

# RÉINITIALISATION DES MOT DE PASSE.

Noah MAILLET  
Projet LAB-CAP





# Table of contents

|                                                                                           |   |
|-------------------------------------------------------------------------------------------|---|
| Préface.....                                                                              | 3 |
| 1 Connexion au tenant Office 365.....                                                     | 4 |
| 2 “Planifier votre déploiement de réinitialisations du mot de passe libre-service ». .... | 5 |



# Préface.

La réinitialisation du mot de passe libre-service est une fonctionnalité clé d'Office 365 qui permet aux utilisateurs de réinitialiser eux-mêmes leurs mots de passe en cas d'oubli ou de perte. Cette fonctionnalité réduit la charge de travail des administrateurs informatiques et améliore l'expérience utilisateur en permettant une récupération rapide et efficace des mots de passe.

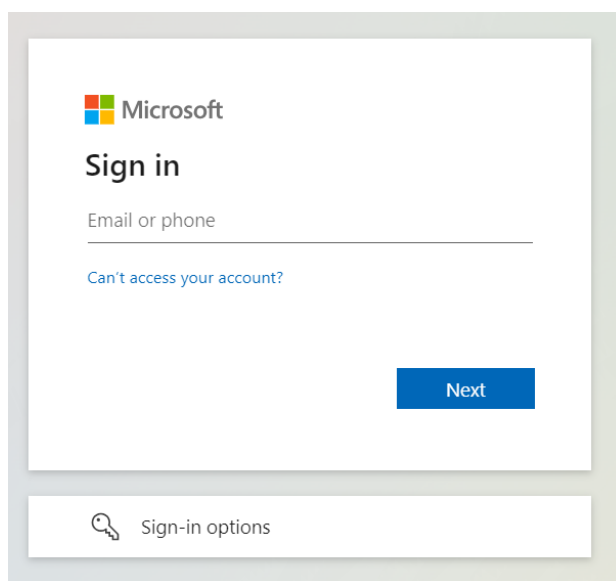
La mise en place d'un tel service doit être soigneusement planifiée pour garantir sa sécurité et son efficacité. Cela implique d'identifier les groupes d'utilisateurs éligibles, de définir les paramètres de sécurité, et d'établir des procédures claires pour la réinitialisation des mots de passe. L'objectif est de fournir un service sécurisé et convivial qui améliore l'expérience utilisateur tout en réduisant la charge de travail des administrateurs.

Dans cette section, nous allons examiner les étapes nécessaires pour planifier et déployer la réinitialisation du mot de passe libre-service dans votre environnement Office 365. Nous aborderons les aspects techniques, organisationnels et de formation pour garantir un déploiement réussi.

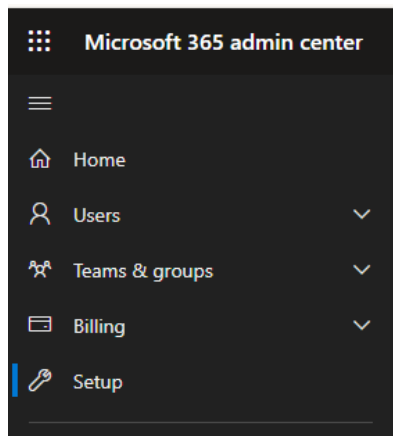


# 1 Connexion au tenant Office 365.

1. Je vais sur mon navigateur habituel.
2. Je me rends sur le portail d'administration (<https://admin.microsoft.com/adminportal/Home#/homepage>):



3. Je me connecte avec les identifiants administrateur du tenant.
4. Je me rends sur « Setup » :



Ce volet de configuration affiche toutes les actions à effectuer pour augmenter la sécurité du tenant.

| Sign-in and security                       |                   |                                                                                                                                                                         |
|--------------------------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name ↑                                     | Status            | Description                                                                                                                                                             |
| Add or sync users to Microsoft Entra ID    |                   | Your journey to the cloud starts with your users and getting their accounts into Microsoft 365.                                                                         |
| Configure multifactor authentication (MFA) | ○ Not started yet | Provide an additional level of security for sign-ins using multifactor authentication (MFA) to access company resources.                                                |
| Get your custom domain set up              | ● Completed       | Connecting a domain will allow users in your organization to send and receive email from a custom domain name.                                                          |
| Help prevent insider risks                 |                   | Set up Microsoft Purview Insider Risk Management to detect risky activity across your org so you can identify, investigate, and take action on potential insider risks. |
| Let users reset their own passwords        | ● Completed       | Reduce your support costs by allowing users to register for self-service password reset.                                                                                |
| Limit admins to the access they need       | ○ Not started yet | Limit risk to your organization by reassigning some global admins to more limited admin roles, removing access to critical features that they don't need.               |
| Set passwords to never expire              | ● Completed       | Setting passwords to never expire is more secure and leads to fewer work stoppages.                                                                                     |



## 2 «Planifier votre déploiement de réinitialisations du mot de passe libre-service ».

Dans notre contexte nous n'avons pas d'Active Directory locale de synchronisée.

1. Je sélectionne « Non ».
2. Je sélectionne « Notification et personnalisations de l'administrateur » ➔ « Suivant ».

3. « Choisir la façon dont les utilisateurs s'authentifient » ➔ « Configurer l'authentification » ➔ « Suivant ».

| <b>Manage migration</b> <small>On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all aut migration from the legacy policies to the new unified policy. <a href="#">Learn more</a></small> |           |         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|---------|
| <a href="#">Manage migration</a>                                                                                                                                                                                                                                                     |           |         |
| Method                                                                                                                                                                                                                                                                               | Target    | Enabled |
| <a href="#">FIDO2 security key</a>                                                                                                                                                                                                                                                   |           | No      |
| <a href="#">Microsoft Authenticator</a>                                                                                                                                                                                                                                              |           | No      |
| <a href="#">SMS</a>                                                                                                                                                                                                                                                                  | All users | Yes     |
| <a href="#">Temporary Access Pass</a>                                                                                                                                                                                                                                                |           | No      |
| <a href="#">Hardware OATH tokens (Preview)</a>                                                                                                                                                                                                                                       |           | No      |
| <a href="#">Third-party software OATH tokens</a>                                                                                                                                                                                                                                     |           | No      |
| <a href="#">Voice call</a>                                                                                                                                                                                                                                                           |           | No      |
| <a href="#">Email OTP</a>                                                                                                                                                                                                                                                            |           | Yes     |
| <a href="#">Certificate-based authentication</a>                                                                                                                                                                                                                                     |           | No      |

Comme peu d'utilisateurs se connectent sur le tenant je laisse les options par défaut (« Email OTP » & « SMS »).



4. « **Activer la réinitialisation de mot de passe en libre-service** » → « Gérer les propriétés » → « Suivant ».

Save Discard

Self service password reset enabled ⓘ

None Selected All

**i** These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

J'ai activé l'autonomie de réinitialisation pour tous les utilisateurs.

5. « **Configurer les notifications et la personnalisation de l'administrateur** » → « Gérer les notifications » → « Suivant ».

Password reset | Notifications ...

Lab Cap - Microsoft Entra ID for workforce

« Save Discard

✕ Diagnose and solve problems

Manage

Properties

Authentication methods

Notify users on password resets? ⓘ

Yes No

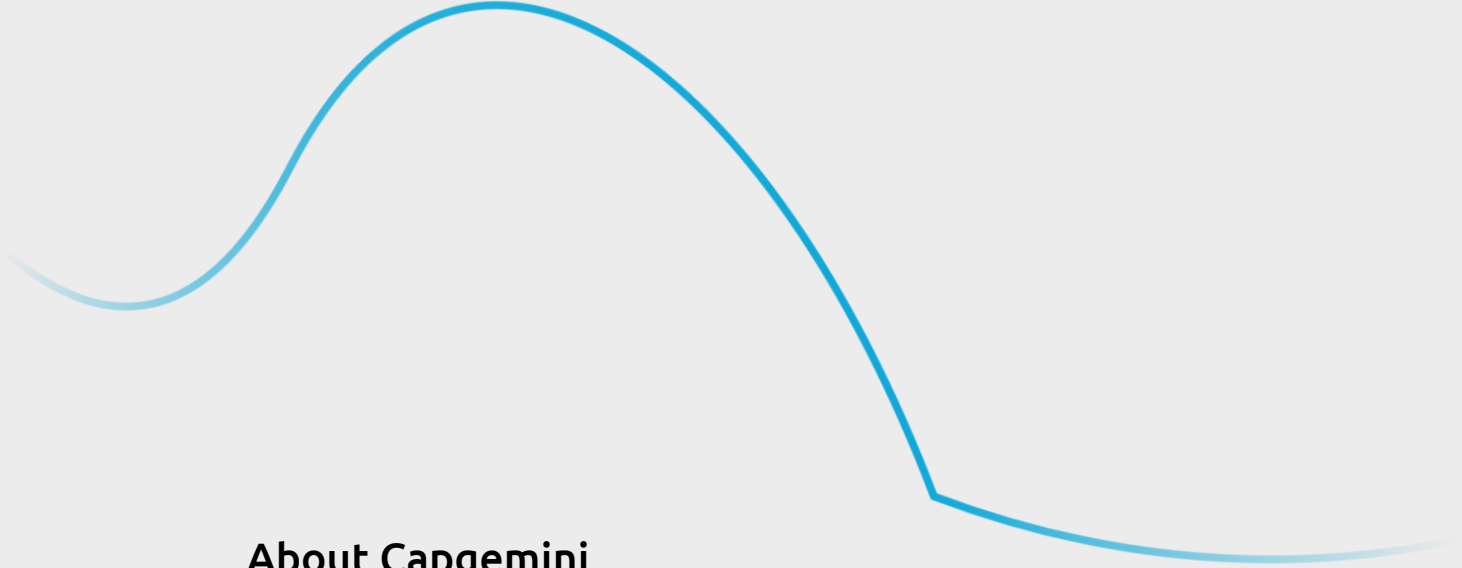
Notify all admins when other admins reset their password? ⓘ

Yes No

6. « **Terminer** » → « OK »

Les options identité sont configurées.

| Identité (2)                                                                  |         |                    |
|-------------------------------------------------------------------------------|---------|--------------------|
| Configurer l'authentification multifacteur (MFA)                              | Terminé | Microsoft Entra ID |
| Planifier votre déploiement de réinitialisation du mot de passe libre-service | Terminé | Microsoft Entra ID |

A thick, light blue line that starts on the left, curves upwards to a peak, then curves downwards to the right, ending in a slight upward curve.

## About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The group is guided every day by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organisation of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design of operations, fuelled by the fast evolving and innovative world of clouds, data, AI, connectivity, software, digital engineering and platforms. The group reported in 2022 global revenues of €22 billion.

Get the Future You Want | [www.capgemini.com](https://www.capgemini.com)



This document contains information that may be privileged or confidential and is the property of the Capgemini Group.

**Company Confidential.** Copyright © 2023 Capgemini. All rights reserved.