

Azure

- Redimensionner disque sur VM Azure
- App Password (ADOC)
- Utilisateur Invité
- Powershell Azure : check IP disponible
- Renouvellement Certificat et Jeton Apple sur MDM
- MFA - Désactivation application Authenticator
- Accès Partenaires SSO

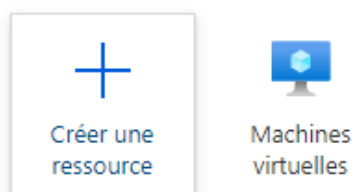
Redimensionner disque sur VM Azure

Procédure :

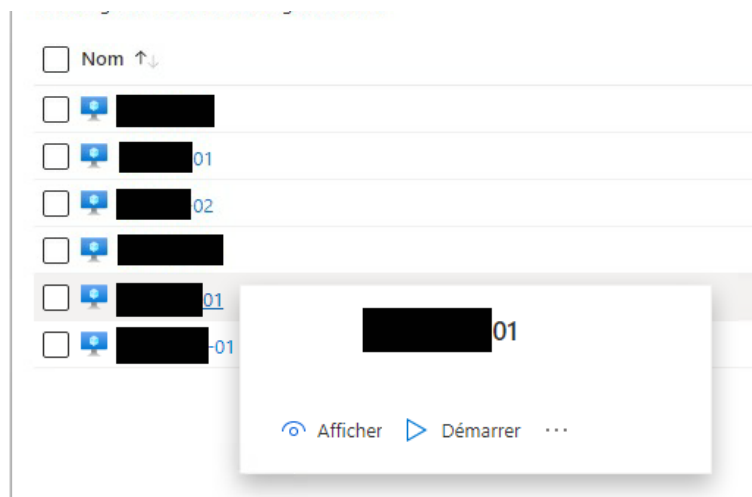
Se connecter au portail Azure du Tenant cible : <https://portal.azure.com/#home>
Avec un compte ayant les privilèges administrateur

Se rendre sur le service Machines virtuelles :

Services Azure



Ouvrir la VM souhaitée :



Une fois sur la fiche serveur > allez dans la section "Disks" puis appuyer sur la croix encadrée en rouge afin de désallouer le disque de la VM.

Virtual machine 01 | Disks

Save Discard Refresh Additional settings Feedback Troubleshoot

OS disk

Swap OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption	Host caching
[Redacted]	Premium SSD LRS	129	1100	125	SSE with PMK	None

Data disks

Filter by name

Showing 1 of 1 attached data disks

Create and attach a new disk Attach existing disks

LUN	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption	Host caching
0	[Redacted]	Premium SSD LRS	5550	16000	500	SSE with PMK	None

Une fois que l'on est certain d'avoir les accès pour démarrer la VM, procéder à son arrêt.

Machine virtuelle 01

Rechercher (Ctrl+/)

Connecter Démarrer Redémarrer Arrêter Capturer Supprimer Actua

Adviser (1 sur 1) : Activer la réplication des machines virtuelles pour protéger vos applications contre une panne

Bases

Groupe de res... (Déplacer) : [Redacted]

Statut : En cours d'exécution

Emplacement : France-Centre

Abonnement (Déplacer) : Paiement à l'utilisation

ID d'abonnement : [Redacted]

Étiquettes (Modifier) : Cliquez ici pour ajouter des étiquettes

Propriétés Supervision Fonctionnalités (7) Recommandations (1) Tutoriels

Machine virtuelle

Nom de l'ordinateur	[Redacted]
État d'intégrité	-
Système d'exploitation	Windows (Windows Server 2012 R2 Datacenter)
Éditeur	MicrosoftWindowsServer
Offre	WindowsServer
Plan	2012-R2-Datacenter
Génération de machine virtuelle	V1
État de l'agent	Ready
Version de l'agent	2.7.41491.1032
Groupe hôte	Aucun
Hôte	-
Groupe de placement de proximité	-
État de colocation	N/A
Groupe de réservations de capacité	-

Dans le menu Disques, ouvrir le disque à modifier :

Machine virtuelle 01 | Disques ...

Rechercher (Ctrl+/) << Enregistrer Ignorer Actualiser Paramètres supplémentaires Commentaires Dépanner

Vue d'ensemble
Journal d'activité
Contrôle d'accès (IAM)
Étiquettes
Diagnostiquer et résoudre les problèmes

Paramètres

Mise en réseau
Connexion
Disques
Taille
Sécurité
Recommandations Advisor
Applications + Extensions
Livraison continue
Disponibilité + mise à l'échelle
Configuration
Identité
Propriétés
Verrous

Opérations

Bastion

Disque OS

Échanger le disque OS

Nom du disque	Type de stockage	Taille (Gio)
[REDACTED]	SSD Premium LRS	129

Disques de données

Filtrer par nom

Affichage de 1 disques de données attachés sur 1

+ Créer un disque et l'attacher Attacher des disques existants

Numéro d'unité	Nom du disque	Type de stockage	Taille (Gio)
0	[REDACTED]	SSD Premium LRS	5000

Plan	2012-R2-Datacenter
Génération de machine virtuelle	V1
État de l'agent	Ready
Version de l'agent	2.7.41491.1032
Groupe hôte	Aucun
Hôte	-
Groupe de placement de proximité	-
État de colocation	N/A
Groupe de réservations de capacité	-

Dans Taille + performance, renseigner la taille du disque en Go
Entrez la taille du disque à créer. Vous êtes facturé le même prix, quel que soit l'espace disque utilisé sur le disque provisionné. Par exemple, si un disque de 200 Gio est provisionné sur un disque de 256 Gio, vous êtes facturé pour le disque de 256 Gio.

Au préalable il est recommandé de vérifier dans quelle catégorie de taille se trouvera le disque après modifications, un changement de catégorie ou performance entraine une facturation différente pour le client.

Disque

Rechercher (Ctrl+/) <<

- Vue d'ensemble
- Journal d'activité
- Contrôle d'accès (IAM)
- Étiquettes
- Paramètres
 - Configuration
 - Taille + performances**
 - Chiffrement
- Réseau
- Exportation de disque
- Propriétés
- Verrous
- Supervision
 - Métriques
- Automatisation
 - Tâches (préversion)
 - Exporter le modèle
- Aide
 - Nouvelle demande de support

Les modifications apportées à la taille du disque peuvent être apportées uniquement

Référence SKU de disque ⓘ

SSD Premium (stockage localement redondant) ▾

Taille	Niveau de disque
4 GiB	P1
8 GiB	P2
16 GiB	P3
32 GiB	P4
64 GiB	P6
128 GiB	P10
256 GiB	P15
512 GiB	P20
1024 GiB	P30
2048 GiB	P40
4096 GiB	P50
8192 GiB	P60
16384 GiB	P70
32767 GiB	P80

Taille de disque personnalisée (Gio) * ⓘ

Niveau de performance ⓘ

P60 - 16000 IOPS, 500 Mbits/s (par défaut) ▾

Cliquer ensuite sur le bouton redimensionner.

Taille de disque personnalisée (Gio) * ⓘ

Niveau de performance ⓘ


P60 - 16000 IOPS, 500 Mbits/s (par défaut) ▾

Redimensionner Abandonner



Notifications

[Plus d'événements dans le journal d'activité →](#)

 **Disque mis à jour**

Disque « XXXXXXXXXX » mis à jour.

 **Arrêt réussi de la machine virtuelle**

Arrêt réussi de la machine virtuelle XXXXXXXXXX.

Attendre la fin du traitement dans les notifications

Vérifier que le disque est de nouveau alloué au serveur sinon le faire puis redémarrer la VM.

Vérifier ensuite que la taille du disque a bien été modifier dans le gestionnaire des disques, et augmenter la taille de la partition.

App Password (ADOC)

Il faut activer la MFA pour le compte souhaité en allant sur la fiche utilisateur

Dans le Centre d'Administration MS 365 > Utilisateurs Actifs

Cliquer sur l'utilisateur puis Gérer l'authentification multifacteur

Utilisateurs actifs

Ajouter un utilisateur | Authentification multifacteur

Nom complet ↑ | Nom d'utilisate...

[redacted] - Comptabilite Fournisse... | etudiant.com

LC [redacted] - **Comptabilite Fo...**

Réinitialiser le mot de passe | Bloquer la connexion

sessions

Adresse email de secours
Aucune fournie
[Ajouter une adresse](#)

Groupes
[Gérer les groupes](#)

Rôles
Aucun accès administrateur
[Gérer les rôles](#)

Informations de contact

Nom d'affichage: [redacted] Comptabilite Fournisseurs | Prénom: [redacted]

Numéro de téléphone: [Gérer les informations de contact](#) | Nom: Comptabilite Fournisseurs

Activations d'Office [Afficher les activations d'Office](#) | **Authentification multifacteur** [Gérer l'authentification multifacteur](#)

Activer sur l'utilisateur

authentification multifacteur

utilisateurs | paramètres du service

À compter du 30 septembre 2022 Les expériences d'inscription combinées pour MFA et SSPR seront activées pour tous les locataires. L'activer maintenant. Avant de commencer, consultez le guide de déploiement de l'authentification multifacteur.

mettre à jour en bloc

Affichage: Connecter les utilisateurs autorisé | Search | État Multi-Factor Authentication: Tous

<input type="checkbox"/>	NOM COMPLET	NOM D'UTILISATEUR	ÉTAT MULTI-FACTOR AUTHENTICATION
<input type="checkbox"/>	[redacted]	[redacted]	Désactivé
<input checked="" type="checkbox"/>	[redacted]	[redacted]	Désactivé
<input type="checkbox"/>	[redacted]	[redacted]	Désactivé
<input type="checkbox"/>	[redacted]	[redacted]	Désactivé
<input type="checkbox"/>	[redacted]	[redacted]	Désactivé
<input type="checkbox"/>	[redacted]	[redacted]	Désactivé

quick steps
[Activer](#)
Gérer les paramètres utilisateur

Appliquer sur l'utilisateur

authentification multifacteur

utilisateurs paramètres du service

À compter du 30 septembre 2022 Les expériences d'inscription combinées pour MFA et SSPR seront activées pour tous les locataires. L'activer maintenant. Avant de commencer, consultez le guide de déploiement de l'authentification multifacteur.

mettre à jour en bloc

Affichage: Connecter les utilisateurs autorisé Search État Multi-Factor Authentication: Tous

<input type="checkbox"/>	NOM COMPLET	NOM D'UTILISATEUR	ÉTAT MULTI-FACTOR AUTHENTICATION
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input checked="" type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Appliquée
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Désactivé
<input checked="" type="checkbox"/>	[REDACTED]	[REDACTED]	Activé

[REDACTED]

[REDACTED]

quick steps

Désactiver

Appliquer

Gérer les paramètres utilisateur

Se connecter au Webmail

Des infos supplémentaires sont demandé dès la première connexion

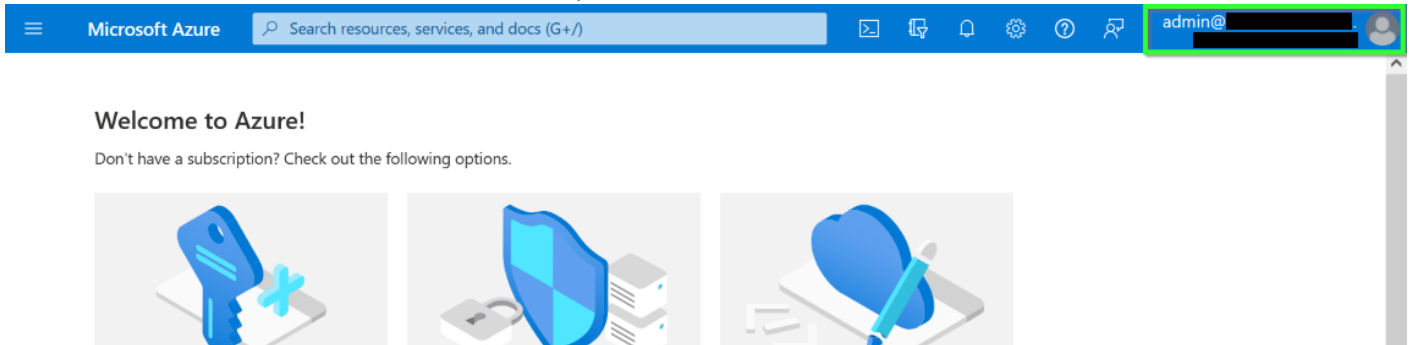
Entrer votre numéro de tél pour la MFA

Entré le code d'authentification reçu par SMS

Copier le App Password dans le KeePass

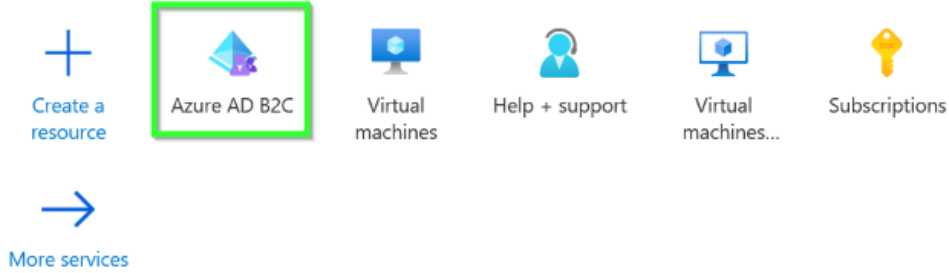
Utilisateur Invité

Se connecter au Tenant et bien vérifier que c'est bien le bon



Aller dans Azure B2C

Azure services



Puis User

Home >

Azure AD B2C

Search

Overview

Manage

- App registrations
- Applications (Legacy)
- Identity providers
- API connectors
- Company branding
- User attributes
- Users**
- Roles and administrators

Cliquer sur New Guest User

Home > Azure AD B2C | Users >

Users

Search

+ New user + **New guest user** Bulk operations Refresh Reset password

All users (preview)

- Audit logs
- Sign-in logs
- Diagnose and solve problems

Manage

- Deleted users (preview)
- Password reset

Search users Add filters

	Name	User name	User type
<input type="checkbox"/>	00000 - VILDRAN Alex	alexandra@vilgrain.fr	Member
<input type="checkbox"/>	00000 - JIMOU Spiney	spiney.alex75@hotmail.com	Member
<input type="checkbox"/>	00100 - AGIER Jean	jean.agier@gmail.com	Member
<input type="checkbox"/>	00150 - AGNEW Joseph	jagnew@yahoo.co.uk	Member
<input type="checkbox"/>	00040 - JALLZ Marc	marc.jalles@sunrise.ch	Member

Remplir les champs encadrés

Select template

- Create user**
Create a new user in your organization.
 - Invite user**
Invite a new guest user to collaborate with your organization.
 - Create Azure AD B2C user**
Create a new user in your organization. This user has a unique username.
- [Help me decide](#)

Dans Groups and Roles,

Bien sélectionner un groupe si besoin et/ou un Role si besoin

Dans cet exemple, l'utilisateur est un prestataire qui nous a confirmé qu'il a besoin de gérer les applications donc il est Application Admin.

Si on vous demande Global Admin, faire confirmer les besoins réels et validé par le DSI (ou équivalent) en lui expliquant les impacts

Groups and roles

Groups **0 groups selected**

Roles **Application administrator**

Le reste des champs est optionnel

Block sign in bloquera la connexion au tenant.

Les autres infos, si vous les avez renseignez les.

Settings

Block sign in

Yes No

Usage location

Job info

Job title

Department

Company name

Manager

No manager selected

Powershell Azure : check IP disponible

Au besoin, pour savoir si une ip est disponible sur Azure :

```
Connect-AzAccount
```

Puis

```
Get-AzVirtualNetwork -Name NOMduVNET -ResourceGroupName RESSOURCEGROUP | Test-AzPrivateIPAddressAvailability -IPAddress IPàTESTER
```

```
PS C:\Windows\system32> Get-AzVirtualNetwork -Name " " -ResourceGroupName " " | Test-AzPrivateIPAddressAvailability -IPAddress .136.65
Available : False
AvailableIPAddresses : [
  "136.69",
  "136.71",
  "136.72",
  "136.73",
  "136.74"
]
```

Renouvellement Certificat et Jeton Apple sur MDM

Certificat à renouveler tous les ans

1. Se connecter à <https://endpoint.microsoft.com/>
2. Allez dans "Appareils" > "Inscrire Appareils"
3. Allez dans "Inscription Apple" > "Certificat Push MDM Apple"

Suivez les étapes de configuration du certificat


Vous avez besoin d'un certificat Push MDM Apple pour gérer des appareils Apple avec Intune.

Étapes :

1. J'autorise Microsoft à envoyer des informations sur l'utilisateur et sur l'appareil à Apple. [Plus d'informations sur l'autorisation Microsoft.](#)

J'accepte.

2. Téléchargez la demande de signature de certificat Intune qui est nécessaire pour créer un certificat Push MDM Apple. [Télécharger votre CSR](#)

3. Créez un certificat Push MDM Apple. [Plus d'informations sur le certificat Push MDM Apple.](#)
[Créer votre certificat Push MDM](#) 

4. Entrez l'ID Apple utilisé pour créer votre certificat Push MDM Apple.

ID Apple *

5. Accédez au certificat Push MDM Apple à charger

Certificat Push MDM Apple *

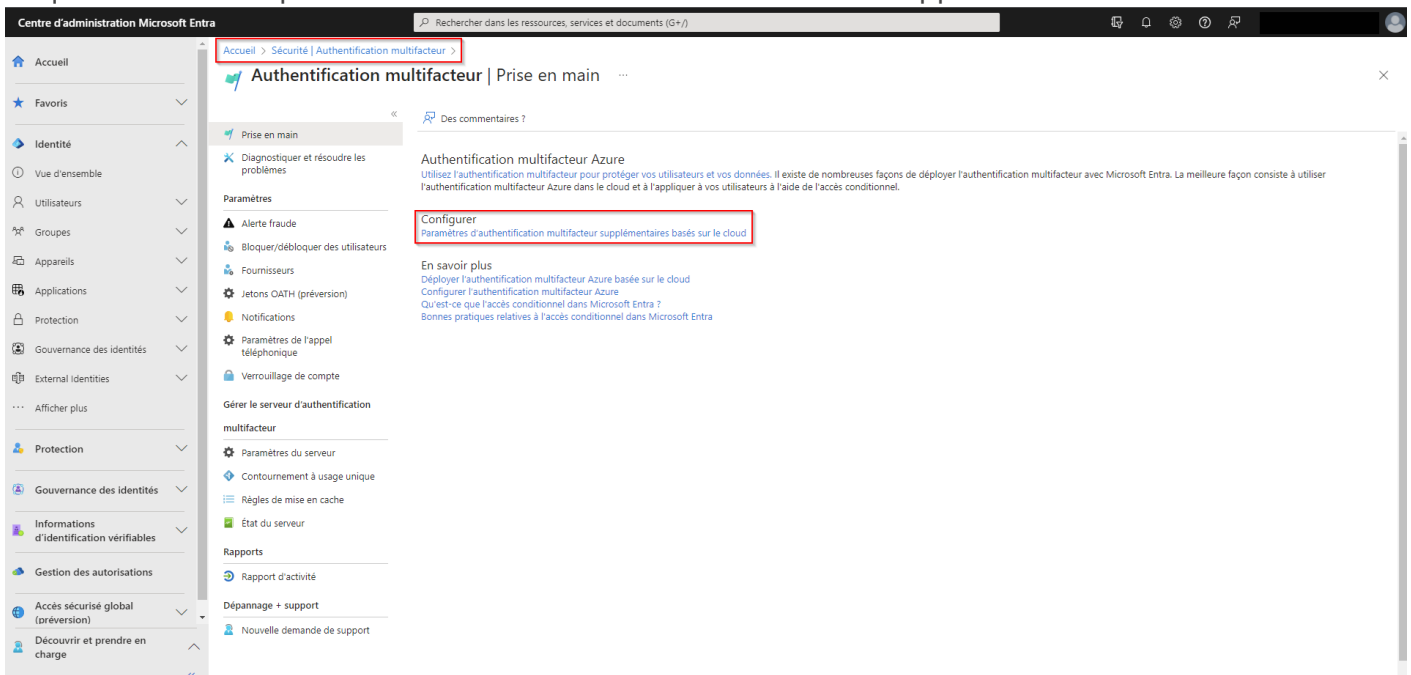


MFA - Désactivation application Authenticator

Microsoft force actuellement les utilisateurs à enregistrer l'application Authenticator comme méthode d'authentification via des campagnes.

Voici les étapes à suivre pour désactiver (temporairement) cette méthode :

Se connecter sur Azure et accéder à la page Accueil > Sécurité | Authentification multifacteur.
Cliquer ensuite sur paramètres d'authentification multifacteur supplémentaires basés sur le cloud.



Sur la page qui s'ouvre, décocher la "Notification via l'application mobile" et valider en enregistrant :

authentification multifacteur

utilisateurs paramètres du service

mots de passe d'application [\(en savoir plus\)](#)

- Autoriser les utilisateurs à créer des mots de passe d'application pour se connecter à des applications sans navigateur
- Ne pas autoriser les utilisateurs à créer des mots de passe d'application pour se connecter à des applications sans navigateur

adresses ip de confiance [\(en savoir plus\)](#)

- Ignorer l'authentification multifacteur pour les demandes issues d'utilisateurs fédérés provenant de mon intranet
- Ignorer l'authentification multifacteur pour les demandes provenant d'une plage spécifique d'adresses IP

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

Input trusted IP list

options de vérification [\(en savoir plus\)](#)

Méthodes disponibles pour les utilisateurs :

- Appel téléphonique
- SMS par téléphone
- Notification via application mobile
- Code de vérification à partir de l'application mobile ou du jeton matériel

mémoriser multi-factor authentication sur un appareil approuvé [\(en savoir plus\)](#)

- Permettre aux utilisateurs de mémoriser l'authentification multifacteur sur les appareils auxquels ils font confiance (de 1 à 365 jours)

Nombre de jours pendant lesquels les utilisateurs peuvent faire confiance aux appareils

REMARQUE : pour une expérience utilisateur optimale, nous vous recommandons d'utiliser la fréquence de connexion Accès conditionnel pour étendre les durées de vie des sessions sur les appareils, les emplacements de confiance ou les sessions à faible risque en tant qu'alternative à l'utilisation des paramètres 'Mémoriser MFA sur un appareil de confiance'. Si vous utilisez 'Mémoriser MFA sur un appareil de confiance', assurez-vous d'étendre la durée à 90 jours ou plus. [En savoir plus sur les invites de réauthentification.](#)

enregistrer

Ensuite, se rendre sur la page "Accueil > Méthodes d'authentification" puis cliquer sur "Campagne d'inscription" et modifier.

Changer l'état sur "Désactivée" puis valider.

- Accueil
- Favoris
- Identité
 - Vue d'ensemble
 - Utilisateurs
 - Groupes
 - Appareils
 - Applications
 - Rôles et administrateurs
 - Facturation
 - Paramètres
 - Protection
 - Gouvernance des identités
 - External Identities
 - Expériences utilisateur
 - Gestion hybride
 - Surveillance et intégrité
 - Afficher moins

Méthodes d'authentification

Méthodes d'authentification | Campagne d'inscription

Rechercher

Des commentaires ?

Gérer

Stratégies

Protection par mot de passe

Campagne d'inscription

Points forts d'authentification

Paramètres

Supervision

Activité

Détails de l'inscription de l'utilisateur

Événements d'inscription et de réinitialisation

Résultats de l'opération en bloc

Paramètres [Modifier](#) [Ignorer](#)

État	Désactivée
Nombre de jours autorisés pour la répétition	1 jour
Nombre limité de répétitions	Activé
Utilisateurs et groupes exclus	Aucun élément sélectionné
+ Ajouter des utilisateurs et des groupes	

Méthode d'authentification

Méthode	Utilisateurs et groupes inclus
Microsoft Authenticator	Tous les utilisateurs

Accès Partenaires SSO

1. Contexte du Projet

Objectif : Permettre aux collaborateurs de sociétés partenaires d'accéder à un CMS via Single Sign-On (SSO).

Méthode : Azure B2B Collaboration via la Gestion des droits d'accès (Entitlement Management).

Domaines concernés :

- Région 1 : @partenaireA.com, @partenaireB.com

- Région 2 : @partenaireC.com, @partenaireB.com

2. Prérequis Azure (Microsoft Entra ID)

Avant la mise en service, les paramètres de collaboration externe ont été vérifiés dans le locataire cible :

- Inscription en libre-service : Activée.

- Restrictions d'accès : Accès limité aux propriétés et appartenances de leurs propres objets.

- Restrictions de collaboration : Invitations limitées aux domaines autorisés.

3. Configuration des Organisations Connectées

Pour établir la confiance avec les domaines externes, les organisations suivantes ont été créées dans Identity Governance :

- Partenaire A : domaine partenaireA.com

- Partenaire B : domaine partenaireB.com

- Partenaire C : domaine partenaireC.com

Ces organisations permettent à Microsoft Entra ID de reconnaître les annuaires sources des utilisateurs.

4. Création du Paquet d'Accès (Access Package)

Nom : Accès CMS Partenaires

Ressources incluses : Application Enterprise du CMS ou groupe de sécurité dédié.

Rôles assignés : Utilisateur / Membre.

Politique de demande :

- Type : Pour les utilisateurs externes non présents dans l'annuaire.
- Filtrage : Organisations connectées autorisées.
- Approbation : Requise par un sponsor interne.

5. Cycle de Vie et Sécurité

Révisions d'accès : Recommandées tous les 6 mois.

Expiration : Configurée automatiquement pour éviter les comptes inactifs.

Sécurité : Garantit la conformité et la protection des ressources de l'organisation.

Guide Utilisateur

1. Objectif

Ce guide explique comment les partenaires accèdent au CMS via le Single Sign-On (SSO).

2. Prérequis

Les utilisateurs doivent disposer :

- D'une adresse e-mail professionnelle appartenant à un domaine autorisé.
- D'un accès à l'URL du portail MyAccess fournie par l'organisation.
- D'une connexion Internet et d'un navigateur web moderne.

[Emplacement pour capture d'écran du portail Microsoft Entra ID]

3. Processus de Demande d'Accès

Étape 1 : Accéder au portail MyAccess via le lien fourni.

Étape 2 : Se connecter avec son adresse e-mail professionnelle.

Étape 3 : Sélectionner le paquet d'accès 'Accès CMS Partenaires'.

Étape 4 : Soumettre la demande pour approbation.

4. Connexion au CMS

Étape 1 : Accéder à la page de connexion du CMS.

Étape 2 : Cliquer sur 'Se connecter avec Microsoft'.

Étape 3 : S'authentifier avec son compte professionnel.

Étape 4 : Accéder au CMS sans avoir à saisir un nouveau mot de passe.