

OFFICE 365

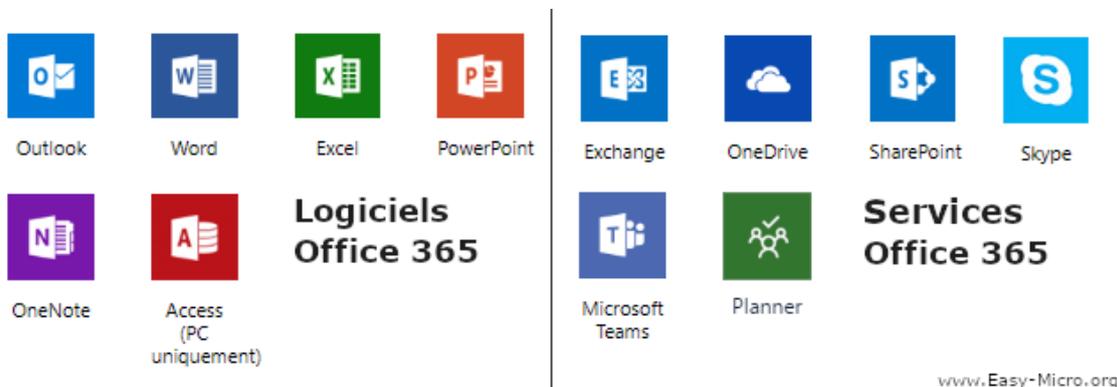


Intégration/ Administration



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.

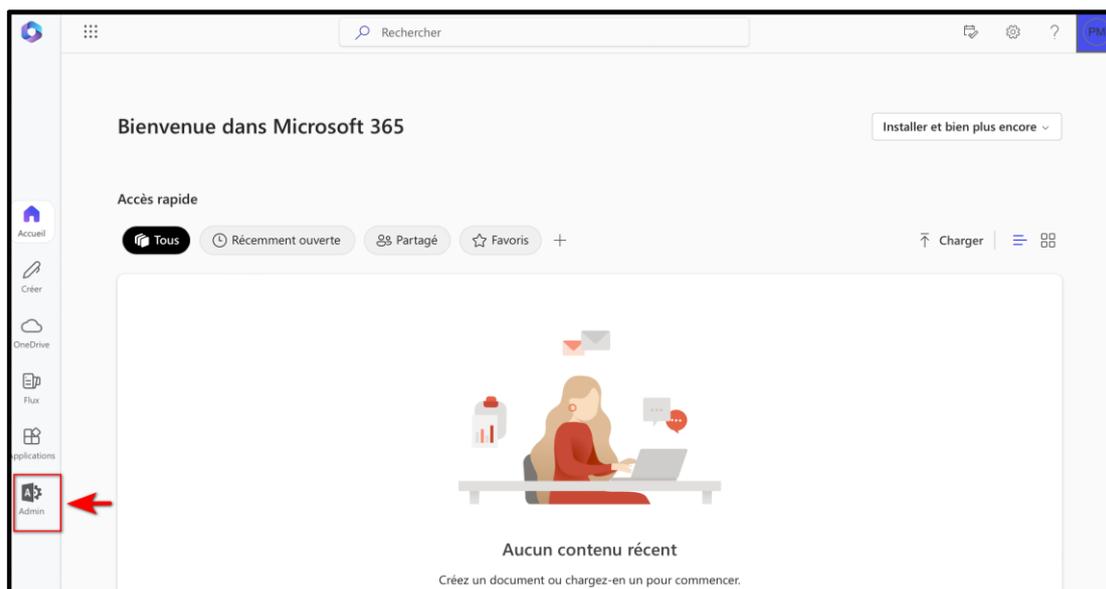
Table des matières

I-	Accès au centre d'administration.....	4
II-	Le centre d'administration.....	4
	A) Configuration d'un utilisateur et de sa licence	
III-	Onglet sécurité	100
	A) Configuration de la messagerie : synchronisation des mails avec Office 365	
	B) Configuration DNS externes pour les boites hybrides dans Office 365	
	C) Validation des connecteurs dans Exchange	
	D) Filtrage des connexions	
	E) Stratégie anti-programme malveillant	
IV-	Reporting et rapports	155
V-	Conclusion.....	177

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.

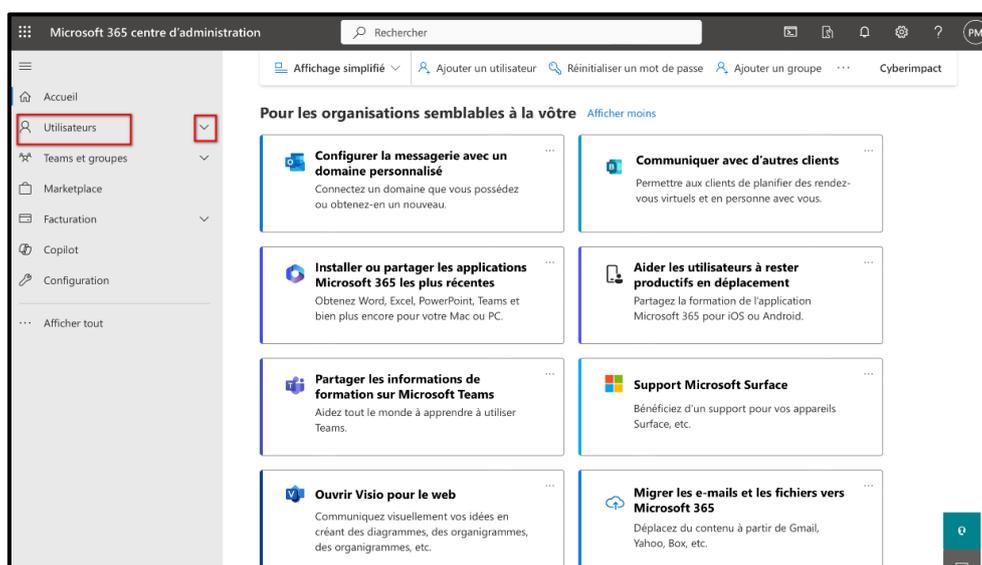
Voici la page d'accueil Office 365 : Cliquer sur « **admin** » en bas à gauche pour accéder au **centre d'administration**.



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** » :

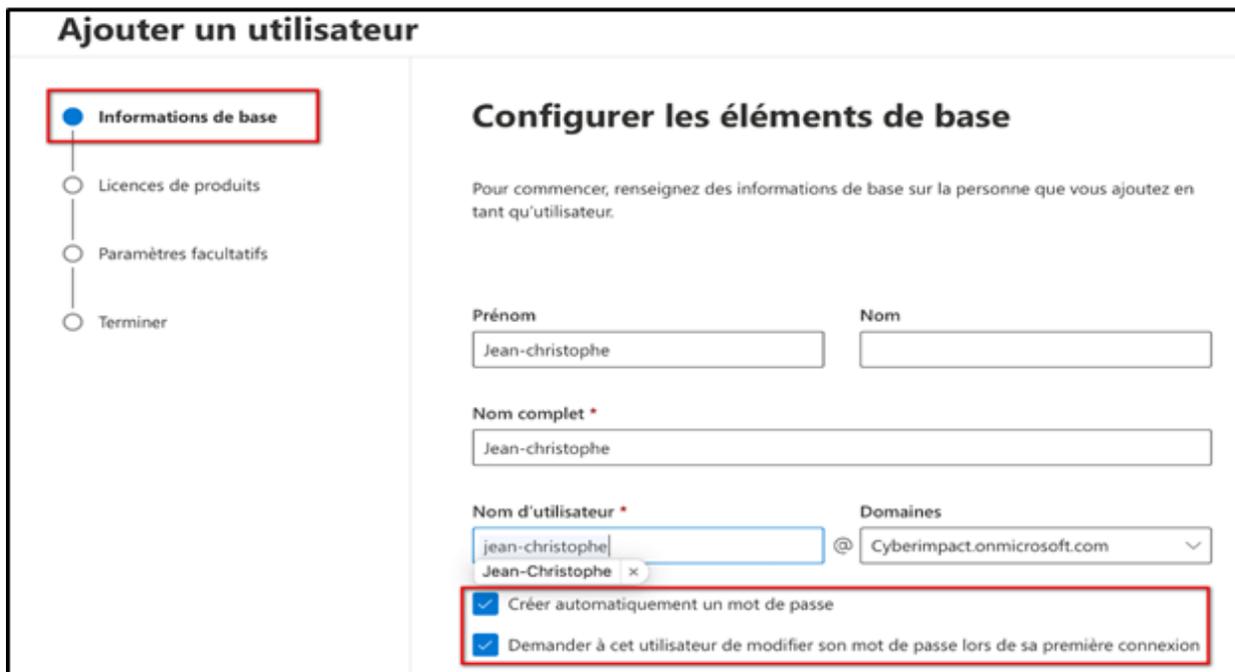


a) Configuration d'un utilisateur et de sa licence

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**.

The screenshot shows the 'Ajouter un utilisateur' (Add user) wizard. The 'Licences de produits' (Product licenses) step is selected and highlighted with a red box. The 'Affecter des licences de produits' (Assign product licenses) section is active. It shows a dropdown for 'Sélectionner un lieu' (Select a location) set to 'France'. Below, the 'Licences (1)' section shows one license selected: 'Microsoft 365 Business Standard', which is also highlighted with a red box. The other option, 'Créer un utilisateur sans licence de produit (non recommandé)', is unselected. At the bottom, there are 'Précédent' (Previous) and 'Suivant' (Next) buttons.

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.

This screenshot shows the 'Ajouter un utilisateur' (Add user) wizard, 'Licences de produits' (Product licenses) step. The 'Applications (4)' section is visible, showing a dropdown menu for 'Afficher les applications pour' (Show applications for) set to 'Microsoft 365 Business Standard'. Below this, the 'Sélectionner tout' (Select all) checkbox is highlighted with a red box and a yellow warning icon with an arrow pointing to it. A list of applications is shown, each with an unchecked checkbox: 'Avatars pour Teams', 'Avatars pour Teams (supplémentaire)', 'Common Data Service', 'Common Data Service pour Teams', 'Connecteurs Graph – Recherche avec index', 'Espaces immersifs pour Teams', and 'Exchange Online (plan 1)'. The 'Licences de produits' step is also highlighted with a red box.

La licence Microsoft 365 Business Standard comprend :

**Microsoft 365
Business Standard**

11,70 € HT
utilisateur/mois

(Payé annuellement – renouvellement automatique)¹

La T.V.A. n'est pas comprise dans le prix

Achetez maintenant

Essayez gratuitement pendant un mois >

Consultez les conditions d'utilisation de l'essai²

Tous les avantages de l'abonnement Business Basic, plus :

- ✓ Versions pour appareils de bureau de Word, Excel, PowerPoint et Outlook
- ✓ Webinaires avec inscription des participants et reporting
- ✓ Espaces de travail collaboratifs pour co-créeer grâce à Microsoft Loop
- ✓ Outils d'édition et de conception vidéo avec Microsoft Clipchamp
- ✓ Microsoft 365 Copilot disponible en tant que module complémentaire³

Microsoft 365

Microsoft 365 Business Premium

Exchange Teams OneDrive SharePoint Outlook

Word Excel PowerPoint Publisher Access

Intune Azure Information Protection Defender Conditional Access Windows Virtual Desktop

Licence Microsoft Office 365 Business Standard comprenant les applications ainsi que les différentes options 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.

Voulez-vous acheter une autre licence ?

Microsoft 365 Business Standard (EUR 11.7 par mois)

Gérez vos abonnements via Facturation > Vos produits.

Oui Annuler

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

The screenshot shows the 'Ajouter un utilisateur' form with the 'Paramètres facultatifs' step selected. The form fields are as follows:

- Stratégie: [Text input]
- Bureau: [Text input]
- Téléphone (bureau): [Text input]
- Numéro de télécopie: [Text input]
- Téléphone mobile: [Text input]
- Adresse postale: [Text input]
- Ville: Metz [Text input]
- Département ou région: [Text input]
- Code postal: 57000 [Text input]
- Pays ou région: France [Dropdown menu]

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 :

The screenshot shows the 'Ajouter un utilisateur' form with the 'Terminer' step selected. The summary section is titled 'Examiner et finaliser' and contains the following information:

- Paramètres affectés**
Passez en revue les informations et paramètres de cet utilisateur avant de finaliser son ajout.
- Nom complet et nom d'utilisateur**
Jean-christophe
Jean-Christophe@Cyberimpact.onmicrosoft.com
[Modifier](#)
- Mot de passe**
Type : Généré automatiquement
[Modifier](#)
- Licences de produits**
Emplacement : France
Licences : Microsoft 365 Business Standard
Applications : Microsoft 365 Lighthouse (plan 1), Nucleus, Microsoft Azure Rights Management Service, 1 autres
[Modifier](#)
- Rôles (par défaut)**
Utilisateur (pas d'accès aux centres d'administration)
[Modifier](#)

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.

Ajouter un utilisateur

- Informations de base
- Licences de produits
- Paramètres facultatifs
- Terminer

✓ Jean-christophe est ajouté aux utilisateurs actifs

jean-christophe apparaîtra désormais dans votre liste d'utilisateurs actifs.

Détails sur l'utilisateur

[Imprimer](#)

Nom complet: Jean-christophe
 Nom d'utilisateur: Jean-Christophe@Cyberimpact.onmicrosoft.com
 Mot de passe: ***** [Afficher](#)

Licences acquises
 Microsoft 365 Business Standard (EUR 11.7 par mois)

Licences attribuées
 Microsoft 365 Business Standard

Voulez-vous enregistrer ces paramètres utilisateur comme modèle ?
 Les modèles d'utilisateurs vous permettent d'ajouter rapidement des utilisateurs

[Fermer](#)

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

Utilisateurs actifs

[Autres actions](#)

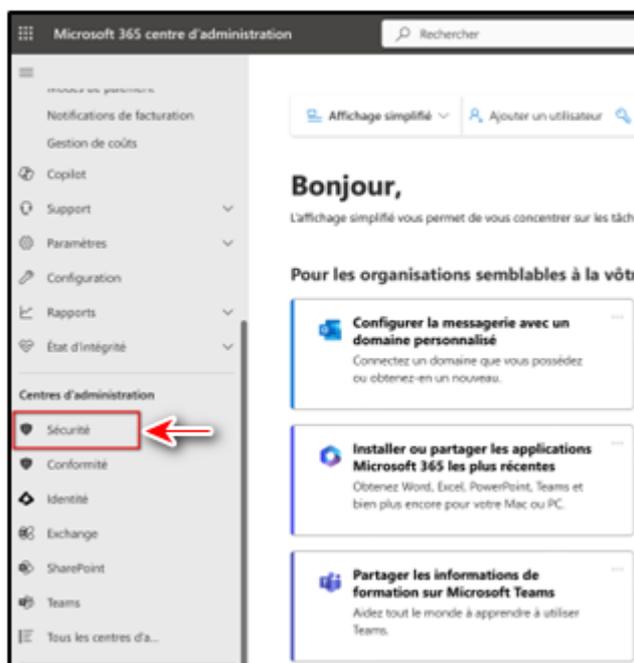
[Ajouter un utilisateur](#) [Modèles utilisateur](#) [Ajouter plusieurs utilisateurs](#)

<input type="checkbox"/>	Nom d'affichage ↑	Nom d'utilisateur	Licences
<input type="checkbox"/>	Jean-christophe	Jean-Christophe@Cyberimpact.onmicrosoft.com	Microsoft 365 Business Standard
<input type="checkbox"/>	Philippe	Philippe @Cyberimpact.onmicrosoft.com	Microsoft 365 Business Standard

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 boîtes aux lettres en hybrides** (2).

Les boîtes 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 boîtes hybrides il faut au préalable disposer d'une licence. Chaque boîte aux lettres dans le cloud doit avoir une licence.

1

- **Gestion des licences EOP.** Obtenir des informations sur les fonctionnalités et les exigences pour Exchange Online Protection.
- **Enregistrements DNS.** Configurer l'enregistrement de Mail Exchanger (MX) et l'enregistrement du Sender Policy Framework (SPF).
- **Connecteurs.** Activez le flux de messagerie entre EOP et les serveurs locaux. Configurez l'accès entrant à l'aide du port 25 SMTP et de l'accès sortant à l'aide du routage de transport.
- **Filtres de connexion.** Définissez les stratégies de filtre de connexion par défaut pour votre liste d'adresses IP autorisées, votre liste d'adresses IP bloquées et votre liste approuvée.
- **Sécurité.** Configurez votre stratégie anti-programme malveillant, créez des filtres de courrier indésirable pour le courrier entrant et sortant, et configurez vos règles de mise en quarantaine de recherche et de mise en production.
- **Reports.** Vérifiez les fonctionnalités des stratégies de courrier indésirable et de programmes malveillants, et signalez le courrier indésirable à Microsoft.
- **Fonctionnalités supplémentaires.** Configurer Defender pour Microsoft 365 et la protection contre la perte de données (DLP).

Comment voulez-vous configurer vos boîtes aux lettres ? *

- Boîtes aux lettres basées sur le cloud
- Boîtes aux lettres locales
- Boîtes aux lettres hybrides (combinaison de boîtes aux lettres locales et cloud)**

2

b) Configuration DNS externes pour les boîtes 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.

The screenshot shows a help article titled "La gestion des enregistrements DNS est un aspect crucial de l'administration des boîtes aux lettres hybrides. Une configuration appropriée des enregistrements MX et SPF garantit une remise fiable du courrier et permet de se protéger contre les attaques par usurpation d'identité et d'hameçonnage. N'oubliez pas de tenir ces enregistrements à jour pour garantir des performances et une sécurité optimales pour votre boîte aux lettres hybride." Below the text is a list of DNS records with expandable sections:

- Enregistrement SPF** (expanded): Si vous envisagez de déplacer votre enregistrement MX maintenant, reportez-vous aux instructions suivantes. Ces étapes peuvent être effectuées ultérieurement.
- Enregistrement MX** (collapsed)
- DKIM (recommandé)** (collapsed)
- DMARC (recommandé)** (collapsed)

At the top of the screenshot, there is a help message: "Vous avez besoin d'aide pour ce produit ? FastTrack aide les clients disposant d'abonnements Microsoft 365 éligibles à déployer des solutions cloud Microsoft 365 sans frais supplémentaires. Pour obtenir de l'aide, envoyez une demande de support FastTrack."

➤ 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 Authentication 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.

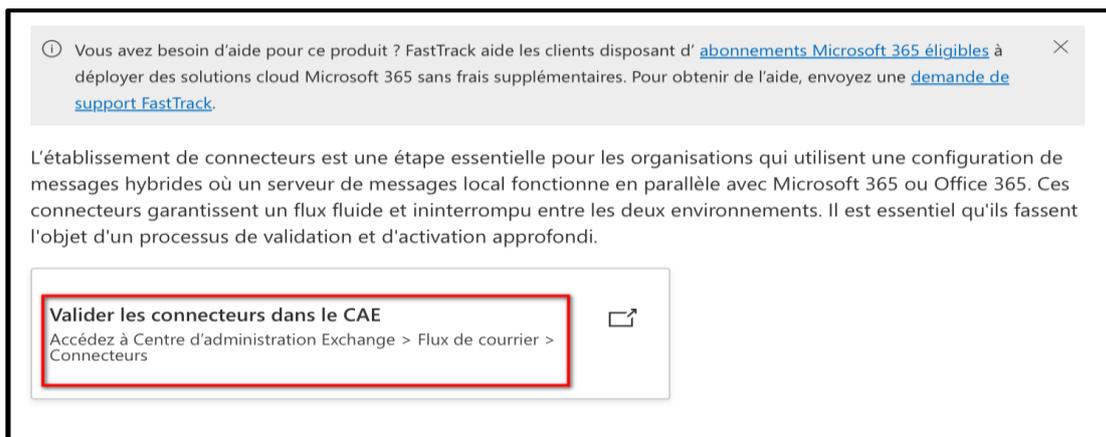
➤ Comment fonctionne MX :

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.

① Vous avez besoin d'aide pour ce produit ? FastTrack aide les clients disposant d' [abonnements Microsoft 365 éligibles](#) à déployer des solutions cloud Microsoft 365 sans frais supplémentaires. Pour obtenir de l'aide, envoyez une [demande de support FastTrack](#). ✕

Utilisez le filtrage de connexion dans EOP pour identifier les bons ou mauvais serveurs de messagerie source par leurs adresses IP. Si vous utilisez une configuration hybride, configurez le filtrage de connexion uniquement si vous avez migré vos enregistrements MX vers Microsoft 365. Les stratégies de filtrage de connexion par défaut sont définies pour la liste d'autorisation IP, la liste de blocage IP et la liste sûre. Pour obtenir des instructions pas à pas, consultez [Configurer le filtrage de connexion](#).

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 boîtes 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.

① Vous avez besoin d'aide pour ce produit ? FastTrack aide les clients disposant d' [abonnements Microsoft 365 éligibles](#) à déployer des solutions cloud Microsoft 365 sans frais supplémentaires. Pour obtenir de l'aide, envoyez une [demande de support FastTrack](#). ✕

Les courriers sont automatiquement protégés par EOP pour les boîtes aux lettres Exchange Online ou EOP autonomes. Les organisations sans boîtes aux lettres Exchange Online peuvent être configurées par EOP pour vous protéger contre les programmes malveillants.

① Les boîtes aux lettres basées sur le cloud possèdent une stratégie anti-programme malveillant appliquée par défaut. Si nécessaire, vous pouvez personnaliser la stratégie de filtrage anti-programme malveillant par défaut ou créer des stratégies supplémentaires pour répondre aux exigences de votre organisation.

Les réponses de détection de programmes malveillants peuvent être définies pour :

- Les pièces jointes à rejeter ou mettre en quarantaine.
- Blocage des pièces jointes en fonction des types de fichiers.
- Prévenir les administrateurs et les utilisateurs lorsque des programmes malveillants sont détectés.

Une stratégie de filtre antivirus peut être configurée. Pour les étapes de configuration, voir [Configurer les stratégies antivirus dans EOP](#).

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

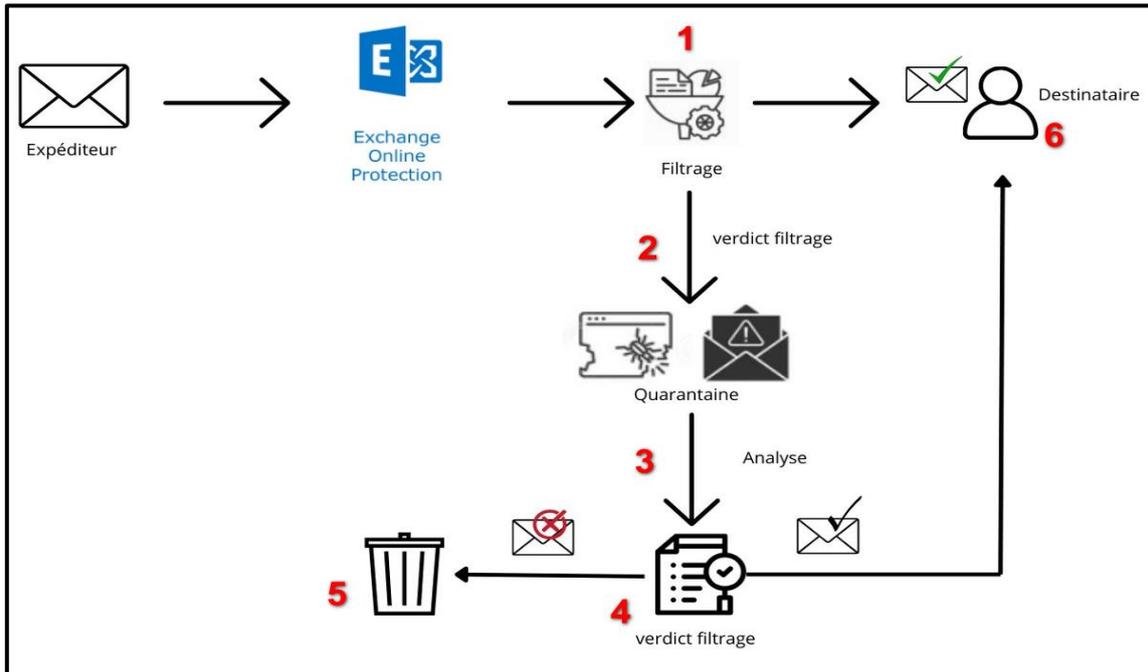


Schéma du déroulement d'un message quand il entre dans l'EOP

- 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 évalués 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 supprimé (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.

Stratégies de surveillance et création de rapports dans EOP

① Vous avez besoin d'aide pour ce produit ? FastTrack aide les clients disposant d' [abonnements Microsoft 365 éligibles](#) à déployer des solutions cloud Microsoft 365 sans frais supplémentaires. Pour obtenir de l'aide, envoyez une [demande de support FastTrack](#). ×

Le portail Microsoft 365 Defender inclut des fonctionnalités qui protègent votre environnement. Il inclut également des rapports et des tableaux de bord que vous pouvez utiliser pour surveiller et prendre des mesures. Certaines zones sont associées à des configurations de stratégie par défaut.

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.

Rapports

View information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.

3 éléments

Fav...	Nom ↑	Description
∨	Email & collaboration (3)	
☆	Email & collaboration reports	Review Microsoft recommended actions to help improve email and collaboration security.
☆	Manage schedules	Manage the schedule for the reports security teams use to mitigate and address threats to your organization.
☆	Reports for download	Download one or more of your reports.

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