

PROCÉDURE

Création d'utilisateurs — Azure Active Directory

Microsoft Entra ID | Portail Azure

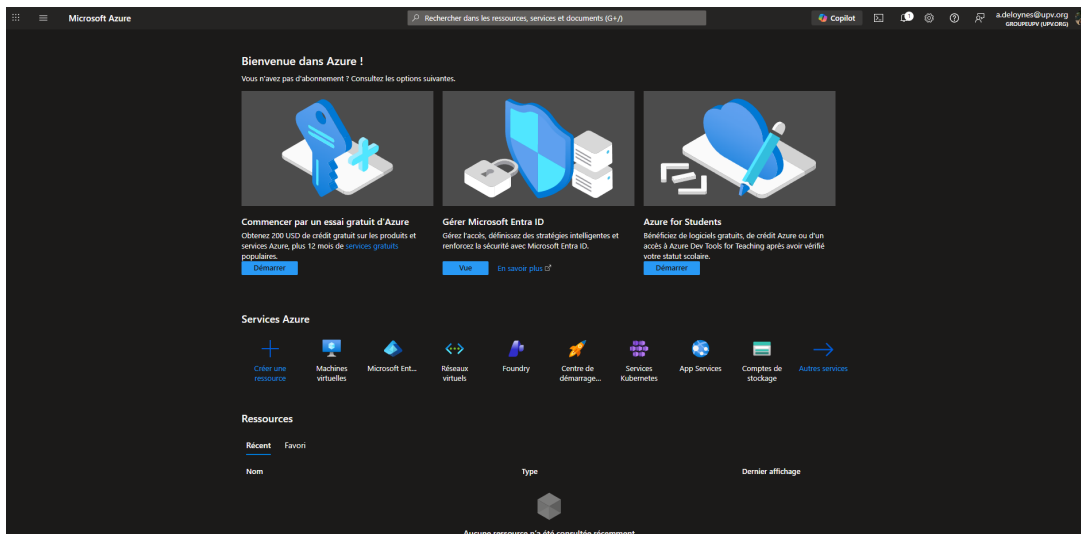
Service : Azure AD / Microsoft Entra ID | Rôle : Administrateur | Activité : Gestion des comptes
utilisateurs cloud

i Azure Active Directory (aujourd'hui renommé Microsoft Entra ID) est le service d'annuaire cloud de Microsoft. Il centralise la gestion des identités et des accès pour les applications Microsoft 365, Azure et les services tiers. Cette procédure couvre la création manuelle d'un compte utilisateur depuis le portail Azure, de l'authentification jusqu'à la communication des accès à l'utilisateur.

PARTIE 1 — Connexion au portail Azure et navigation

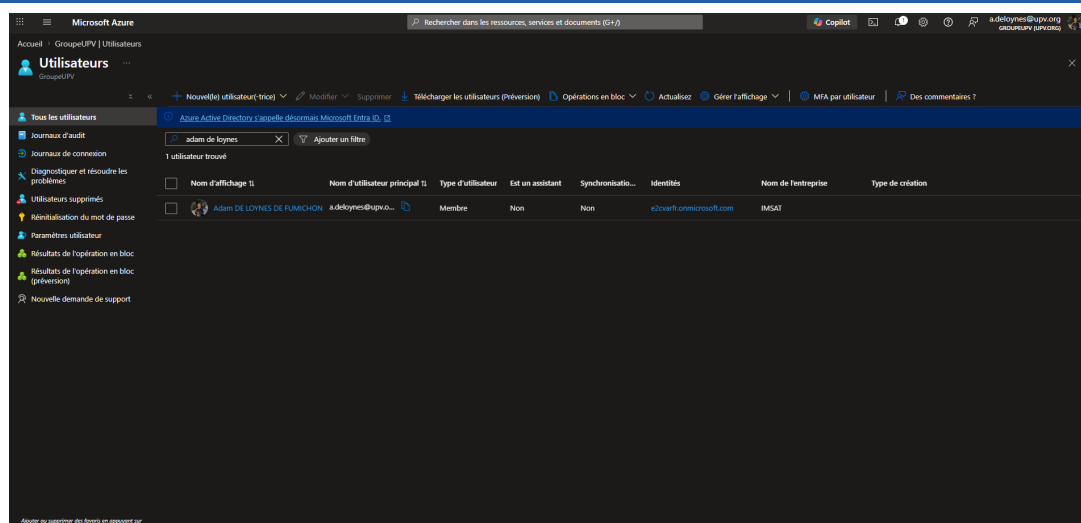
i La création d'utilisateurs nécessite un compte disposant d'un rôle suffisant dans Azure AD : au minimum Administrateur d'utilisateurs (User Administrator) ou Administrateur général (Global Administrator).

Étape 1 — Connexion au portail Azure et accès à Microsoft Entra ID



► Se connecter sur portal.azure.com avec le compte administrateur du tenant. Sur le tableau de bord Azure, rechercher « Microsoft Entra ID » (anciennement Azure Active Directory) dans la barre de recherche en haut ou le sélectionner dans la liste des services favoris. La page d'accueil Entra ID affiche une vue synthétique du tenant : nombre d'utilisateurs, de groupes, d'applications enregistrées et l'état de la licence.

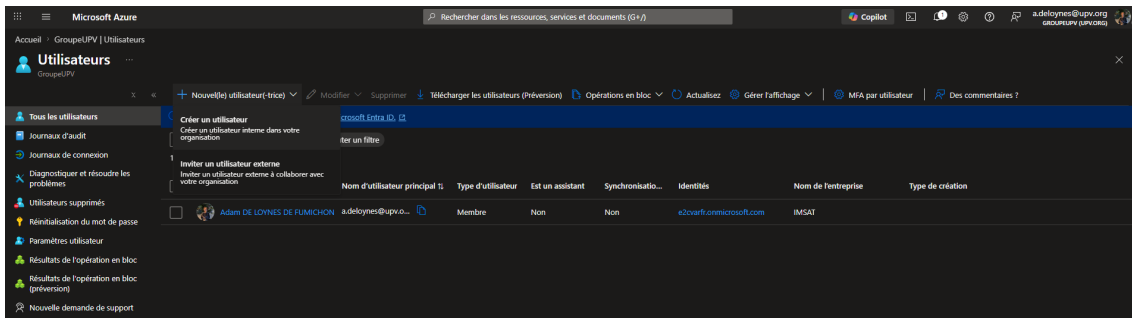
Étape 2 — Accès à la liste des utilisateurs



► Dans le menu latéral gauche de Microsoft Entra ID, cliquer sur « Utilisateurs » pour afficher la liste complète des comptes du tenant. La vue liste montre le nom d'affichage, le nom d'utilisateur (UPN), le type de compte (Membre / Invité) et le statut de synchronisation (cloud uniquement ou hybride via Azure AD Connect).

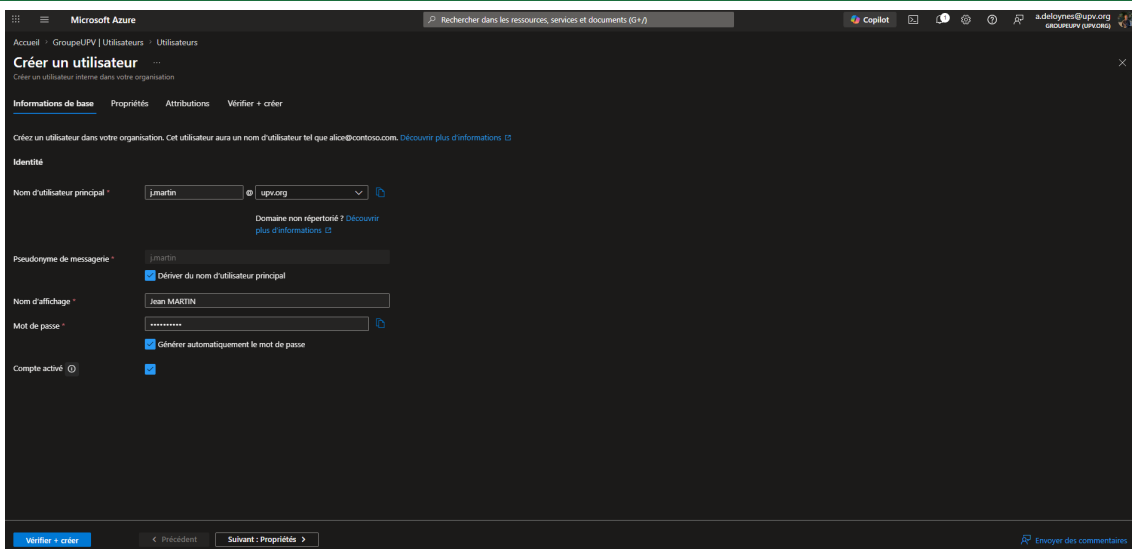
PARTIE 2 — Création du compte utilisateur

Étape 3 — Lancer la création d'un nouvel utilisateur



► Depuis la liste des utilisateurs, cliquer sur « + Nouvel utilisateur » puis sélectionner « Créer un utilisateur ». L'option « Inviter un utilisateur externe » est réservée aux comptes B2B (partenaires, prestataires). La fenêtre de création s'ouvre sur l'onglet Informations de base.

Étape 4 — Renseigner les informations de base



► Compléter les champs obligatoires de l'onglet Informations de base :

- Nom d'utilisateur : partie de l'adresse UPN avant @[nomdudomaine].onmicrosoft.com (ex. prenom.nom)
- Nom d'affichage : prénom et nom complet de l'utilisateur
- Mot de passe : laisser Azure générer un mot de passe initial ou en définir un manuellement

Le mot de passe généré est temporaire — l'utilisateur sera invité à le modifier dès la première connexion.

Étape 5 — Configurer les propriétés supplémentaires

The screenshot shows the 'Créer un utilisateur' page in the Microsoft Azure portal. The 'Propriétés' tab is selected. The form is divided into several sections:

- Informations de base:** Prénom (Jean), Nom (MARTIN), Type d'utilisateur (Membre).
- Informations sur l'autorisation:** Modifier ID des utilisateurs du certificat.
- Informations de travail:** Poste (Comptable), Nom de l'entreprise (UPV), Département (Service Comptabilité), ID d'employé, Type d'employé, Date d'embauche de l'employé, Lieu du bureau, Gestionnaire (Ajouter un responsable).
- Informations de contact:** Adresse postale, Ville, Département ou région, Code postal.

Buttons at the bottom include 'Vérifier > créer', '< Précédent', and 'Suivant > Attributions'.

► Passer à l'onglet **Propriétés** pour renseigner les métadonnées du profil :

- Prénom et Nom
- Poste (titre du rôle)
- Nom de l'entreprise
- Département
- Numéro de téléphone (optionnel)
- Pays / Région

Étape 6 — Valider la création et vérifier le compte

The screenshot shows the 'Créer un utilisateur' page in the Microsoft Azure portal. The 'Vérifier > créer' tab is selected. The page displays a summary of the user's information:

- Informations de base:** Nom d'utilisateur principal (j.martin@upv.org), Nom d'affichage (Jean MARTIN), Pseudonyme de messagerie (j.martin), Mot de passe (*****), Compte activé (Oui).
- Propriétés:** Prénom (Jean), Nom (MARTIN), Type d'utilisateur (Membre), Poste (Comptable), Nom de l'entreprise (UPV), Département (Service Comptabilité).
- Attributions:** Unités administratives, Groupes, Rôles.

A 'Créer' button is visible at the bottom left, along with navigation buttons '< Précédent' and 'Suivant >'.

► Une fois tous les champs renseignés, cliquer sur « **Créer** » pour finaliser la création du compte. Le compte apparaît immédiatement dans la liste des utilisateurs. Vérifier que le statut est « **Actif** » et que le type de compte est bien « **Membre** ». En cas d'anomalie (compte désactivé, UPN incorrect), ouvrir la fiche utilisateur pour corriger les informations.

PARTIE 3 — Communication des accès à l'utilisateur

❗ Le mot de passe temporaire ne doit jamais être transmis par e-mail non chiffré. Privilégier la communication en face-à-face, par téléphone ou via un canal sécurisé (messagerie chiffrée, vault de mots de passe).

Communiquer à l'utilisateur les éléments suivants :

- Son identifiant complet (adresse UPN — ex. prenom.nom@domaine.onmicrosoft.com)
- Son mot de passe temporaire généré par Azure
- L'URL de connexion : <https://portal.office.com> ou <https://myaccount.microsoft.com>
- La procédure de changement de mot de passe lors de la première connexion
- Les applications auxquelles il a accès (Microsoft 365, etc.)

CONCLUSION

Cette activité m'a permis de comprendre et de maîtriser la gestion des utilisateurs dans un annuaire cloud comme Azure Active Directory (Microsoft Entra ID). J'ai appris à créer des comptes manuellement, à paramétrer les informations de profil et à gérer les accès selon les besoins de l'organisation. La maîtrise de ces opérations est fondamentale dans un environnement hybride ou full-cloud, où la gestion des identités constitue le premier niveau de sécurité du système d'information.

Compétences BTS SIO SISR validées :

- ✓ Mettre à disposition des utilisateurs un service informatique
- ✓ Gérer le patrimoine informatique