

ANALYSEUR DE SÉCURITÉ

Noah MAILLET Projet LAB-CAP



Table of contents

Préfa	ce		3
1	Connexi	on au tenant	4
2	Analyseu	ır de sécurité	5
2.1	« Micros	oft Solution »	5
	2.1.1	«Configuration de l'identité initiale ».	5
	2.1.2	« Sécurité des identités de bases »	8
	2.1.3	«Identité et Automatisation avancées »	10
	2.1.4	«Vérification et finalisation ».	11



Préface

L'analyseur de sécurité Office 365 est un outil puissant qui offre une visibilité et un contrôle supplémentaire sur les activités et les configurations de sécurité dans l'environnement cloud de votre entreprise. En mettant en place cette fonctionnalité, vous pouvez identifier les menaces potentielles, réagir rapidement aux incidents de sécurité et améliorer votre posture de sécurité globale.

La procédure de configuration de l'analyseur de sécurité Office 365 comprend plusieurs étapes critiques. Tout d'abord, il est nécessaire de créer et de configurer une politique de sécurité appropriée, qui détermine comment les alertes de sécurité seront traitées. Ensuite, il faut déployer l'analyseur de sécurité et le connecter à votre environnement Office 365. Cela implique souvent d'installer un agent sur les appareils clients et de configurer les règles de collecte de données.

Une fois l'analyseur de sécurité configuré, il est important de suivre régulièrement les alertes de sécurité et d'y répondre rapidement. Cela peut impliquer d'investiguer les incidents de sécurité, de supprimer les menaces et les vulnérabilités, et de mettre en place des mesures pour prévenir de futurs incidents.



1 Connexion au tenant.

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

Next
Next

- 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)	O 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	O 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 Analyseur de sécurité.

1. «Overview»; «Analyse your security posture» → je réponds au questionnaire → « Suivant ».

2.1 « Microsoft Solution ».

« Review the benefits of Microsoft Entra ID premium »; « Deploy » → « Go to the Microsoft Entra setup guide » → « Suivant ».

2.1.1 « Configuration de l'identité initiale ».

Donnez aux utilisateurs privilégiés uniquement l'accès dont ils ont besoin.

Configuration d'un utilisateur administrateur. -

Établissez une identité commune entre le cloud et les utilisateurs locaux.

Pas de contrôleur de domaine local. \rightarrow Non applicable.

Contrôlez votre infrastructure d'identité sur site.

-Pas de contrôleur de domaine local → non applicable.

Donnez aux utilisateurs une expérience d'authentification familière.

Je clique sur « Donnez aux utilisateurs une expérience d'authentification familière ».

Étape 1 :

Le domaine a déjà été configuré au par avant.

Étape 2 :

« Configurer la marque de société » :

« Default sign-in experience » \rightarrow « Basics ».

1. J'ajoute le « Favicon »,

Favicon (i)

LOGO_SANDBOX_LABCAP-min.jpg	Brow
-----------------------------	------

se



Image size: 32x32px (resizable) Max file size: 5KB File Type: PNG (preferred), JPG, or JPEG Remove



2. J'ajoute le « Background image ».

Favicon 🛈	LOGO_SAN	DBOX_LABCAP-min.jpg	Browse
	LABCAP	lmage size: 32x32px (resizable) Max file size: 5KB File Type: PNG (preferred), JPG, or JPEG Remove	

3. Je configure le « background colour ».

Page background color 🛈	#036ed0 F	Remove			
				(
			0		1
	Hex	Red	Green	Blue	
	036ed0	3	110	208	

« Default sign-in experience » → « Layout ».

- 1. Je laisse les options par défaut → « Next: Header ».
- 2. « Default sign-in experience » → « Header ».
- 3. Je n'ai rien à modifier →« Next: Footer. »
- 4. « Default sign-in experience » → « Footer ».
- 5. Je décoche les options « Privacy & Cookie » & « Terms of use » → suivant.
- 6. « Default sign-in experience » \rightarrow « Sign-in form ».
- 7. Je sélectionne la « Banner logo ».

Banner logo (j)	Banner_LABCAP_245x36.png	Brows
	LABCAP.OVH	
	Image size: 245x36px Max file size: 50KB File Type: Transparent PNG, JPG, or JPEG	
	Bomovo	



8. Je sélectionne le « Square logo (light theme) »

Browse ×
lmage size: 240x240px (resizable) Max file size: 50KB File Type: PNG (preferred), JPG, or JPEG
AP

9. Je sélectionne le « Square logo (dark theme) »

Square logo (dark theme) 🛈	DARK.png		Browse
			×
	LABCAP	lmage size: 240x240px (resizable) Max file size: 50KB File Type: PNG (preferred), JPG, or JPEG Remove	

- a. Je décoche « Show self-service password reset ».
- b. Je n'ai rien à modifier →« Next: Review. »
- 10. « Review »

a. Je vérifie que les informations sont correctes → « Create ».
 11. Après avoir fini la configuration je sélectionne terminer → suivant.



2.1.2 « Sécurité des identités de bases ».

- « Permettre aux utilisateurs de gérer eux-mêmes les informations d'identification en toute sécurité » :
 - o Déjà détaillé en amont
 - Terminé.
 - « Créez des stratégies pour gérer l'accès aux applications et aux services d'entreprise » :
 - Dans notre contexte nous n'avons pas besoin de créer des stratégies pour l'accès des applis.
 Non applicable.
- « Intégrer des applications cloud tierces pour améliorer la sécurité et l'expérience utilisateurs » :
 - Cette option a été détaillée par un autre collaborateur.
 - Terminé.
 - « Implémenter une authentification forte sans mot de passe » :
 - Cette option n'est pas nécessaire pour notre configuration
 - Non applicable.
- « Permettre aux utilisateurs finaux de créer et gérer l'appartenance à un groupe cloud » :
 - Cette option n'est pas nécessaire pour notre configuration
 - Non applicable.
- « Détecter et empêcher l'utilisation de mots de passe courants et faibles ».
 - Custom smart lockout:
 - Lockout threshold:

Lockout threshold ()	10					
 Lockout duration in seconds: 						
Lockout duration in seconds ①	60					
 Custom banned passwords: Enforce custom list: 						
Enforce custom list 🛈	Yes	No				
 Custom banned password list → 'à laisser vide' Password protection for windows Server active Directory: Enable password protection on the server active directory: 						
Enable password protection on Window Server Active Directory ①	s Yes	No				
 Mode : 						

Mode 🛈 Enforced Audit



Si vous avez la suivie la configuration si dessus vous devriez avoir ce résultat :

Tâche recommandée	Priorité	Fonctionnalités	État
Permettre aux utilisateurs de gérer eux-mêmes les informations d'identification en toute sécurité	Moyen	Réinitialisation de mot de passe en libre-service (SSPR)	Terminé
Créez des stratégies pour gérer l'accès aux applications et aux services d'entreprise	Élevé	Stratégies d'accès conditionnel, MFA	Non applicable V
Intégrer des applications cloud tierces pour améliorer la sécurité et l'expérience utilisateur	Élevé	Authentification unique	Terminé
Implémenter une authentification forte sans mot de passe	Moyen	Authentification sans mot de passe	Non applicable V
Permettre aux utilisateurs finaux de créer et gérer l'appartenance à un groupe cloud	Faible	Gestion des groupes en libre-service	Non applicable V
Détecter et empêcher l'utilisation de mots de passe courants et faibles.	Moyenne	Protection par mot de passe	Terminé v



2.1.3 « Identité et Automatisation avancées ».

- « Créer des stratégies automatisées pour les événements de risque lié aux utilisateurs et aux connexions. »
 - Dans notre contexte nous n'avons pas d'utilisateurs :
 - Non applicable.
 - « Automatiser l'approvisionnement des utilisateurs dans les applications SaaS tierces. » :
 - Dans notre contexte nous n'avons pas à configurer cette option
 - non applicable.
- « Approuver et déléguer l'accès administrateur temporel » :
 - Dans notre contexte nous n'avons pas à configurer cette option.
 - Non applicable.
 - « Automatiser les requêtes d'accès, les affectations et autres ».
 - Dans notre contexte nous n'avons pas à configurer cette option :
 - Non applicable.
- « Évaluez les appartenances aux groupes l'accès aux applications et les rôles ».
 - Dans notre contexte nous n'avons pas à configurer cette option :
 - Non applicable.

Si vous avez suivi notre configuration vous devriez avoir cette configuration :

Tâche recommandée	Priorité	Fonctionnalités	État
Créer des stratégies automatisées pour les événements de risque liés aux utilisateurs et aux connexions	Élevé	de protection d'identitéMicrosoft Entra ID	Non applicable
Automatiser l'approvisionnement des utilisateurs dans les applications SaaS tierces	Faible	Approvisionnement automatique des utilisateurs	\odot Non applicable \checkmark
Approuver et déléguer l'accès administrateur temporel	Élevé	Privileged Identity Management (PIM)	\odot Non applicable \checkmark
Automatiser les requêtes d'accès, les affectations et autres	Moyenne	Gestion des droits d'utilisation.	8 Non applicable
Évaluez les appartenances aux groupes, l'accès aux applications et les rôles.	Moyenne	Révisions d'accès	8 Non applicable



2.1.4 « Vérification et finalisation ».

1. Je vérifie que toutes les informations sont correctes. →Suivant.

📀 Véri	fication	et finalisa	tion		
Ovus avez besoin d'aide pour ce produit ? FastTrack aide les clients disposant d' <u>abonnements Microsoft 365 éligibles</u> à déployer des solutions cloud Microsoft 365 sans frais supplémentaires. Pour obtenir de l'aide, envoyez une <u>demande de support FastTrack</u> .					
Vous avez tern	niné le guide de co	onfiguration de Micro	osoft Entra ID	. Après avoir examiné l'état des tâches	
recommandée	s ci-dessous, passe	ez à la section ressou	urces supplém	nentaires.	
recommandée 쥿 Nous air	s ci-dessous, passe nerions recevoir v	ez à la section ressou os commentaires.	urces supplém	ournir des commentaires à Microsoft	×
recommandée	s ci-dessous, passe nerions recevoir v é de l'état de chao	ez à la section ressou os commentaires. cune des tâches reco	urces supplém Fi	ournir des commentaires à Microsoft	×



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.