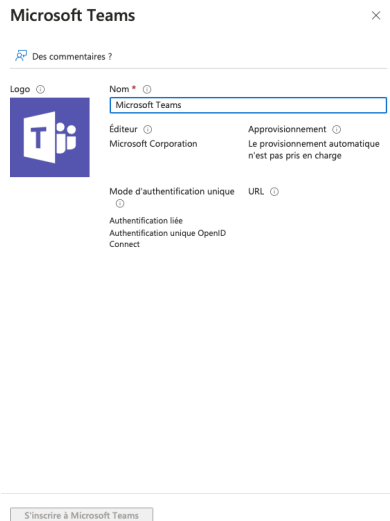
Tester l'accès à Trello pour les membres de l'équipage :

- tester l'accès en se connectant avec un compte utilisateur
- L'utilisateur a pu accéder à Trello sans entrer de mot de passe supplémentaire, grâce au SSO.

On fait la même chose pour Microsoft Teams

Nous sommes allés dans Applications d'entreprise

Sous la section Toutes les applications, nous avons trouvé Microsoft Teams.



si nous avions pu le télécharger nous aurions suivi les étapes suivantes
accédé à l'onglet Utilisateurs et groupes dans la page de configuration de Teams.
affecté les groupes suivants à l'application :

- Officiers Supérieurs : Pour accéder à la gestion stratégique.
- Équipe d'exploration : Pour la coordination des missions.

Une fois les groupes ajoutés, il faut enregistrer les modifications.

Tester l'accès à Teams pour les membres d'équipage :

- se connecter avec un compte
- accéder à Teams et confirmer que l'authentification SSO fonctionnait correctement.

2. Ajouter une application personnalisée : Gestion des Réparations

Créer une application personnalisée :

- Nous avons cliqué sur **+ Nouvelle application** dans **Applications d'entreprise**.



+ Nouvelle application

+ Créer votre propre application

- Nous avons sélectionné **Créer votre propre application** et entré le nom **Gestion des Réparations**.
- Nous avons choisi **Intégrer toute autre application que vous ne trouvez pas dans la galerie**.
- Nous avons cliqué sur **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 Réparation ✓

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

Configurer l'authentification unique (SSO) :

- Nous avons accédé à l'onglet **Authentification unique** et sélectionné **SAML**.

Configuration SAML de base



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](#)

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).



Authentification par mot de passe

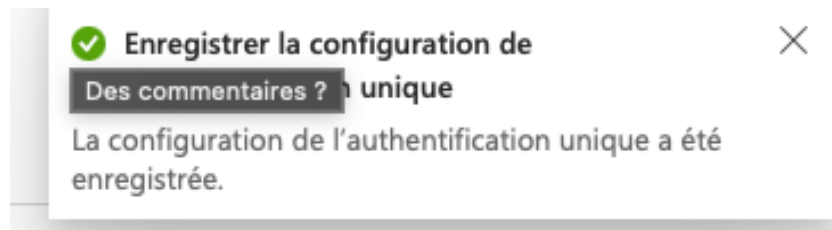
Relecture et stockage de mot de passe à l'aide d'une extension de navigateur web ou d'une application mobile.



Lié

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

- Nous avons configuré les champs suivants :
 - **URL SAML d'ACS** : <https://repair-management.starfleet.com/login>.
 - **Identifiant SAML (ID d'émetteur)** : repair-management.starfleet.com.



Configuration SAML de base

Enregistrer | Des commentaires ?

Identificateur (ID d'entité) * ⓘ

ID unique qui identifie votre application à Microsoft Entra ID. Cette valeur doit être unique dans toutes les applications de votre locataire Microsoft Entra. L'identificateur par défaut sera l'audience de la réponse SAML pour l'authentification unique initiée par IDP.

Par défaut
repair-management.starfleet.com ✓ [checkbox] ⓘ [trash]
[Ajouter un identificateur](#)

URL de réponse (URL Assertion Consumer Service) * ⓘ

L'URL de réponse correspond à l'emplacement où l'application est supposée recevoir le jeton d'authentification. Cette URL est parfois appelée « Assertion Consumer Service » (ACS) dans SAML.

Index Par défaut
https://repair-management.starfleet.com/login ✓ [checkbox] ⓘ [trash]
[Ajouter une URL de réponse](#)

- Nous avons téléchargé le certificat SAML généré par Entra ID et l'avons fourni à l'équipe en charge de l'application.

Certificat (en base64)

[Télécharger](#)

Ensuite on se connecte à l'interface d'administration ou aux paramètres de configuration de l'application personnalisée (**Gestion des Réparations** dans notre cas).

On recherche la section **Authentification unique (SSO)** ou **Configuration SAML**.

Dans la section **Configuration SAML**, on clique sur Charger le certificat

On téléverse le fichier que l'on a téléchargé.

Cela permet à l'application de vérifier les réponses SAML signées émises par Microsoft Entra ID.

Certificats de vérification



ⓘ L'exigence des certificats de vérification affecte certaines expériences d'administrateur et d'utilisateur final, telles que la fonctionnalité de

Chargez un certificat

Télécharger un certificat avec une extension de nom de fichier .cer

Gestion des Réparation.cer

OK Annuler

Autoriser les demandes signées avec RSA-
SHA1 ☐

↑ Chargez un certificat

Empreinte numérique	ID de clé	Date de début	Date d'expiration
---------------------	-----------	---------------	-------------------

Vous n'avez aucun certificat de vérification.

Enregistrer Ignorer



Certificats de vérification



Vérification de signature mise à jour

On a ensuite créé le groupe d'ingénieurs , puis si on avait eu l'accès on l'aurait ajouté



1. Attribuer des utilisateurs et des groupes

Fournir à des utilisateurs et groupes spécifiques un accès aux applications

[Attribuer des utilisateurs et des groupes](#)



Ajouter un utilisateur/groupe

On aura utilisé l'URL de connexion ACS

puis se connecter avec un utilisateur assigné pour vérifier :

- Que l'authentification redirige bien vers Microsoft Entra ID.
- Qu'une fois authentifié, on est redirigé vers l'application avec succès.

En fournissant le **certificat SAML**, on établit une **connexion sécurisée** entre Microsoft Entra ID (le fournisseur d'identité ou **IdP**) et l'application personnalisée. Cela garantit que :

1. Les réponses d'authentification sont **signées** et vérifiées.
2. Seuls les utilisateurs autorisés par Entra ID peuvent accéder à l'application.
3. L'application peut s'assurer que les requêtes proviennent bien de Microsoft Entra ID.

Le résumé des étapes donc :

1. On a téléchargé le certificat SAML depuis Microsoft Entra ID au format .cer ou .pem.
2. On a importé ce certificat dans les paramètres de l'application personnalisée.
3. On a configuré les autres paramètres SAML comme **URL ACS** et **ID d'émetteur**.
4. On a testé l'accès SSO avec un utilisateur ou un groupe assigné.

Surveillance et Réponse aux Incidents

Étape 1 : Accéder aux journaux d'audit dans Microsoft Entra ID

1. On a navigué vers **Surveillance** dans le menu de gauche.
2. On a sélectionné **Journaux d'audit** pour voir l'ensemble des activités des utilisateurs et des administrateurs.

▼ Supervision

➡ Journaux de connexion

📅 Journaux d'audit



clients

Microsoft Entra Connect

Noms de domaine 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 en bloc (préversion)

Dépannage + support

Répertoire par défaut | Journaux d'audit

Télécharger

Exporter les paramètres de données

Actualiser

Gérer la vue

Des commentaires ?

Vous souhaitez revenir à l'expérience de journaux d'audit héritée ? Cliquez ici pour quitter la préversion.

Ajouter un filtre

Afficher les dates au format : Local

Plage de dates : 24 derniers heures

Service : Tout

Catégorie : Tout

Activité : Tout

Réinitialiser les filtres

Annuaire

Sécurité personnalisée

Date ↓	Service	Catégorie	Activité	Statut	Motif du statut
15/12/2024 13:40:08	Self-service Group Mana...	GroupManagement	Group_GetDynamicGrou...	Opération réussie	OK
15/12/2024 13:38:17	B2C	PolicyManagement	Get authenticationEvent...	Opération réussie	
15/12/2024 13:38:17	B2C	Authorization	Get authenticationEvent...	Opération réussie	Access granted because th
15/12/2024 13:38:17	B2C	Authentication	Validate user authentica...	Opération réussie	Token is valid
15/12/2024 13:36:48	Core Directory	ApplicationManagement	Update service principal	Opération réussie	
15/12/2024 13:36:47	Core Directory	ApplicationManagement	Update application	Opération réussie	
15/12/2024 13:36:47	Core Directory	ApplicationManagement	Update service principal	Opération réussie	
15/12/2024 13:36:47	Core Directory	ApplicationManagement	Update service principal	Opération réussie	
15/12/2024 13:32:20	Core Directory	ApplicationManagement	Add service principal	Opération réussie	
15/12/2024 13:32:15	B2C	PolicyManagement	Get authenticationEvent...	Opération réussie	
15/12/2024 13:32:15	B2C	Authorization	Get authenticationEvent...	Opération réussie	Access granted because th
15/12/2024 13:32:15	B2C	Authentication	Validate user authentica...	Opération réussie	Token is valid
15/12/2024 13:31:01	Core Directory	ApplicationManagement	Update service principal	Opération réussie	

Les **journaux d'audit** permettent de surveiller les activités liées aux connexions, aux modifications de configuration ou aux tentatives d'accès aux ressources.

Ajouter un filtre

Afficher les dates au format

Ajouter un filtre

Filter

Statut

Valeur

Tout

Tout

Opération réussie

Échec

Date ↓	Service	Catégorie	Activité	Statut	Motif du statut
14/12/2024 20:37:59	Core Directory	ApplicationManagement	Update application	Échec	Microsoft.Online.Workflow
14/12/2024 20:37:59	Core Directory	ApplicationManagement	Update service principal	Échec	Microsoft.Online.Workflow
14/12/2024 20:37:46	Core Directory	ApplicationManagement	Update service principal	Échec	Microsoft.Online.Workflow
14/12/2024 20:37:46	Core Directory	ApplicationManagement	Update application	Échec	Microsoft.Online.Workflow
14/12/2024 20:08:13	Core Directory	ApplicationManagement	Add service principal	Échec	Microsoft.Online.Workflow
14/12/2024 20:08:12	Core Directory	ApplicationManagement	Add service principal	Échec	Microsoft.Online.Workflow

Toujours dans **Surveillance**, on a sélectionné **Journaux de connexion**. Cela permet d'obtenir des informations détaillées sur chaque tentative d'authentification.

Supervision

Journaux de connexion

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...	
15/12/2024 à 11:34:42	66b6fadd-470f-4e5a...	hanafi gaci		Azure Portal	Opération réussie	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	
14/12/2024 à 20:49:34	94d432b8-8edf-405f...	hanafi gaci		Trello	Échec	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	
14/12/2024 à 20:49:30	1c3bb70b-27a6-44d...	hanafi gaci		My Apps	Opération réussie	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	
14/12/2024 à 18:11:32	38503b5e-853a-4e2...	hanafi gaci		Azure Portal	Opération réussie	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	
14/12/2024 à 18:11:31	38503b5e-853a-4e2...	hanafi gaci		Azure Portal	Échec	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	
14/12/2024 à 16:49:44	e5a49fa8-15fb-4ad5...	hanafi gaci		Azure Portal	Opération réussie	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	
14/12/2024 à 15:51:08	d0a4e715-925a-4b3...	hanafi gaci		Azure Portal	Opération réussie	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	
14/12/2024 à 14:21:32	405bcabd-4483-499...	hanafi gaci		Azure Portal	Opération réussie	2001:861:e3d1:9870:...	Marseille, Bouches-D...	Non appliqué	

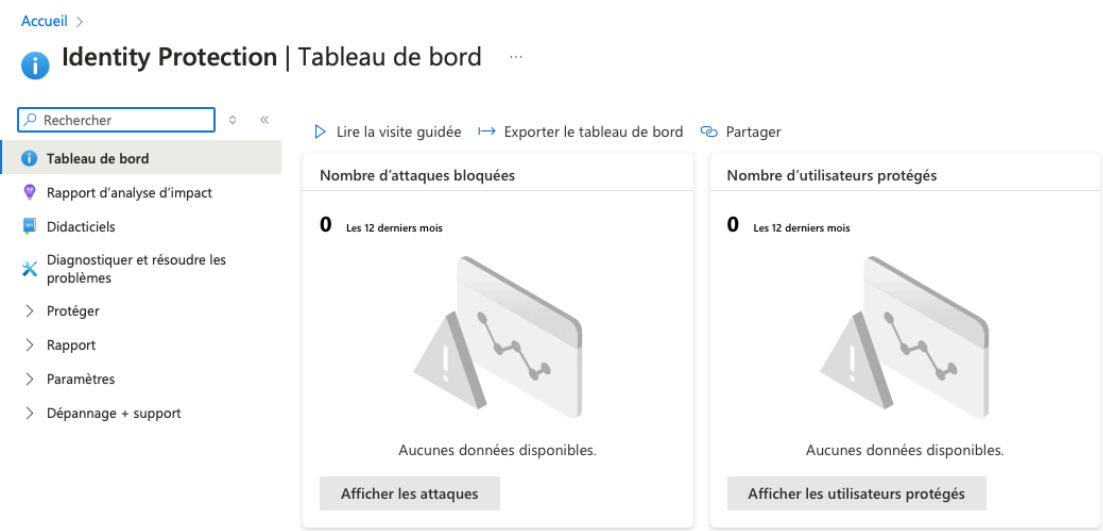
Marseille, Bouches-Du-Rhone, FR

Configurer des alertes pour les activités anormales

Étape 1 : Utiliser des alertes d'identité dans Entra ID

⚠ **Fonctionnalité premium** : Si l'on avait un abonnement **Microsoft Entra ID P2**, voici ce qu'on aurait fait :

1. Accéder à **Protection des identités** dans Entra ID.



1. Aller dans **Alertes** et configurer des alertes pour :
 - Les connexions depuis des localisations inconnues.
 - Les connexions provenant d'adresses IP suspectes.
 - Les activités inhabituelles, comme les accès en dehors des heures de travail.

Paramètres



et Définir une **notification automatique** pour recevoir des alertes par e-mail.

Sans l'abonnement premium, on a documenté la procédure pour :

- **Identifier les activités suspectes manuellement** via les journaux de connexion.
- Imaginer comment des alertes auraient été envoyées aux administrateurs pour signaler les tentatives suspectes.

Simuler des incidents de sécurité et tester les réponses

Nous avons simulé une tentative de piratage pour voir comment réagir en cas d'incident.

Étape 1 : Détecter l'incident

On a analysé les journaux d'audit et identifié une connexion suspecte depuis une adresse IP inconnue.

hanafi gaci	Azure Portal	Échec
-------------	--------------	-------

On a confirmé que cette tentative visait un compte administrateur critique.

Réinitialisation des accès :

- On a réinitialisé le mot de passe du compte compromis depuis **Utilisateurs** dans Microsoft Entra ID.
- Si l'on avait des politiques d'accès conditionnel, on aurait créé une **règle** pour bloquer les connexions depuis cette adresse IP.

dans un cas réel on aurait isolé en quarantaine , afin d'**empêcher toute communication du système avec le reste du réseau**

Voici comment on aurait procédé pour mettre en quarantaine un système compromis afin de limiter les dégâts.:

Identifier le système compromis

- **Pourquoi ?** Avant d'isoler un système, il est essentiel de l'identifier correctement pour éviter des interruptions inutiles.
- **Actions réalisées :**
 - Analyser les **journaux d'audit** et les **journaux de connexion** dans Microsoft Entra ID pour identifier l'adresse IP, l'utilisateur ou le système suspect.
 - Recueillir les informations suivantes :
 - **Nom du système**
 - **Adresse IP**
 - **Utilisateur concerné**

Exemple : On a repéré un accès suspect provenant de l'IP 203.0.113.45 et lié au serveur **Gestion des Réparations**.

Déconnecter le système du réseau

Pour isoler un système compromis, il faut **le déconnecter du réseau interne** pour stopper la propagation d'une menace (ex. : virus, attaques, exfiltration de données)

Utiliser la commande suivante pour désactiver le réseau : `sudo ifconfig eth0 down`

ou **Débrancher physiquement le câble réseau** si le serveur est accessible.

Si le compromis concerne un compte utilisateur, on aurait également isolé ce compte pour éviter de nouvelles connexions suspectes.

Étapes dans Microsoft Entra ID :

1. Aller dans **Utilisateurs** dans le portail Microsoft Entra ID.
2. Sélectionner le compte compromis.
3. Réinitialiser le mot de passe pour empêcher l'accès non autorisé.
4. **Désactiver temporairement le compte :**
 - Cliquer sur **Bloquer l'utilisateur** dans les options.

cette mise en quarantaine est cruciale car Isoler le système compromis empêche l'attaquant de : Propager une menace à d'autres systèmes, Accéder à des données sensibles, Exfiltrer ou modifier des informations critiques.