

CONFIGURATION MULTIFACTOR AUTHENTICATION (MFA)

Noah MAILLET
PROJET LAB-CAP





Table of contents

Preface	3
1 Connexion à Azure Directory.	4
2 Configuration – The multifactor authentication (MFA).	5



Preface.

La sécurité des données est au cœur des préoccupations de toute entreprise moderne. Les entreprises doivent protéger leurs informations sensibles contre un large éventail de menaces, qu'il s'agisse d'attaques de logiciels malveillants, de piratages de réseau, de vols d'identité ou d'autres formes de cybercriminalité.

Une étape essentielle pour renforcer la sécurité des données est d'adopter une stratégie de sécurité multicouche, qui combine plusieurs méthodes pour vérifier l'identité d'un utilisateur avant de lui donner accès à des informations sensibles ou à des ressources critiques. C'est là qu'intervient le Multifactor Authentication (MFA).

Le Multifactor Authentication (MFA) est une méthode de sécurité qui nécessite la vérification de l'identité de l'utilisateur à l'aide de plusieurs facteurs, souvent trois, avant de lui permettre d'accéder à des ressources ou à des informations sensibles. Ces facteurs peuvent inclure quelque chose que l'utilisateur connaît (comme un mot de passe), quelque chose qu'il possède (comme un téléphone portable ou un jeton de sécurité) et quelque chose qu'il est (comme une empreinte digitale ou un scan rétinien).

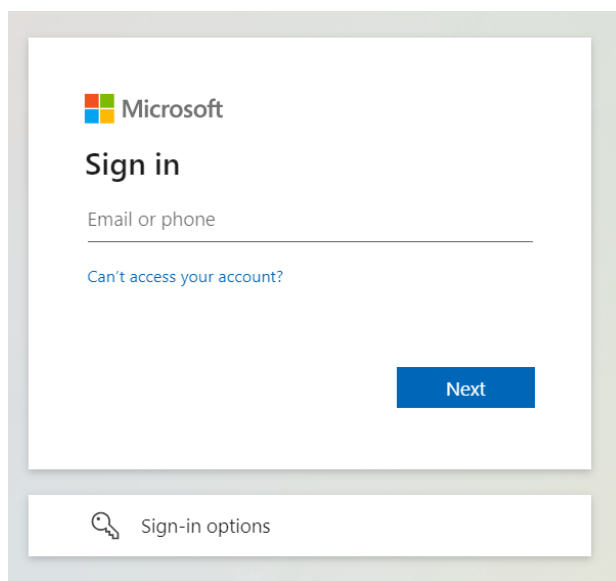
Azure Active Directory (Azure AD) est un service d'authentification cloud qui permet aux utilisateurs d'accéder à des ressources en ligne à l'aide de leurs identifiants de connexion. En combinant le MFA avec Azure AD, les entreprises peuvent ajouter une couche supplémentaire de sécurité pour protéger leurs ressources et données les plus précieuses. Cela signifie que même si un pirate parvient à voler les identifiants de connexion d'un utilisateur, il ne pourra pas accéder aux informations sensibles sans également fournir les autres facteurs d'authentification requis.

En somme, le Multifactor Authentication (MFA) pour azure Active Directory est une fonctionnalité de sécurité essentielle pour les entreprises modernes qui cherchent à protéger leurs ressources et données sensibles contre un large éventail de menaces. »

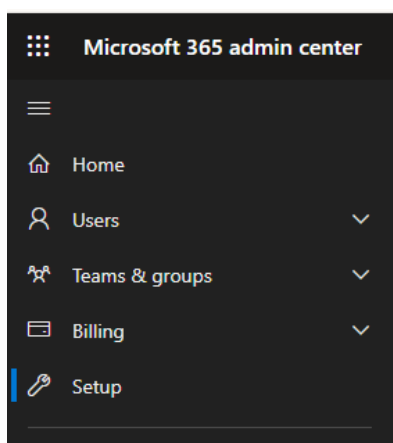


1 Connexion au Tenant Azure.

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



3. Je me connecte avec les identifiants administrateur du tenant.



4. Je me rends sur « Setup » :

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.

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



2 Configuration – The multifactor authentication (MFA).

1. Je clique sur « The multifactor authentication (MFA) » → « Prise en main » → « Next ».

Enforce multifactor authentication

Multifactor authentication (MFA) is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

Why is it important

- Secure against breaches from lost or stolen credentials
- Users are automatically protected when added to groups protected with Adaptive MFA
- MFA can help facilitate your users setup of Passwordless
- Block access automatically when conditions change like user and sign-in risk detection (requires P2 licensing)

Insights

Adaptive MFA using Conditional Access

☐ Off

Admins protected by MFA

2/2

[What does this mean and how it's calculated?](#)

[Keep your users up-to-date with customizable email templates?](#)

2. Je sélectionne « SMS (text) » → « Suivant ».

Choose Authentication methods for your organization

When choosing authentication methods for an organization, it's important to consider factors such as security, usability, scalability, and cost. Here are some authentication methods that could be suitable for most organizations, select at least one to start with.

High security

☐ Microsoft Authenticator App (recommended)

☐ FIDO 2 security keys

Medium security

☐ Third-party software OATH tokens

☐ Temporary Access Pass

Low security

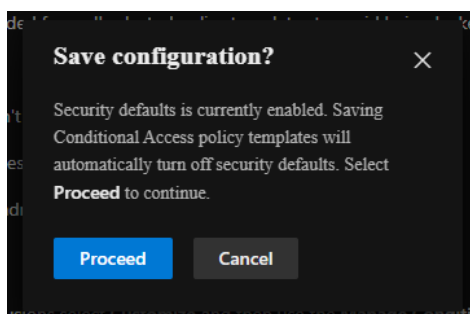
☒ SMS (text)

☒ Email One-time password

☐ Call



3. Je vérifie que les informations sont correctes → « Next ».
4. Je sauvegarde la configuration → « Proceed ».



5. Je coche la case « I attest that I've selected the low [...] my organisation vulnerable to attacks » et je sélectionne l'option « My end users don't want [...] mobile devices » → « Save configuration ».

Review and finish

Review the configuration for MFA policy. The policy will take effect immediately after you create it, and we recommend letting your users know how these changes will impact them.

Authentication methods

Low security: Email One-time password, SMS (text)

☒ I attest that I've selected the low security authentication methods that could be hacked via SIM hacking or other methods that could leave my organization vulnerable to attacks. [Learn more](#)

What is the reason for you to select low security authentication methods? (Optional)

My end users don't want to install the Authentication app on their mobile device

[Edit Authentication methods](#)

Adaptive MFA using Conditional Access

Require MFA for admins: Yes
User exemptions: Noah MAILLET

Block all legacy sign-ins that don't support MFA: Yes
User exemptions: Noah MAILLET

Require MFA for external and guest users: Yes
User exemptions: Noah MAILLET

Require MFA for internal users (admins not included) - Advanced risk detection: Yes
User exemptions: Noah MAILLET

[Edit MFA option](#)

[Back](#) [Save configuration](#)

6. « Done ».

Après chaque opération de sécurité le tenant, renvoie vers la page « Guides de déploiement avancé et assistance ».

Cette page regroupe des informations sur la sécurité du tenant elle permet aussi de renvoyer vers des guides pour la configuration des options de sécurité.



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



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.