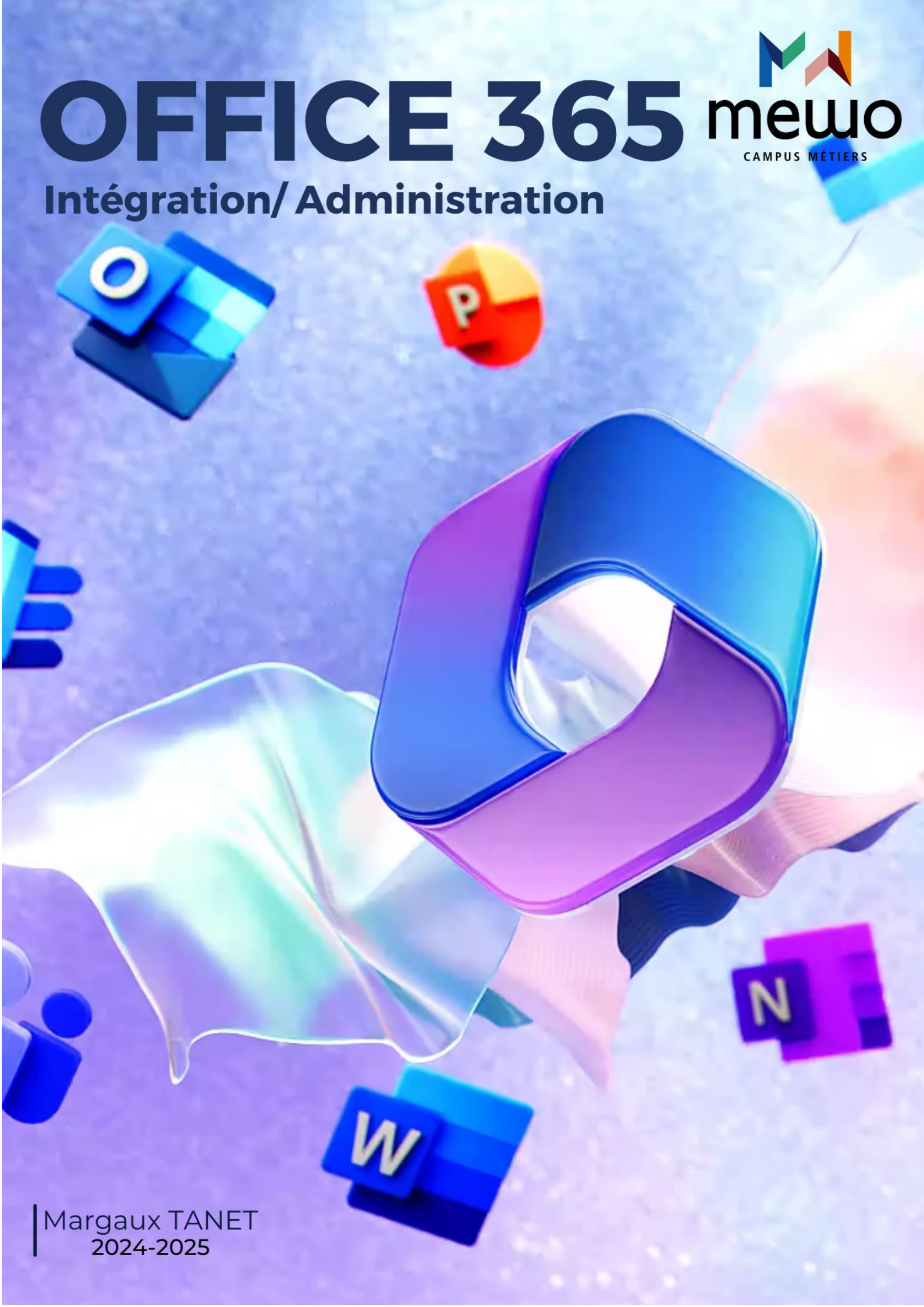
OFFICE 365

Intégration/ Administration

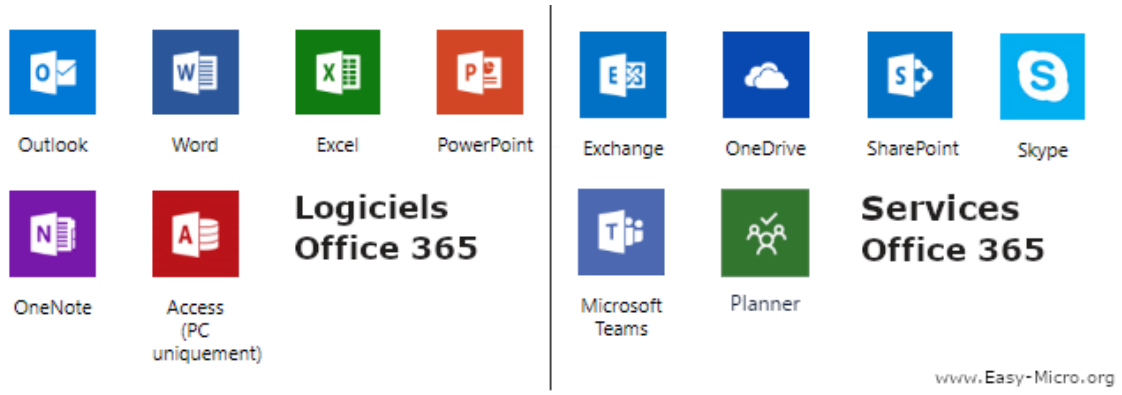
mewo
CAMPUS MÉTIERS



Margaux TANET
2024-2025

Introduction :

Office 365, plus connu sous le nom de Microsoft 365 aujourd'hui, est rattaché à un ensemble de services Cloud. Il est constitué de la suite Office ainsi que d'un ensemble de services en lignes.



Ensemble de la suite office (Excel, Word, ...) et de service en lignes (Exchange, Teams,)

Grâce au cloud, les utilisateurs peuvent accéder à leurs fichiers et leurs applications depuis n'importe quel appareil à tout moment ce qui favorise ainsi le travail à distance et la collaboration en temps réel.

Le centre d'administration Microsoft 365, Microsoft Defender et le portail de conformité Microsoft Purview permettent de gérer directement les autorisations des utilisateurs qui effectuent des tâches de sécurité et de conformité dans Microsoft 365. Ces portails gèrent les autorisations de manière centralisée.

Objectif :

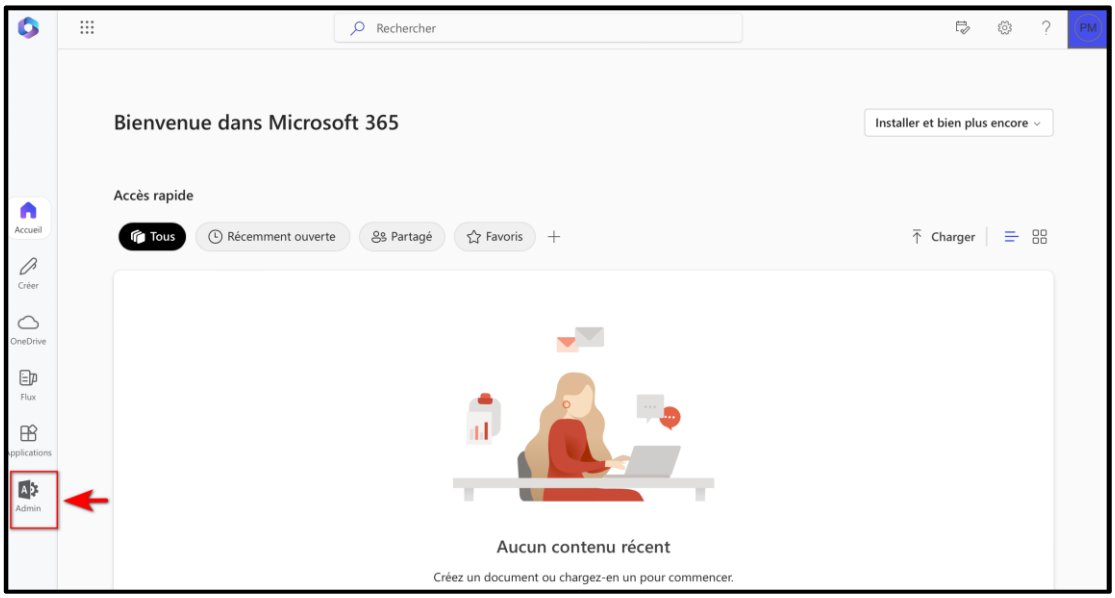
L'objectif est de mettre en place un office 365 avec la création d'un utilisateur puis l'achat de sa licence. Il faudra configurer la messagerie afin d'avoir une synchronisation au niveau des mails avec office 365. Il sera important de voir les différentes méthodes que l'on peut mettre en place pour assurer la sécurité et l'accessibilité aux différentes interfaces.

Table des matières

I- Accès au centre d'administration

Le centre d'administration permet la gestion d'autorisations au sein de l'environnement Microsoft 365 d'une entreprise. Il prend en charge la gestion des utilisateurs/ groupes ; contrôle l'accès basé sur les rôles Azure ; gère les autorisations d'applications. Il permet donc en tant qu'administrateur d'attribuer des rôles, de configurer des autorisations, de garantir un contrôle d'accès sécurisé.

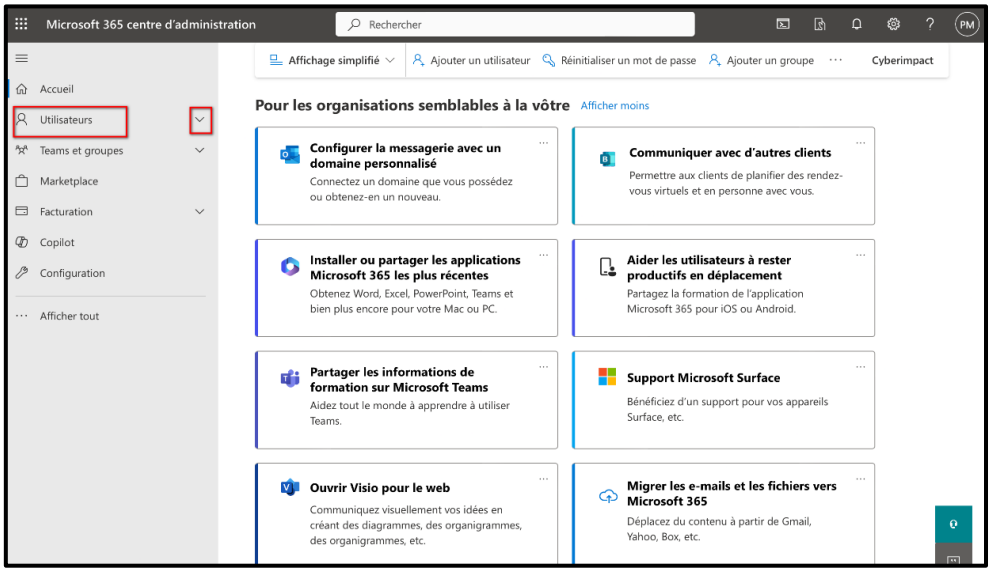
Voici la page d'accueil Office 365 : Cliquer sur « **admin** » en bas à gauche pour accéder au **centre d'administration**.



Centre d'administration Office 365

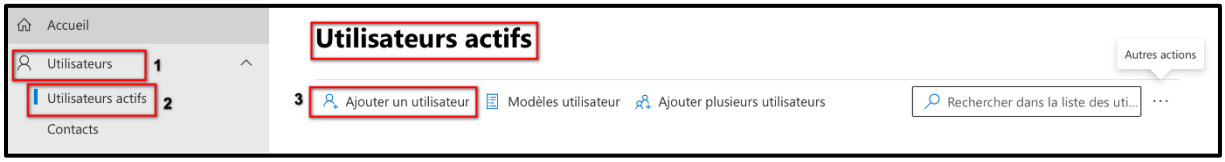
II- Le centre d'administration

Une fois arrivé sur la page du centre d'administration, se rendre dans l'onglet « **utilisateurs** » et aller sur « **les utilisateurs actifs** » :

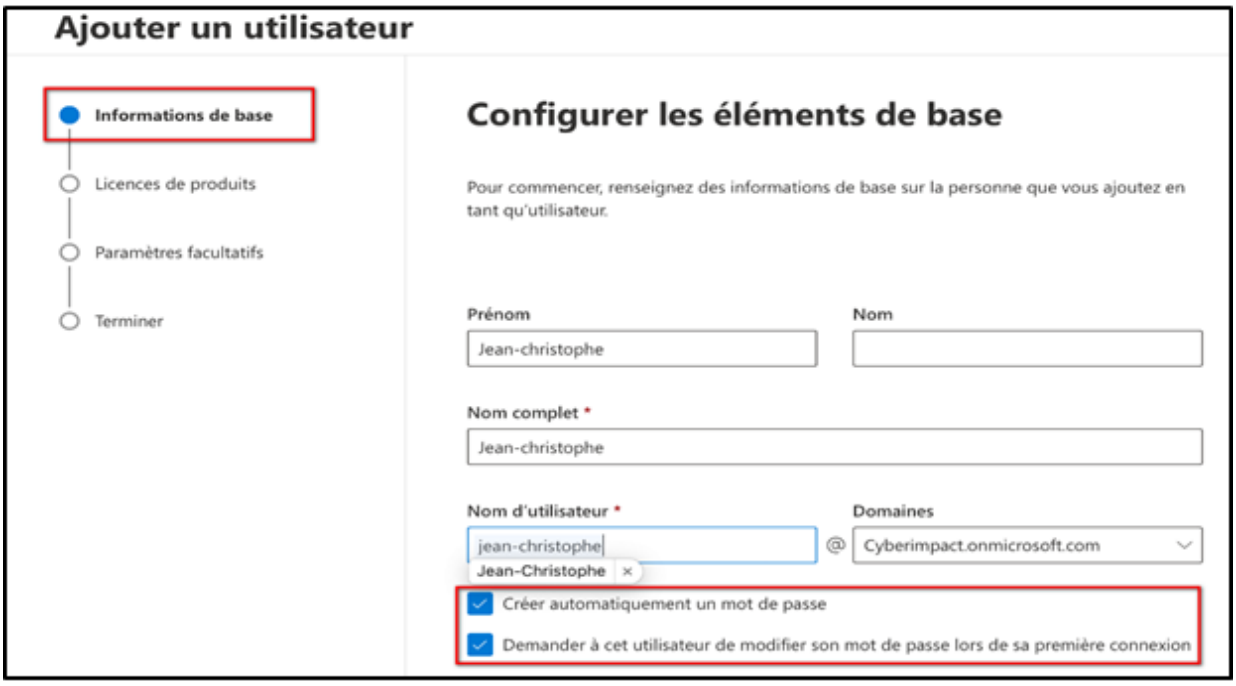


a) Configuration d'un utilisateur et de sa licence

Pour créer un utilisateur, il faut se rendre dans « **Utilisateurs** », « **Utilisateurs actifs** » puis cliquer sur « **ajouter un utilisateur** » :

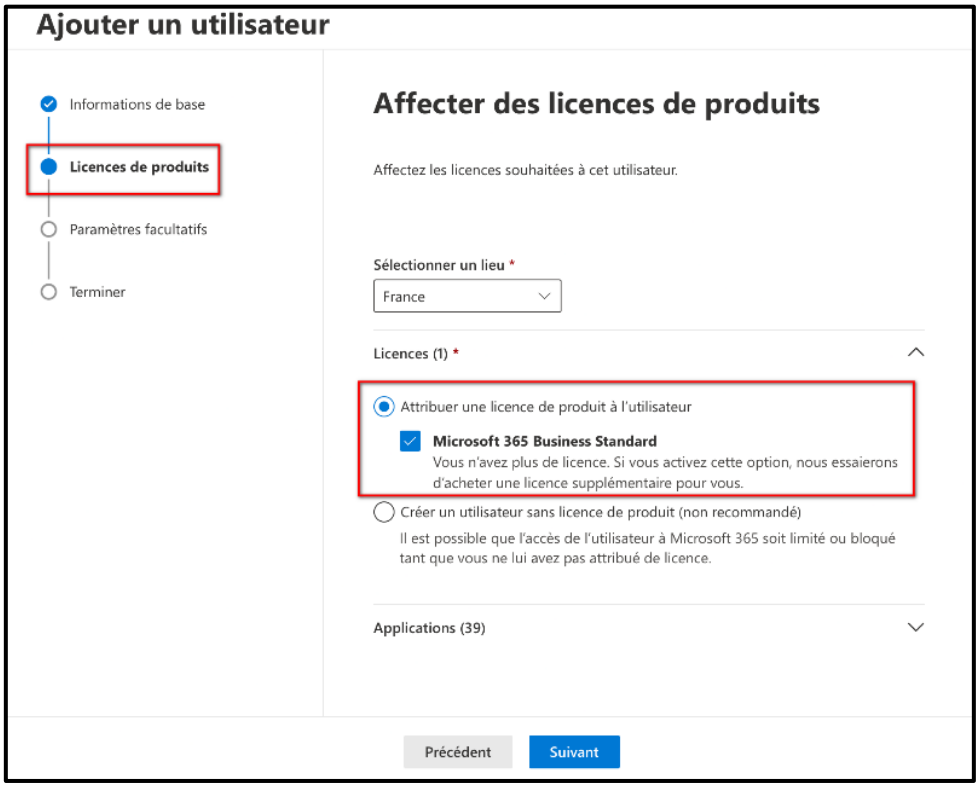


A présent, il faut rentrer les informations de base pour la création de l'utilisateur : Remplir les champs requis et cocher la création automatique d'un mot de passe et demander à l'utilisateur de modifier son mot de passe lors de sa première connexion.



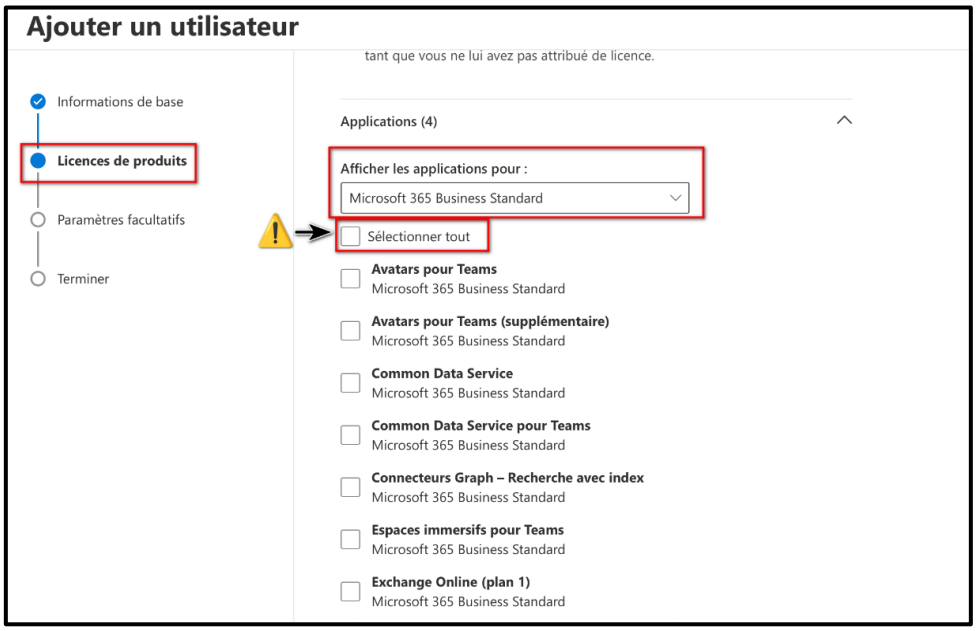
Ensuite, vient l'étape de **l'affectation de la licence**. En effet, il est utile de créer une licence pour l'utilisateur afin qu'il puisse avoir accès à des fonctionnalités sans en être limités : avoir accès aux applications en lignes des applications Office, accéder au Cloud, participer à des réunions Teams, ...

Ici, il est demandé d'affecter une licence à cet utilisateur qui est en train d'être créé. La licence sélectionnée est **Microsoft 365 Business Standard.**

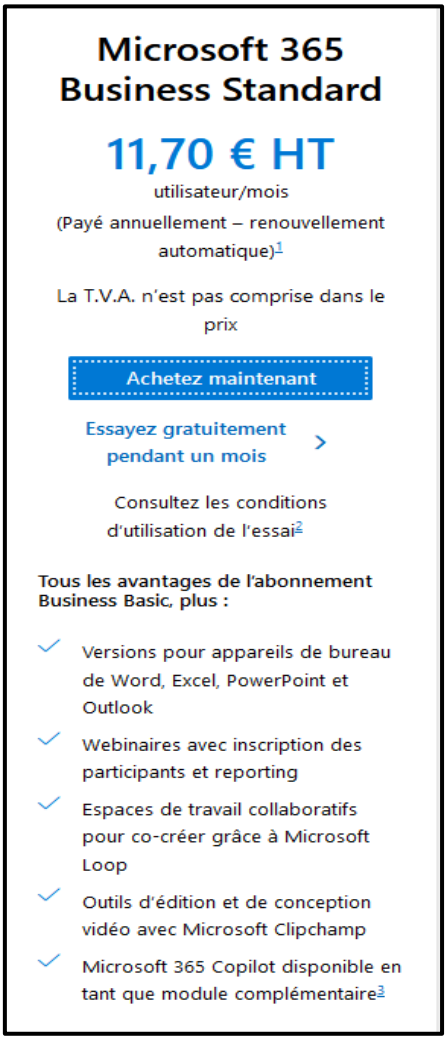


Par défaut, il est sélectionné toutes les options pour la licence donc il faut bien penser à **décocher « sélectionner tout »** ou décocher chaque case pour éviter d'avoir des produits inutiles dans le pack.

Mettre **Microsoft standard** pour une utilisation standard, cela peut changer et devenir du cas par cas pour chaque utilisateur.



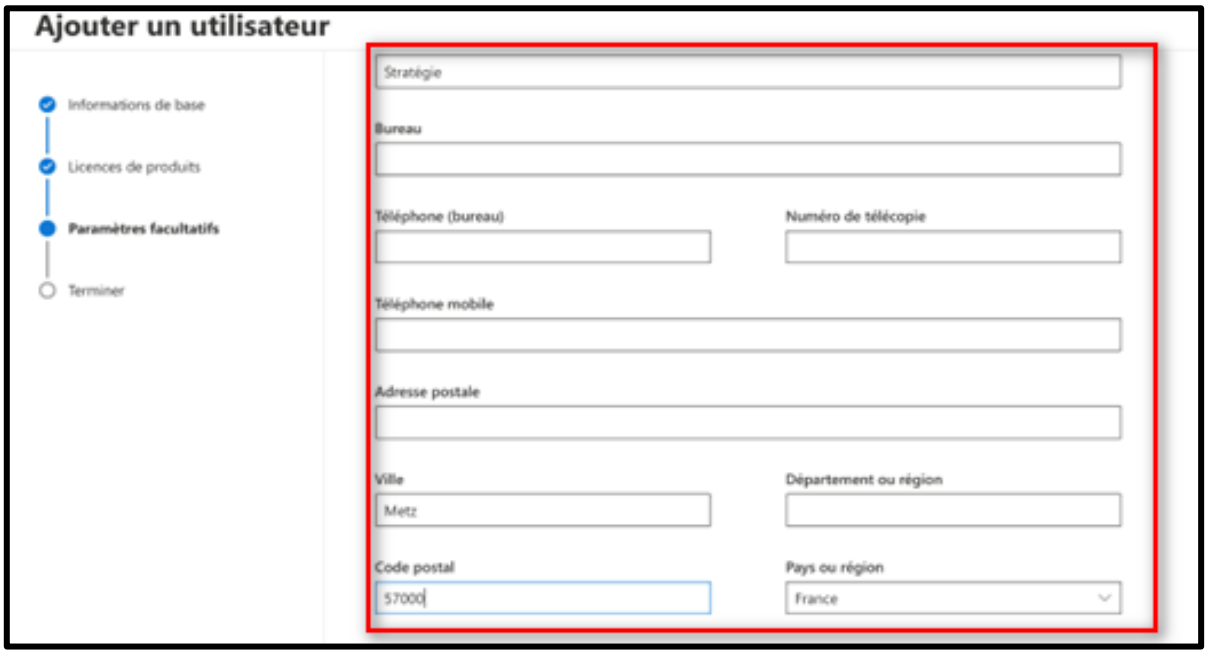
La licence Microsoft 365 Business Standard comprend :



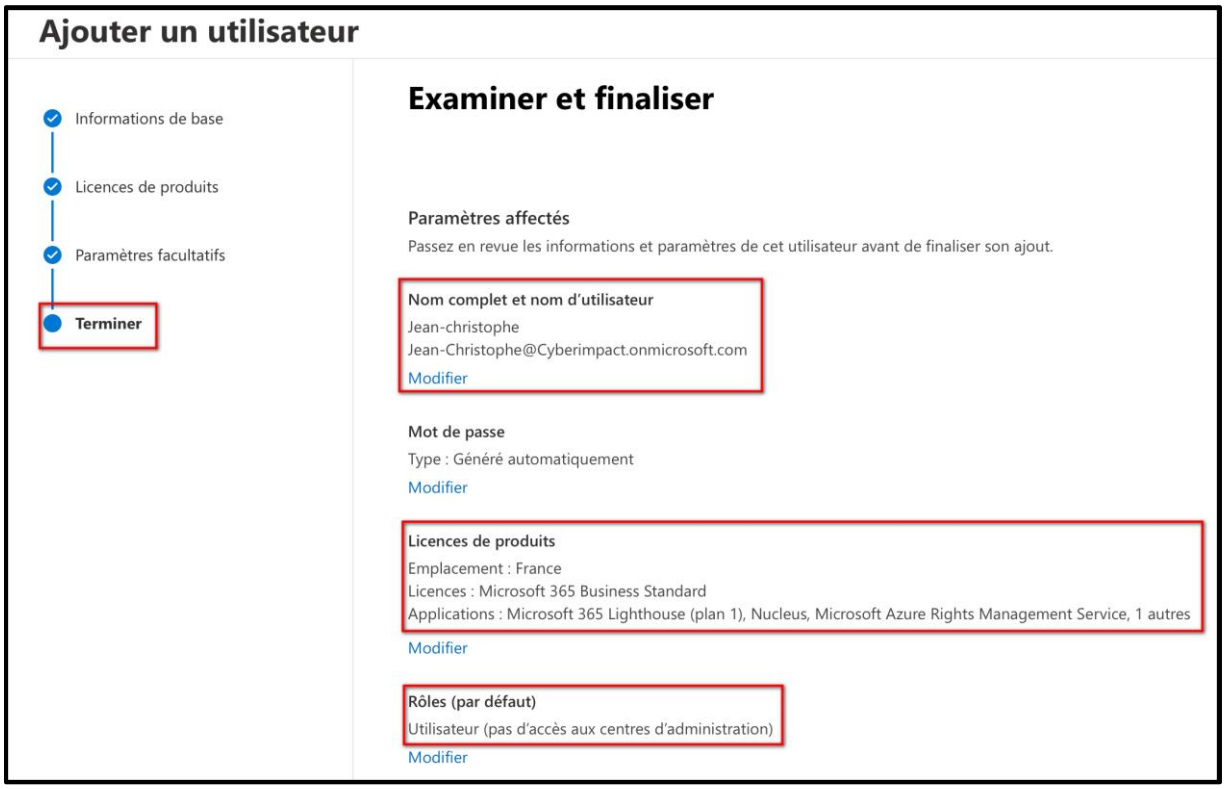
Licence Microsoft Office 365 Business Standard comprenant les applications ainsi que les différentes otpions possibles

Un message apparaîtra ensuite pour récapituler l'achat effectué (licence Microsoft 365 Business Standard ici) et proposer l'achat d'une autre licence. La licence achetée sera attribuée à l'utilisateur en train d'être créée.

Pour la suite de la configuration de l'utilisateur, il est possible de rentrer des informations facultatives :

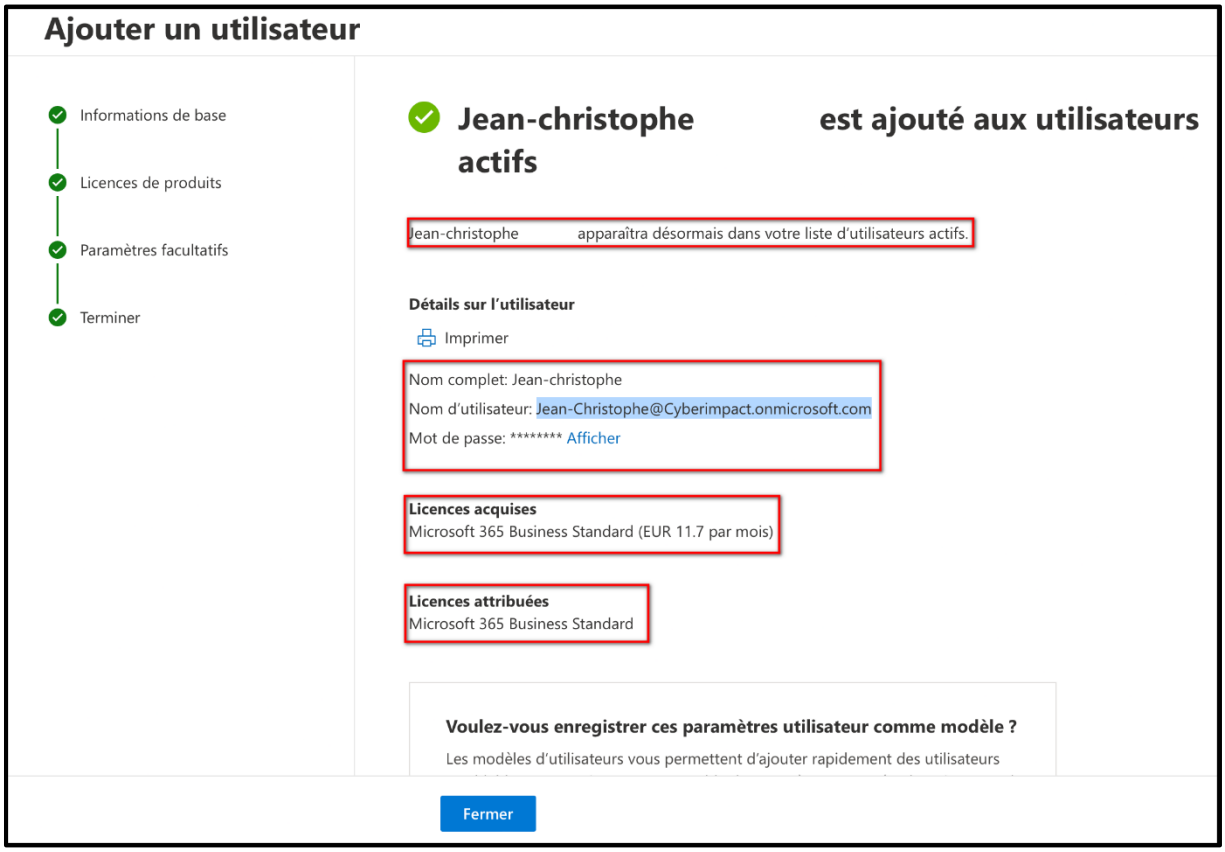


Pour finaliser l'ajout de notre utilisateur, un résumé nous est indiqué détaillant le nom d'utilisateur, l'adresse utilisée, la licence adoptée ainsi que les applications allant avec et le rôle qui lui a été désigné :



Une fois que tous les paramètres et informations ont été confirmés, l'utilisateur est ajouté aux utilisateurs actifs :

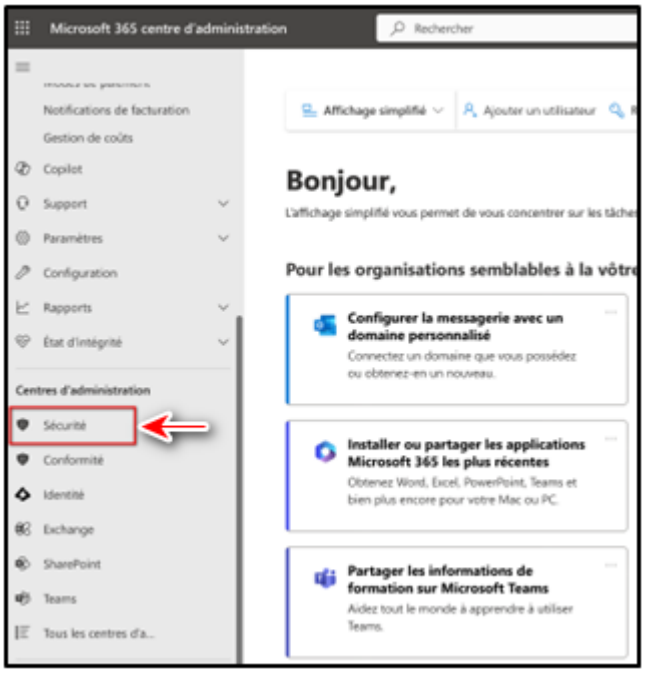
Il y apparait la licence attribuée et les détails sur l'utilisateur.



Un exemple de liste des utilisateurs crée pour les utilisateurs actifs avec la licence attribuée :

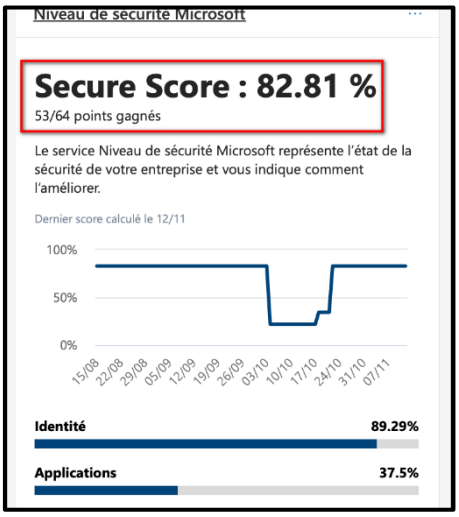
III- Onglet sécurité

L'onglet sécurité dans Office 365 permet de gérer entre autres les utilisateurs (leur accès, l'authentification, ...) mais aussi la possibilité de réaliser des rapports ainsi que des surveillances et enfin de pouvoir visualiser si les utilisateurs respectent les politiques de sécurité.
Cet onglet se trouve dans le « **centre d'administration** », « **Sécurité** » :



Evaluer la posture de sécurité avec Microsoft Secure Score :

Microsoft Secure Score permet de mesurer la posture de sécurité d'une organisation, en ayant un score élevé, cela indique une posture de sécurité forte : de nombreuses mesures de sécurité sont mises en place, l'entreprise suit les recommandations de sécurités recommandées par Microsoft, réduction des risques d'attaques et un investissement de la part de l'entreprise à maintenir sa sécurité.



On a un Secure score de 53/64 points gagnés pour un paramétrage par défaut.

On attribue un pourcentage sur 100 indiquant le niveau de sécurité de l'entreprise sur les configurations et la sécurité mise en place.

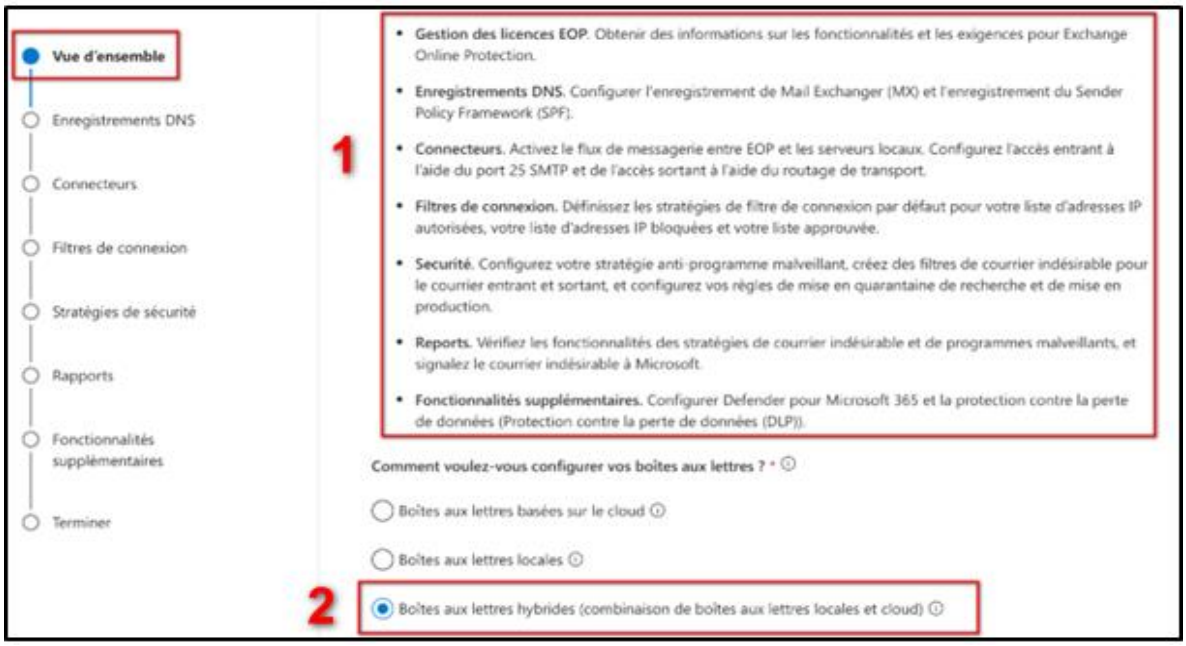
a) Configuration de la messagerie : synchronisation des mails avec Office 365

La synchronisation des mails permet de consulter des mails sur plusieurs appareils, les données sont protégées et sauvegardées dans le cloud ce qui permet le partage de mails et d'avoir une synchronisation en temps réel des mails/tâches.

- Pour cela, il faut se rendre dans le « **Centre d'administration** » puis dans « **Configuration de la messagerie** ». Il est décrit ici les différentes étapes pour configurer Exchange Online Protection avec les options présentes en dessous (1) :
- Sélectionner l'option pour **configurer les boites aux lettres en hybrides** (2).

Les boites hybrides sont la combinaison de messagerie locale et celle du cloud. Cela permet de pouvoir accéder à l'une des deux messageries et une facilité lors d'une migration.

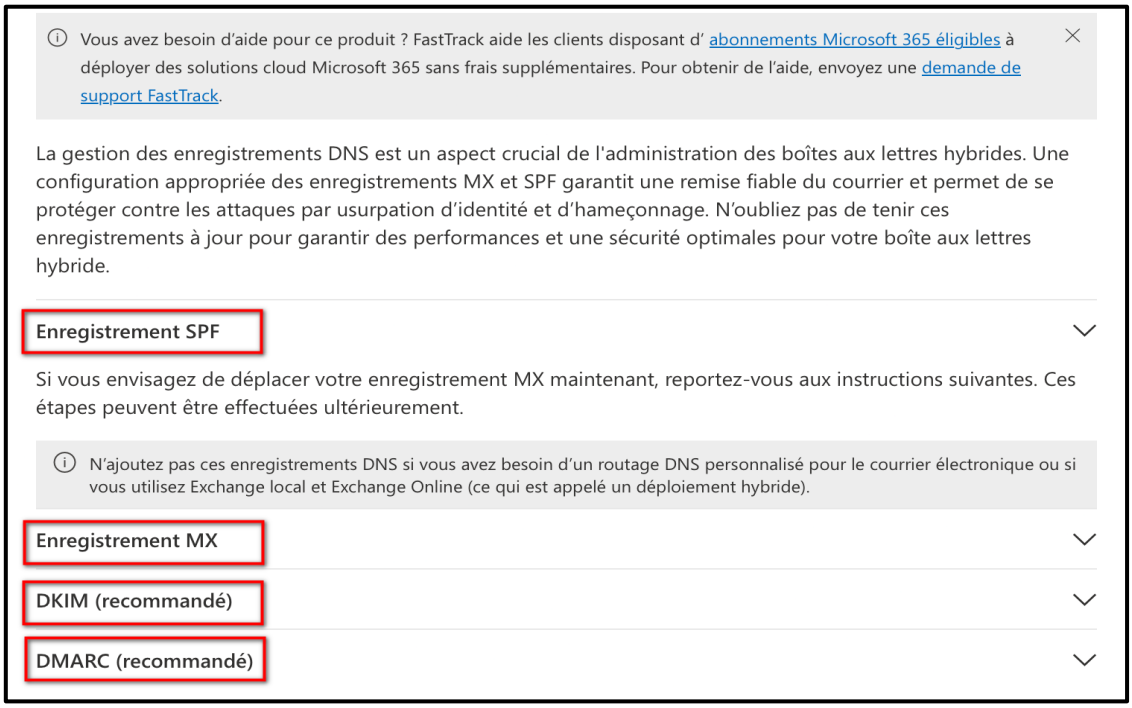
Pour la configuration de boites hybrides il faut au préalable disposer d'une licence. Chaque boîte aux lettres dans le cloud doit avoir une licence.



b) Configuration DNS externes pour les boites hybrides dans Office 365

Beaucoup d'entreprises migrent leur infrastructure entièrement ou partiellement vers le cloud. Au cours de cette migration, il est nécessaire d'intégrer des solutions DNS pour garantir la sécurité et la performance de ce contexte hybride.

DMARC, **DKIM** et **SPF** sont 3 méthodes d'authentification de courrier électronique. DMARC indique aux serveurs de messagerie ce qu'ils doivent faire en cas d'échec de DKIM/ SPF.



- Comment fonctionne SFP :

Sender Policy Framework est un moyen pour un domaine de répertorier tous les serveurs à partir desquels il envoie des mails. Il permet d'empêcher d'autres personnes d'utiliser le domaine pour envoyer du courrier indésirable voir malveillant.

- Comment fonctionne DKIM :

DomainKeys Identified Mail permet aux propriétaires de domaines de signer automatiquement des mails provenant de leur domaine. La signature est une signature numérique qui utilise la cryptographie pour vérifier que le mail vient du domaine.

- Comment fonctionne DMARC :

Domaine Based Message Authentification Reporting and Conformance (DMARC) indique au serveur de messagerie récepteur ce qu'il doit faire en fonction des résultats de la vérification de SPF et DKIM. Ainsi la politique DMARC peut demander aux serveurs

de messagerie de mettre en quarantaine des mails, de les rejeter ou de les distribuer pour ceux qui ne répondent pas aux critères SPF et DKIM.

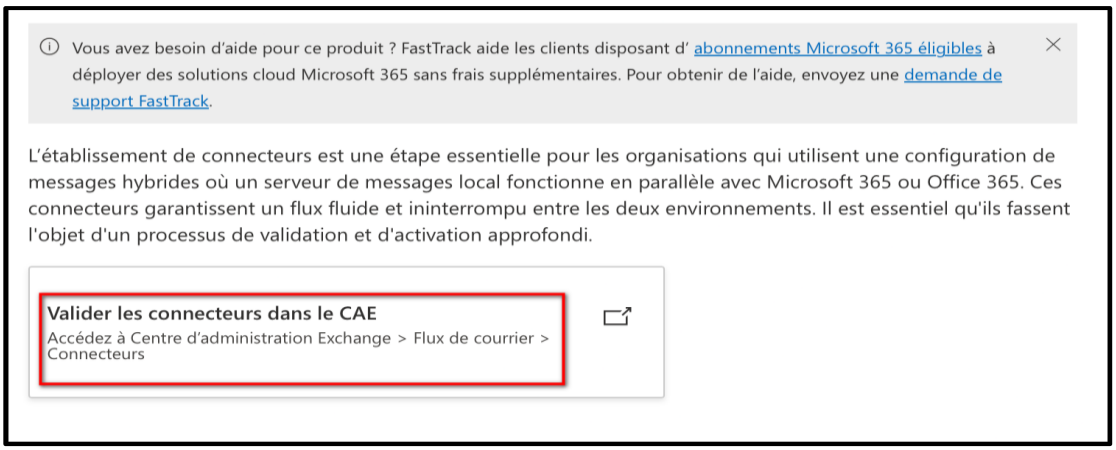
➢ Comment fonctionne MX :

Mail Exchange (MX) indique aux serveurs de courrier, les serveurs de messagerie autorisés à recevoir des mails pour un domaine.

Grâce à la configuration de ces enregistrements DNS cela permet l'intégrité des communications des mails dans Microsoft 365.

c) Validation des connecteurs dans Exchange

Il existe la possibilité de configurer des connecteurs Exchange et cela fait partie du processus de déploiement des solutions cloud. Ils servent à intégrer et à synchroniser des communications entre les entreprises et les services Microsoft. Les connecteurs Microsoft 365 s'administrent dans le Centre d'Administration Exchange (CAE). C'est ici que les administrateurs vont pouvoir gérer et valider la configuration de connecteurs Microsoft :

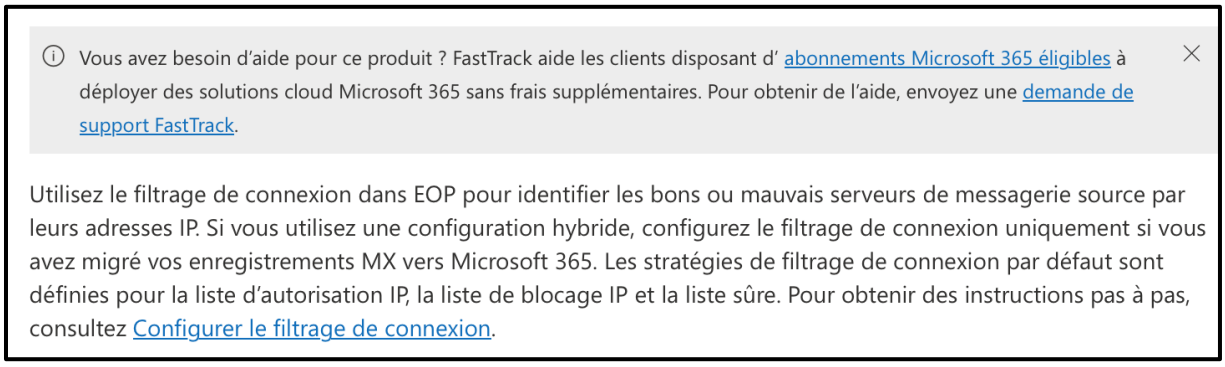


Mise en place de connecteurs via Flux de courrier > Connecteurs

d) Filtrage des connexions

Le filtrage de connexions dans Exchange Online Protection (EOP) permet d'identifier les bons et/ou les mauvais serveurs de messagerie par leurs adresses IP. Les principaux composants de la stratégie de filtrage des connexions par défaut sont les suivants :

- Liste d'adresses IP autorisées : Tous les messages entrants sont analysés à la recherche de programmes malveillants et d'hameçonnage à haut niveau de confiance.
- Liste d'adresses IP bloquées : bloque tous les messages entrants provenant des adresses IP sources ou des plages d'adresses IP spécifiées.
- Liste sécurisée : Microsoft identifie ces sources de messagerie approuvées à partir d'abonnements à diverses listes.

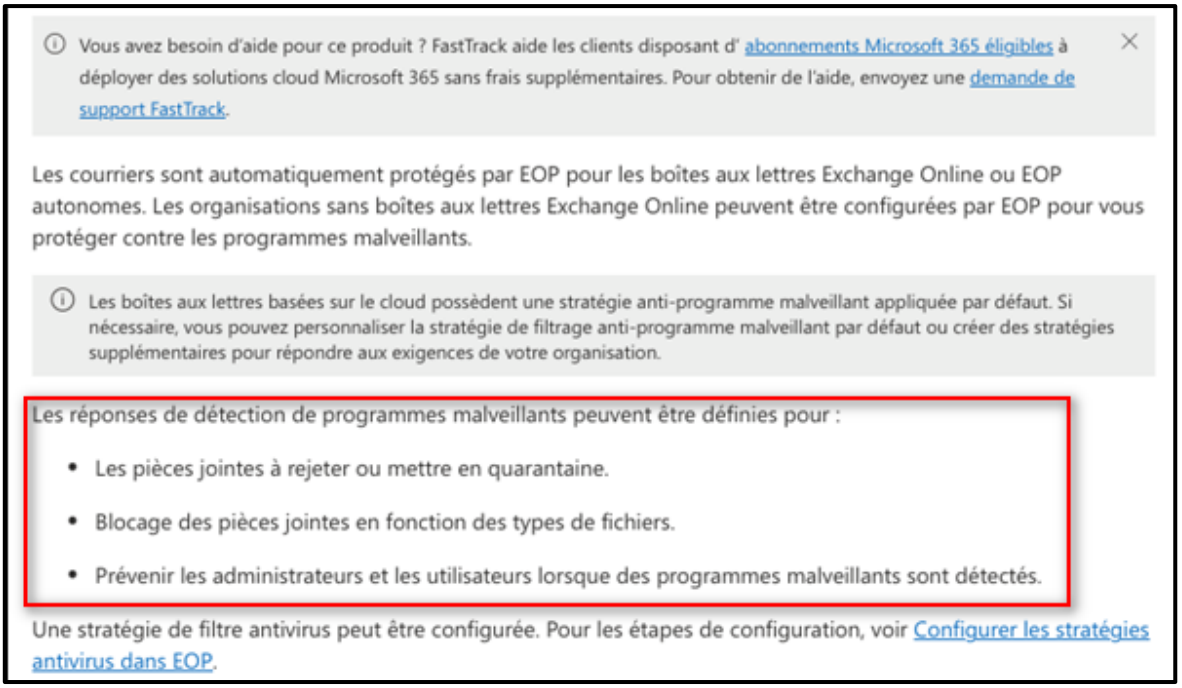


e) Stratégie anti-programme malveillant

La configuration d'une stratégie anti-programme malveillant permet à ce que les courriers soient protégés automatiquement par Exchange Online Protection (EOP). La détection de programmes malveillants mise en place est la suivante :

- Les pièces jointes sont mises en quarantaine
- Blocage de pièces jointes en fonction du type de fichiers
- La détection prévient les administrateurs/ utilisateurs lorsqu'un programme malveillant est détecté

Les boites mail sur le cloud possède déjà une stratégie anti-programme malveillant mails, il est possible de personnaliser cette stratégie ou d'en créer d'autres.



Voici comment se déroule lorsqu'un message entre avec l'EOP :

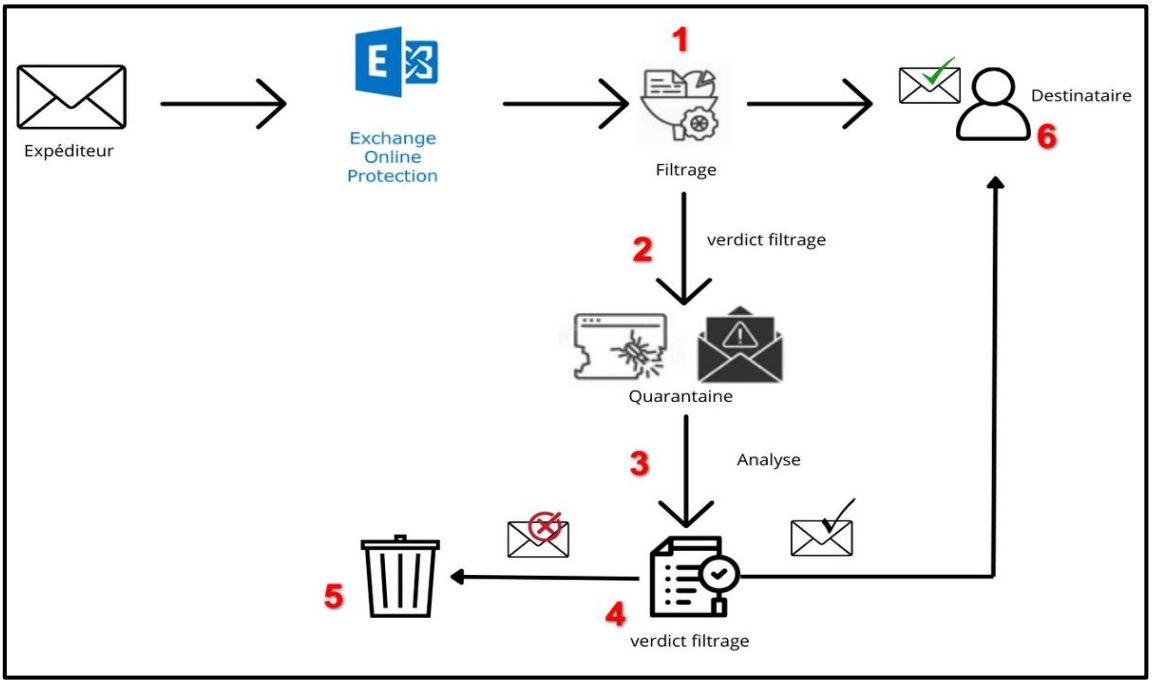


Schéma du déroulement d'un message quand il entre dans l'EOP

1) Le message entrant passe le filtrage de connexion et vérifie l'expéditeur.
2) Si des programmes malveillants sont détectés, ils sont mis en quarantaine.
3) Ils sont ensuite analysés puis évaluer par rapport aux règles de flux de courrier créés auparavant par les administrateurs. Ils passent aussi par le filtrage de contenu (courriers indésirables, hameçonnage, usurpation, ...).
4) Un verdict de filtrage est réalisé : soit le message est replacé en quarantaine ou supprimer (5) soit le message traverse l'ensemble des protections sans menace et est remis au destinataire (6).

IV- Reporting et rapports

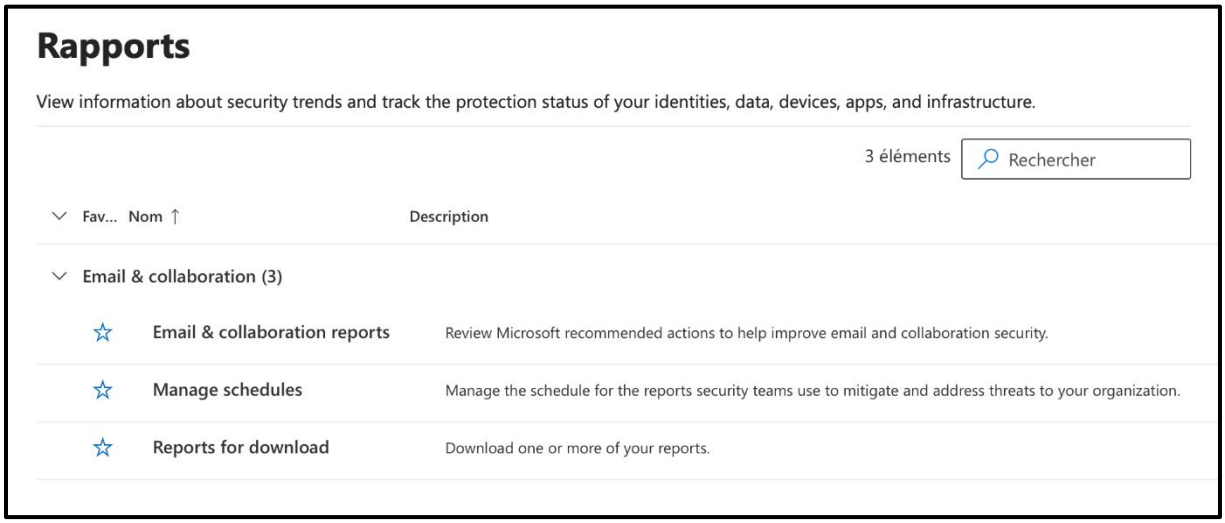
Le portail Microsoft Defender permet de visualiser l'état de l'entreprise grâce à différents rapports. Ils permettent la remontée de menaces détectées, rapport de licence, rapport de sécurité, rapport de protection de menaces, rapport d'intégrité des appareils, inventaire des appareils, protection web, pare-feu, ... Avec par exemple, Microsoft Secure Score comme vu juste avant, qui donne une indication sur l'état au niveau de la sécurité de l'entreprise.

Types de rapports disponibles sous Microsoft Defender pour Office 365 (vu en cours) :

Il est possible de visualiser un tableau de bord « Rapports » dans le **centre d'administration Office 365** en tant qu'administrateur ou un avec un profil équivalent (niveau droit). Il permet d'obtenir des informations précises sur l'utilisation d'un service (données, appareils, application, infrastructure, ...). Par exemple, la quantité de mails qui circulent dans l'entreprise. Ici, il est possible de visualiser les rapports de sécurité de mails **: Email & collaboration reports**. On y retrouve ce type de rapports :

- Protection des URL
- Sur l'état de la protection contre les menaces
- Programmes malveillants détectés dans le rapport par mail
- Courrier indésirable

On peut gérer aussi le calendrier des rapports que les équipes de sécurité utilisent pour traiter les menaces de l'entreprise. Et enfin, la possibilité de télécharger les différents rapports.



V- Conclusion

Ce rapport met en évidence les étapes clé pour gérer et sécuriser un environnement Office 365. L'onglet sécurité a montré l'importance de mettre en place ces stratégies afin de sécuriser les données et de les protéger : paramètres DNS, connecteurs Exchanges, définir des règles pour des connexions plus sécurisés, ... Dernier point abordé, le reporting permettant de suivre, d'analyser et d'améliorer au niveau de la sécurité, les données et équipements de l'entreprise.

Sources :

Microsoft Learn

Forum