GUIDE INSTALLATION DE MICROSOFT DEFENDER POUR OFFICE 365

Noah MAILLET

Projet LAB-CAP

Table of contents

Company Confidential. © 2023 Capgemini. All rights reserved.

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.

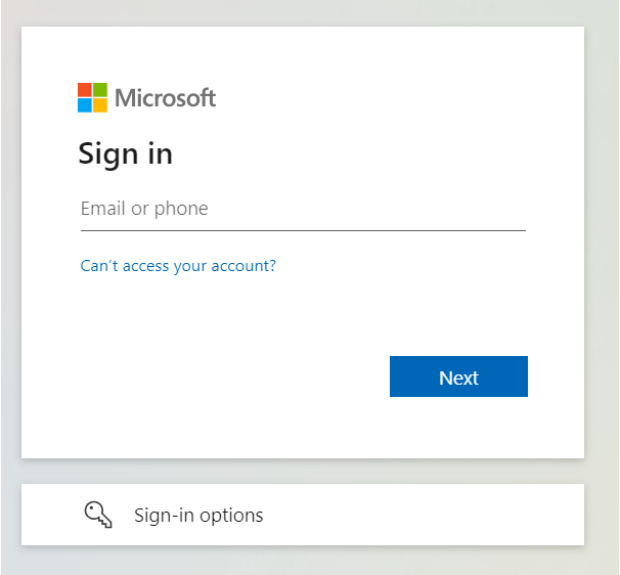
Ensuite, il faut télécharger et installer le client Defender pour Office 365 sur chaque appareil client dans votre environnement. Cela implique souvent l'utilisation de PowerShell ou d'autres outils de gestion pour automatiser le processus.

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.

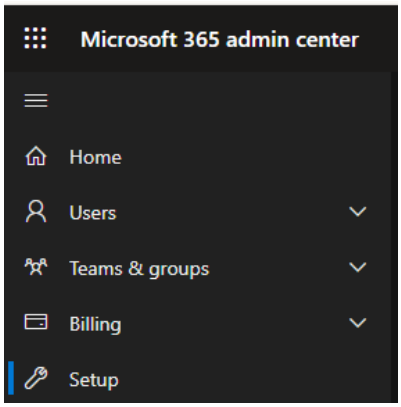
Company Confidential. © 2023 Capgemini. All rights reserved.

1 Connexion Tenant office 365.

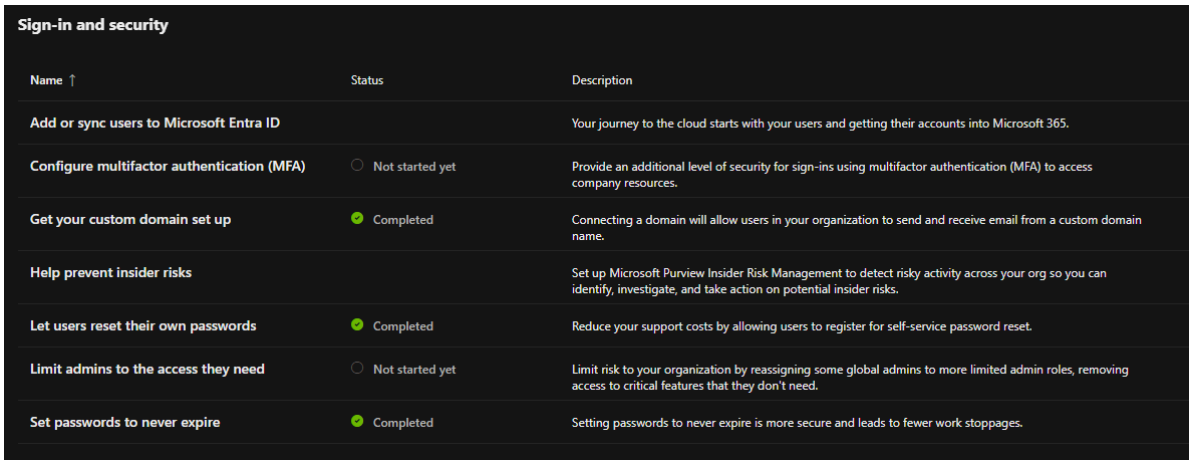
1. Je vais sur mon navigateur habituel.
2. Je me rends sur le portail administrateur (https://admin.microsoft.com/Adminportal/Home#/homepage) :



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



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



Company Confidential. © 2023 Capgemini. All rights reserved.

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 :

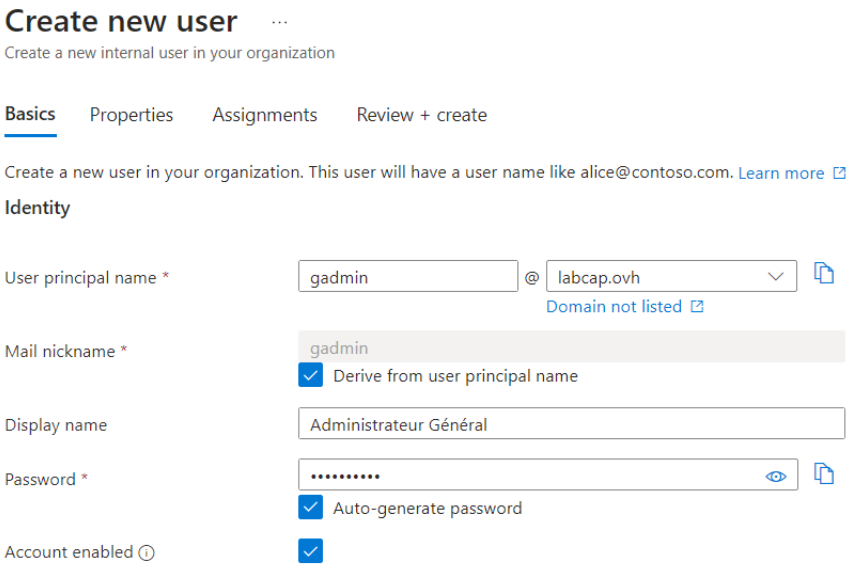
- Administrateur général,
- Administrateur de sécurité
- Administrateur de simulation d’attaque.

Company Confidential. © 2023 Capgemini. All rights reserved.

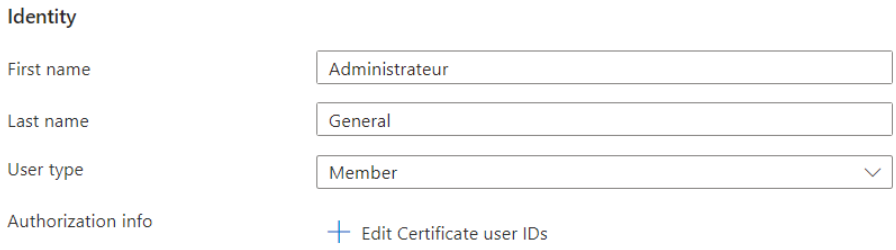
2.2 « Préparation » — Création des utilisateurs :

2.2.1 Création de l'Administrateur général.

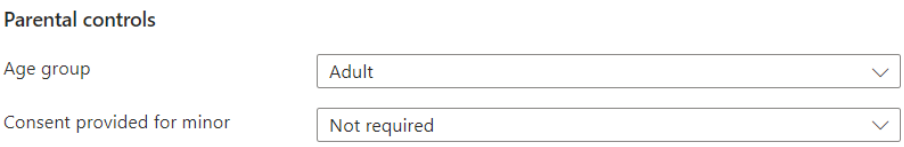
1. Je me rends dans Identité.
2. « Users » ➔« All users » ➔« New user » ➔je rentre les informations de l'utilisateurs :



3. « Next: Properties ».
4. Je remplis les informations de « identity » :

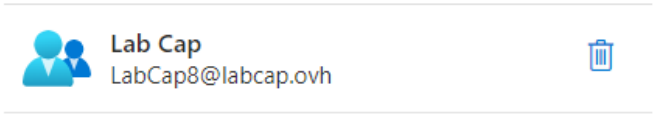


5. Je remplis les informations de « Parental Control » :

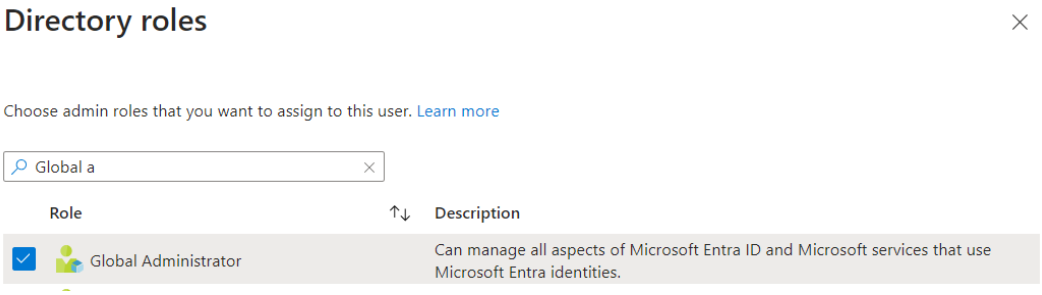


6. Je remplis les informations de « Settings » :

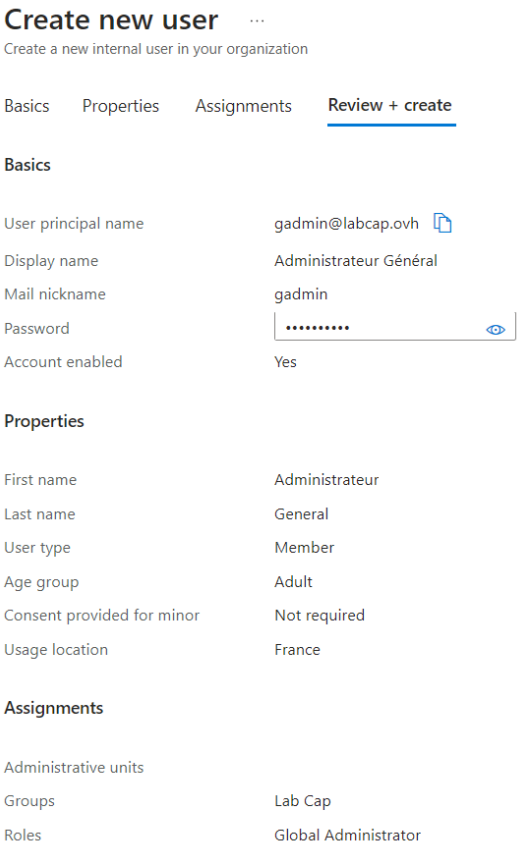
7. « Next Assignments ».
8. « Addgroup » ➔je sélectionne « Lab Cap » ➔« Select » :



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



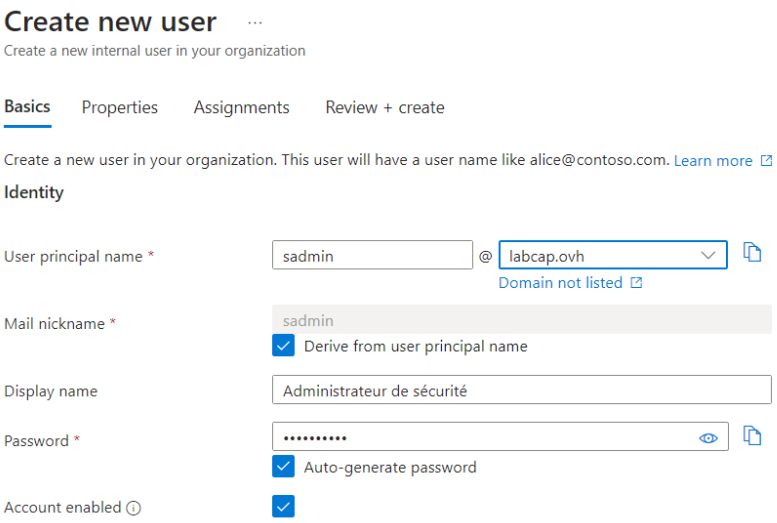
10. « Next: Review + Create » ➔je vérifie que toutes les informations sont correctes ➔« Create ».



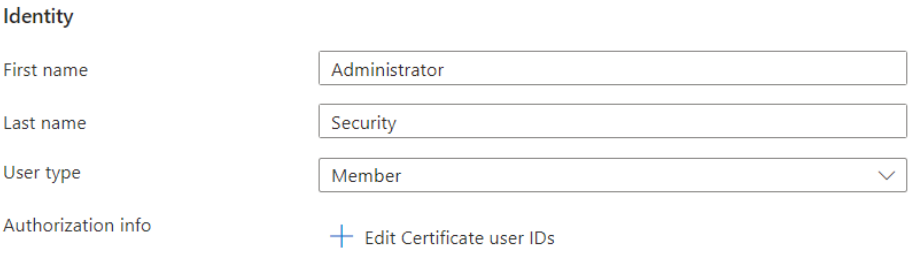
Company Confidential. © 2023 Capgemini. All rights reserved.

2.2.2 Création de l'administrateur de sécurité :

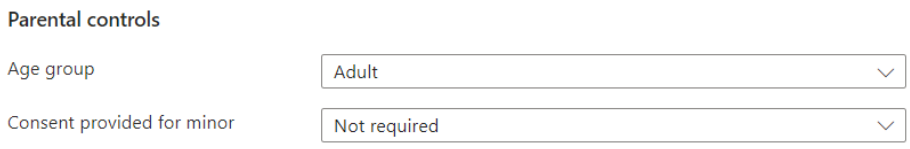
1. Je me connecte à la console d'administration.
2. Je me rends dans Identité.
3. « Users » ➔« All users » ➔« New user » ➔je rentrer les informations de l'utilisateurs :



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

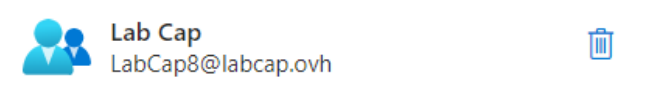


6. Je remplis les informations de « Parental Controls » :



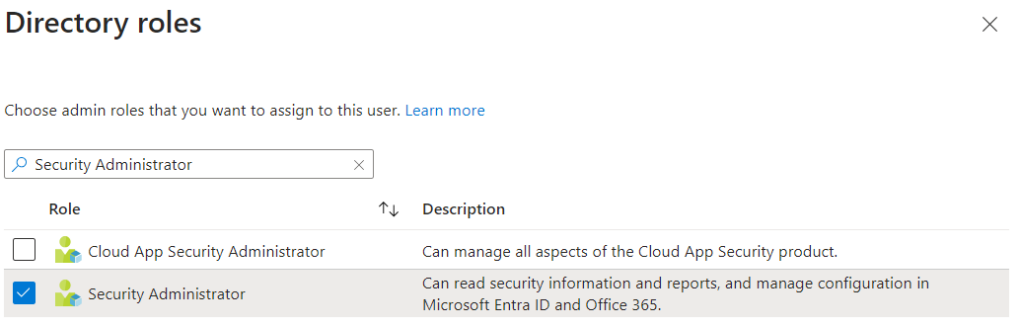
7. Je remplis les informations de « Settings » :

8. « Next: Assignements »
9. « Addgroup » ➔je sélectionne « Lab Cap » ➔« Select » :

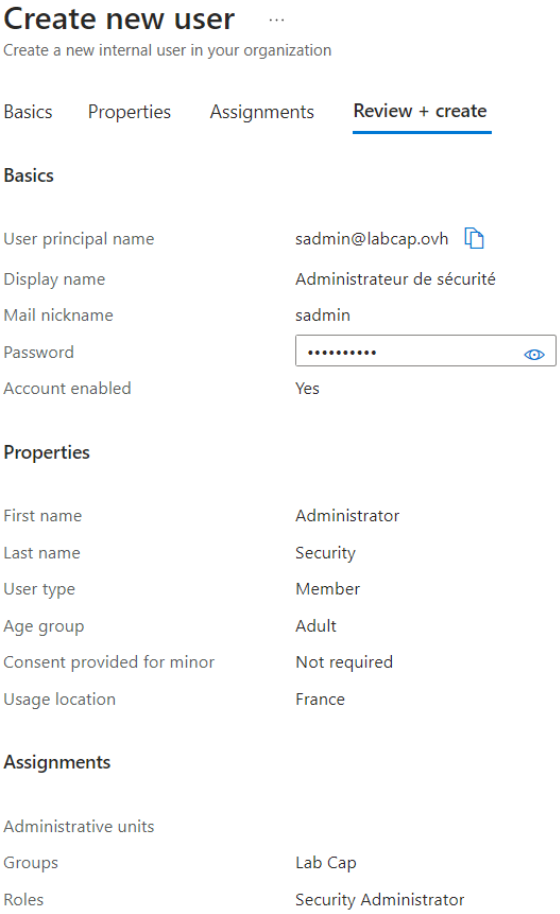


Company Confidential. © 2023 Capgemini. All rights reserved.

10. « Add Role » ➔je recherche et je sélectionne le rôle « Security Administrator » ➔« Select » :



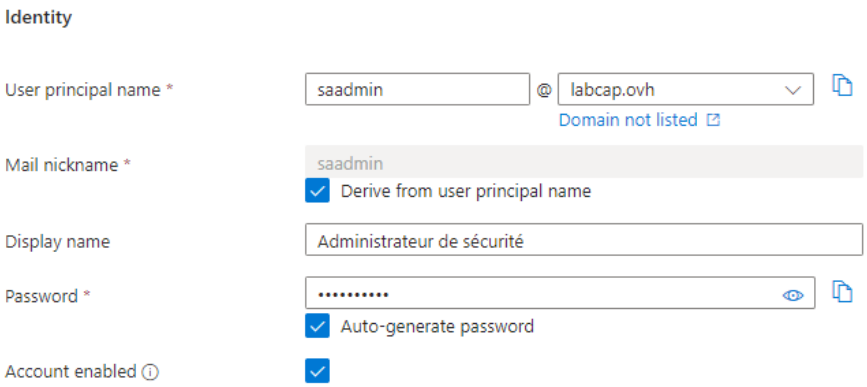
11. « Next: Review + create » ➔je vérifie la conformité des informations ➔Create.



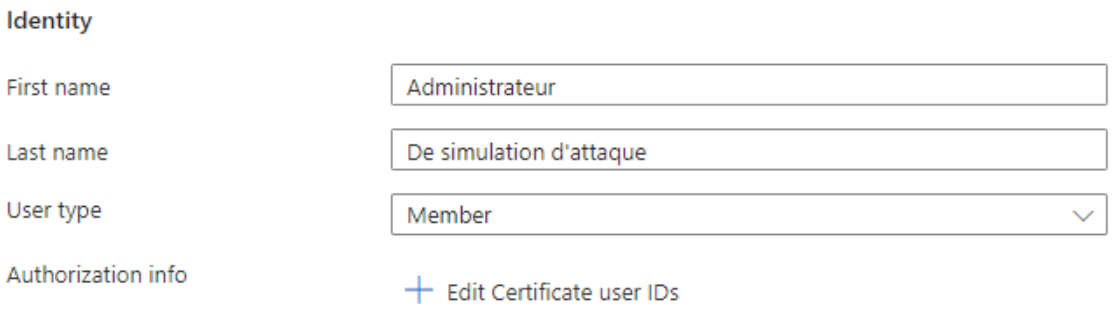
Company Confidential. © 2023 Capgemini. All rights reserved.

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

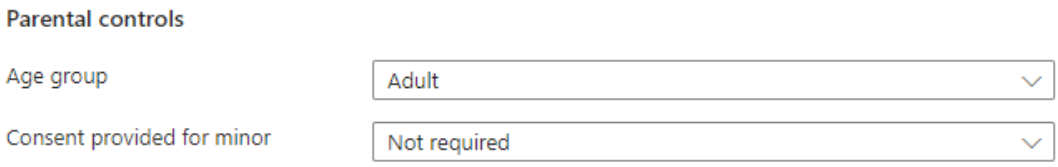
1. Je me connecte à la console d'administration.
2. Je me rends dans Identité.
3. « Users » ➔« All users » ➔« New user » ➔je rentre les informations de l'utilisateurs :



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

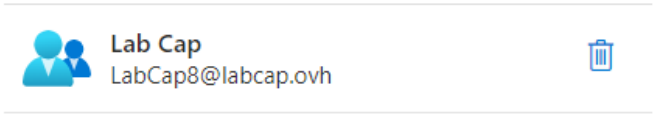


6. Je remplis les informations de « Parental controls » :

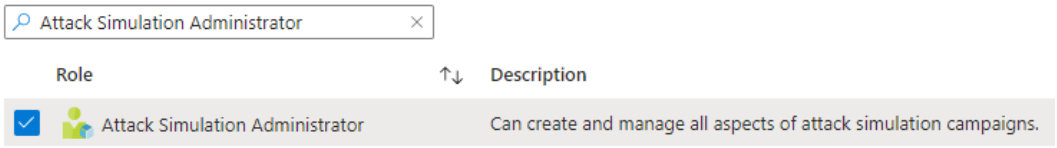


7. Je remplis les informations de « Settings » :

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



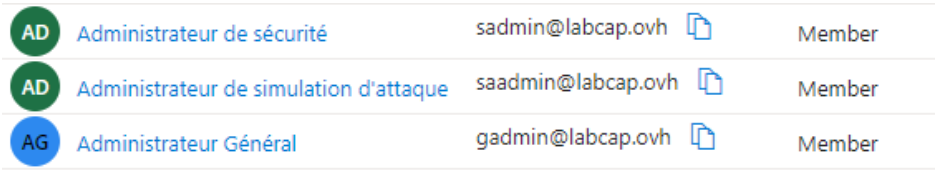
10. « Add Role » ➔je recherche et sélectionne « Attack Simulation Administrator » ➔« Select » :



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 :



2. « Administrateur Général » :

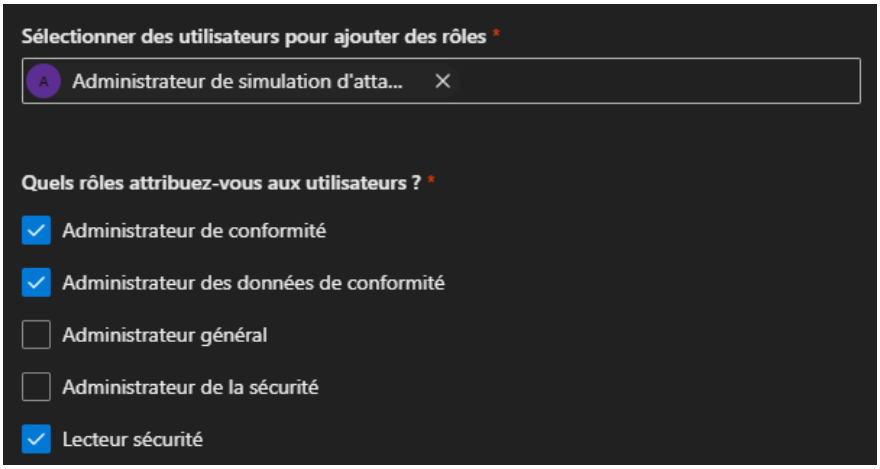
- J'ai créé « gadmin » qui est mon administrateur général donc je positionne l'état de progression sur terminer.

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 :
  - Administrateur de conformité,
  - Administrateur de données de conformité,
  - Lecteur sécurité.

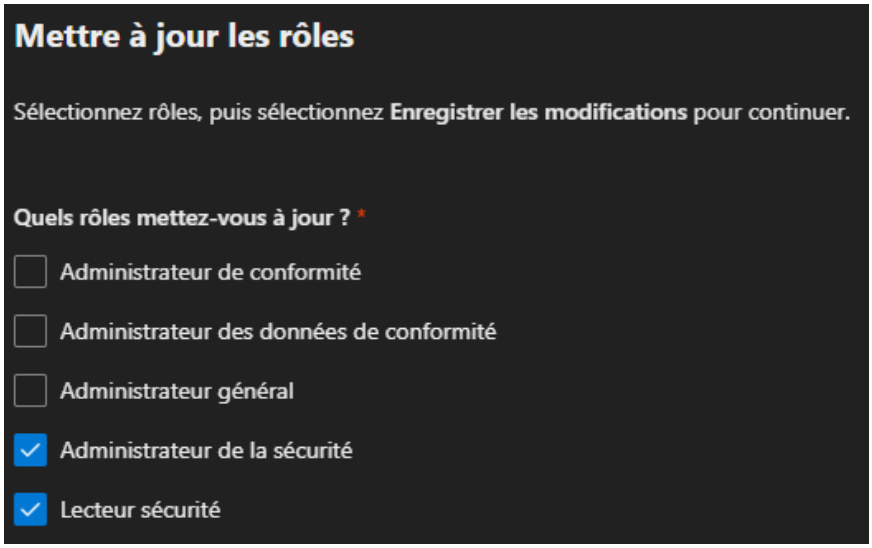


- « Enregistrer les modifications ».
- Je positionne l'état de progression sure terminée.

Company Confidential. © 2023 Capgemini. All rights reserved.

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

Company Confidential. © 2023 Capgemini. All rights reserved.

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.