

GUIDE INSTALLATION DE MICROSOFT DEFENDER POUR OFFICE 365

Noah MAILLET Projet LAB-CAP



Table of contents

Prefa	ce		. 3
1	Connexio	on Tenant office 365	. 4
2	Guide d'i	nstallation de défendre pour office 365	. 5
2.1	Vue d'en	semble	. 5
2.2	« Рге́рага	stion » — Création des utilisateurs :	. 6
	2.2.1	Création de l'Administrateur général	. 6
	2.2.2	Création de l'administrateur de sécurité :	. 8
	2.2.3	Création de l'administrateur de simulation d'attaque :	10
2.3	Configur	ation des rôles :	12



Preface

Office 365 Defender est un service de sécurité avancé qui offre une protection en temps réel contre les menaces avancées dans votre environnement Microsoft Office 365. En configurant et installant correctement ce service, vous pouvez protéger vos données et vos ressources contre les attaques de phishing, de ransomware et d'autres menaces potentielles.

La procédure de configuration et d'installation de Defender pour Office 365 implique plusieurs étapes critiques. Tout d'abord, il est nécessaire de planifier et de préparer votre environnement pour l'installation. Cela inclut la création d'un compte d'administrateur avec les permissions appropriées et la vérification de la compatibilité des logiciels avec votre système.

Ensuite, il faut télécharger et installer le client Defender pour Office 365 sur chaque appareil client dans votre environnement. Cela implique souvent l'utilisation de PowerShell ou d'autres outils de gestion pour automatiser le processus.

Une fois l'installation terminée, 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 Tenant office 365.

- 1. Je vais sur mon navigateur habituel.
- 2. Je me rends sur le portail

administrateur (<u>https://admin.microsoft.com/Adminportal/Home#/homepage</u>):

Microsoft		
Sign in		
Email or phone		
C/		
can t access your account?		
Can Laccess your account?		
Can't access your account?	Next	
Can t access your account?	Next	
Can t access your account?	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 1	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	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 Guide d'installation de défendre pour office 365.

2.1 Vue d'ensemble.

- 1. «Vue d'ensemble » → « Suivant ».
- 2. « Préparation » « Autorisations de défendre pour office 365 ».

Tâche	Description
Administrateur général	Le rôle d'administrateur général dans Microsoft 365 est une position administrative critique responsable de la gestion et de la sécurisation de l'environnement de courrier et de collaboration du organization.
Administrateur de sécurité	Le rôle Administrateur de la sécurité dans Microsoft 365 est une position administrative spécialisée qui se concentre sur la protection de l'infrastructure et des données informatiques du organisation.
Administrateur de simulation d'attaque	Le rôle d'administrateur de simulation d'attaques dans Microsoft 365 est une position spécialisée visant le renforcement de la posture de sécurité d'un organisation par le biais de cyberattaques simulées.
Gestion de l'organisation dans Exchange Online	Le rôle Gestion de l'organisation dans Exchange Online offre un contrôle et une supervision complets sur l'environnement Exchange Online au sein d'une organisation.

Ci-dessus on peut voir que l'on doit avoir les administrateurs suivants :

- Administrateur général,
- Administrateur de sécurité
- Administrateur de simulation d'attaque.



2.2 « Préparation » — Création des utilisateurs :

2.2.1 Création de l'Administrateur général.

- 1. Je me rends dans Identité.
- 2. «Users » → « All users » → « New user » → je rentre les informations de l'utilisateurs :

Create new user Create a new internal user in your organiz	ation				
Basics Properties Assignmer	nts Review + create				
Create a new user in your organization	. This user will have a user na	ame	like alice@contoso.com. Le	arn mo	ore 🛙
Identity					
User principal name *	gadmin	@[labcap.ovh Domain not listed ☑	~	D
Mail nickname *	gadmin				
	Derive from user principal name				
Display name	Administrateur Général				
Password *	•••••			٢	D
Account enabled 🕕	 Auto-generate password 	1			

3. «Next: Properties ».

4. Je remplis les informations de « identity » :

Identity		
First name	Administrateur	
Last name	General	
User type	Member	\sim
Authorization info	+ Edit Certificate user IDs	

5. Je remplis les informations de « Parental Control » :

Parental controls		
Age group	Adult	\sim
Consent provided for minor	Not required	\sim

6. Je remplis les informations de « Settings » :

Settings		
Usage location	France	\sim



- 7. «Next Assignments ».
- 8. «Addgroup » → je sélectionne « Lab Cap » → « Select » :



9. «Add Role» → je recherche «Global Administrator» et je sélectionne le rôle «Global administrator» → «Select».

Directory roles		×
Choose admin roles that you want to	o assign to this user.	Learn more
🔎 Global a	×	
Role	\uparrow_{\downarrow}	Description
Slobal Administrator		Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.

10. « Next: Review + Create » → je vérifie que toutes les informations sont correctes → « Create ».

Create new user Create a new internal user in your organization						
Basics	Properties	Assignme	ents	Review + create		
Basics						
User prir	ncipal name		gadm	nin@labcap.ovh 🜓		
Display r	name		Admi	nistrateur Général		
Mail nick	kname		gadm	nin		
Password	d			•••••	•	
Account	enabled		Yes			
Propert	ies		6 alara 5			
Last nam			Gene	ral		
User typ	e		Mem	ber		
Age grou	up		Adult			
Consent	provided for mi	nor	Not required			
Usage lo	cation		Franc	e		
Assignn	nents					
Administ	trative units					
Groups			Lab C	Сар		
Roles			Globa	al Administrator		



2.2.2 Création de l'administrateur de sécurité :

- 1. Je me connecte à la console d'administration.
- 2. Je me rends dans Identité.
- 3. «Users » → « All users » → « New user » → je rentrer les informations de l'utilisateurs :

Create new user ···· Create a new internal user in your organization							
Basics Properties Assignm	Basics Properties Assignments Review + create						
Create a new user in your organizati	ion. This user will have a user name like alice@contoso.com. Learn more 🛽						
Identity							
User principal name *	sadmin @ labcap.ovh V Domain not listed I						
Mail nickname *	sadmin						
	Derive from user principal name						
Display name	Administrateur de sécurité						
Password *	••••••						
	🖌 Auto-generate password						
Account enabled (i)							

4. «Next Properties ».

5. Je remplis les informations « D'identity » :

Identity		
First name	Administrator	
Last name	Security	
User type	Member	~
Authorization info	+ Edit Certificate user IDs	

6. Je remplis les informations de « Parental Controls » :

Parental controls		
Age group	Adult	~
Consent provided for minor	Not required	\sim

7. Je remplis les informations de « Settings » :

Settings		
Usage location	France	\sim

8. «Next: Assignements »

9. «Addgroup » → je sélectionne « Lab Cap » → « Select » :





Directory roles		\times
Choose admin roles that you want to assign to this user.	Learn more	
Role ↑↓	Description	
🗌 🏰 Cloud App Security Administrator	Can manage all aspects of the Cloud App Security product.	
🗹 🛛 🎍 Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	

11. « Next: Review + create » →je vérifie la conformité des informations →Create.

Create new user Create a new internal user in your organization						
Basics	Properties	Assignme	nts	Review + create		
Basics						
User princi	pal name		sadmin@labcap.ovh 🜓			
Display na	me		Admini	strateur de sécurité		
Mail nickn	ame		sadmin			
Password			•••••	••••	•	
Account er	nabled		Yes			
Propertie	s					
First name			Admini	strator		
Last name		Security				
User type		Member				
Age group		Adult				
Consent provided for minor		or	Not required			
Usage loca	ition		France			
Assignme	ents					
Administra	itive units					
Groups			Lab Cap	þ		
Roles			Security Administrator			



2.2.3 Création de l'administrateur de simulation d'attaque :

- 1. Je me connecte à la console d'administration.
- 2. Je me rends dans Identité.
- 3. «Users » → « All users » → « New user » → je rentre les informations de l'utilisateurs :

Identity			
User principal name *	saadmin	@ labcap.ovh Domain not listed E	✓ D 3
Mail nickname *	saadmin	er principal name	
Display name	Administrateur de	sécurité	
Password *	✓ Auto-generate	password	• Î
Account enabled (i)	~		

4. «Next: Properties »

5. Je remplis les informations « d'identity » :

Identity	
First name	Administrateur
Last name	De simulation d'attaque
User type	Member ~
Authorization info	+ Edit Certificate user IDs

6. Je remplis les informations de « Parental controls » :

Parental controls Age group Adult ✓ Consent provided for minor Not required ✓

France

7. Je remplis les informations de « Settings » :

Settings

Usage location

 \sim



- 8. «Next: Assignements »:
- 9. «Add Group » → je sélectionne « Lab Cap » → « Select » :



10. « Add Role » → je recherche et sélectionne « Attack Simulation Administrator » → « Select » :

۹	Attack Simulation Administrator	×	
	Role	\uparrow_{\downarrow}	Description
~	🍰 Attack Simulation Administrator		Can create and manage all aspects of attack simulation campaigns.

11. « Next: Review + create ».

12. « Review + Create » → je vérifie que les informations sont correctes → « Create ».



2.3 Configuration des rôles :

1. Les administrateurs demandés sont créés :

AD	Administrateur de sécurité	sadmin@labcap.ovh [🗋	Member
AD	Administrateur de simulation d'attaque	saadmin@labcap.ovh 🗈	Member
AG	Administrateur Général	gadmin@labcap.ovh 🗋	Member

- 2. « Administrateur Général » :
- J'ai créé « gadmin » qui est mon administrateur général donc je positionne l'état de progression sur terminer.
 - 3. « Administrateur de sécurité » :
- J'ai créé « sadmin » qui est mon administrateur de sécurité donc je positionne l'état de progression sur terminer.
 - 4. « Administrateur de simulation d'attaque » :
- «Ajouter des utilisateurs et des rôles » → je recherche « Administrateur de simulation d'attaque »
 → je sélectionne les rôles suivants :
 - o Administrateur de conformité,
 - o Administrateur de données de conformité,
 - Lecteur sécurité.

Sélectionner des utilisateurs pour ajouter des rôles *				
Administrateur de simulation d'atta ×				
Quels rôles attribuez-vous aux utilisateurs ? *				
Administrateur de conformité				
Administrateur des données de conformité				
Administrateur général				
Administrateur de la sécurité				
✓ Lecteur sécurité				

- « Enregistrer les modifications ».
- Je positionne l'état de progression sure terminée.



- 5. « Gestion de l'organisation dans Exchange online » :
- Je sélectionne « Administrateur de sécurité » → « Mettre à jour les rôles » → je sélectionne les rôles :
 - Administrateur de la sécurité,
 - Lecteur de sécurité.

• «Enregistrer les modifications. »

Si vous avez suivi les mêmes configurations voici les résultats que vous devriez avoir :

Tâche	Description	Attribuée à	Date d'échéance	Progression
Administrateur général	Le rôle d'administrateur général dans Microsoft 365 est une position administrative critique responsable de la gestion et de la sécurisation de l'environnement de courrier et de collaboration du organization.		January 29, 2024	Terminé
Administrateur de sécurité	Le rôle Administrateur de la sécurité dans Microsoft 365 est une position administrative spécialisée qui se concentre sur la protection de l'infrastructure et des données informatiques du organisation.		January 29, 2024	Terminé
Administrateur de simulation d'attaque	Le rôle d'administrateur de simulation d'attaques dans Microsoft 365 est une position spécialisée visant le renforcement de la posture de sécurité d'un organisation par le biais de cyberattaques simulées.		January 29, 2024	Terminé
Gestion de l'organisation dans Exchange Online	Le rôle Gestion de l'organisation dans Exchange Online offre un contrôle et une supervision complets sur l'environnement Exchange Online au sein d'une organisation.		January 29, 2024	Terminé



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.