

# Exchange 365

- [La boîte aux lettres locale de cet utilisateur n'a pas été migrée vers Exchange Online.](#)
- [Règle de transport 365 - copie vers une BAL user](#)
- [Utilisateurs messagerie bloquée -](#)
- [Les connecteurs 365](#)
- [Activer le transfert automatique sur une BAL Exchange 365](#)
- [Mise en place d'une nouvelle stratégie d'archivage automatique](#)
- [Modification du quota d'une BAL Exchange.](#)
- [La quarantaine Exchange 365](#)
- [Forward des mails vers l'extérieur - Pour tout le tenant \(non recommandé\).](#)
- [Forward des mails vers l'extérieur - Pour un compte du tenant](#)
- [Vérifier les règles de courrier cachées d'une BAL](#)
- [Gestion des réponses automatiques \(Shell\)](#)
- [Publier un calendrier 365](#)
- [Partage d'un calendrier de ressource vers l'extérieur](#)
- [Problème de Time Zone lors des invitations Teams](#)
- [Règle de courrier pour SPAM d'adresses au niveau du tenant](#)
- [Règle de courrier whitelist \(exemple d'un formulaire de contact\)](#)
- [Configurer l'envoi direct \(via le MX\)](#)
- [Procédure mail frauduleux](#)
- [Calendrier exchange > suppression délégation obsolète](#)
- [Voir les abonnements auquel un utilisateur est abonné](#)
- [Salles de réunion](#)
- [En shell - vérifier les droits sur un calendrier](#)
- [En Shell > activer l'archivage à extension automatique](#)
- [Activer l'archivage en ligne !](#)

# La boîte aux lettres locale de cet utilisateur n'a pas été migrée vers Exchange Online.

*La boîte aux lettres Exchange Online sera disponible une fois la migration terminée.*

[This user's on-premises mailbox hasn't been migrated to Exchange Online. The Exchange Online mailbox will be available after migration is completed. | Experts Exchange](#)

"MsExchMailboxGuid", "MsExchRecipientDisplayType", and "MsExchRecipientTypeDetails"

Les nettoyer

Synchroniser

# Règle de transport 365 - copie vers une BAL user

Mise en place d'une règle de transport pour transférer un mail vers une BAL utilisateur sous conditions.

## Set rule conditions

Name and set conditions for your transport rule

Name \*

Exploitation ajouter en cci patricia@attard-trans.com

Apply this rule if \*

The sender

address matches any of these text pat...



The sender address matches any of these text patterns



And

The sender

IP address is in any of these ranges or...



Sender's IP address is in the range



Do the following \*

Add recipients

to the Bcc box



Blind carbon copy (bcc) the message to



Dans le champ 1 > indiquer l'adresse de l'expéditeur.

Dans le champ 2 > préciser l'adresse IP du serveur de messagerie de l'expéditeur.

Dans le champ 3 > indiquer l'adresse vers laquelle envoyer une copie.

# Utilisateurs messagerie bloquée -

Dans les organisations Microsoft 365 avec des boîtes aux lettres dans des organisations Exchange Online ou autonomes Exchange Online Protection (EOP) sans boîtes aux lettres Exchange Online, plusieurs choses se produisent si un utilisateur dépasse les [limites d'envoi sortant du service](#) ou les [limites des stratégies de courrier indésirable sortant](#) :

- L'utilisateur n'est pas autorisé à envoyer des e-mails, mais il peut toujours recevoir des e-mails.
- L'utilisateur est ajouté à la page **Entités restreintes** dans le portail Microsoft Defender. Une *entité restreinte* est un **compte d'utilisateur** ou un **connecteur** qui n'est pas autorisé à envoyer des e-mails en raison d'indications de compromission, ce qui inclut généralement le dépassement des limites de réception et d'envoi de messages.
- Si l'utilisateur tente d'envoyer un e-mail, le message est retourné dans un rapport de non remise (également appelé notification d'échec de remise ou message de rebond) avec le code d'erreur [5.1.8](#) et le texte suivant :

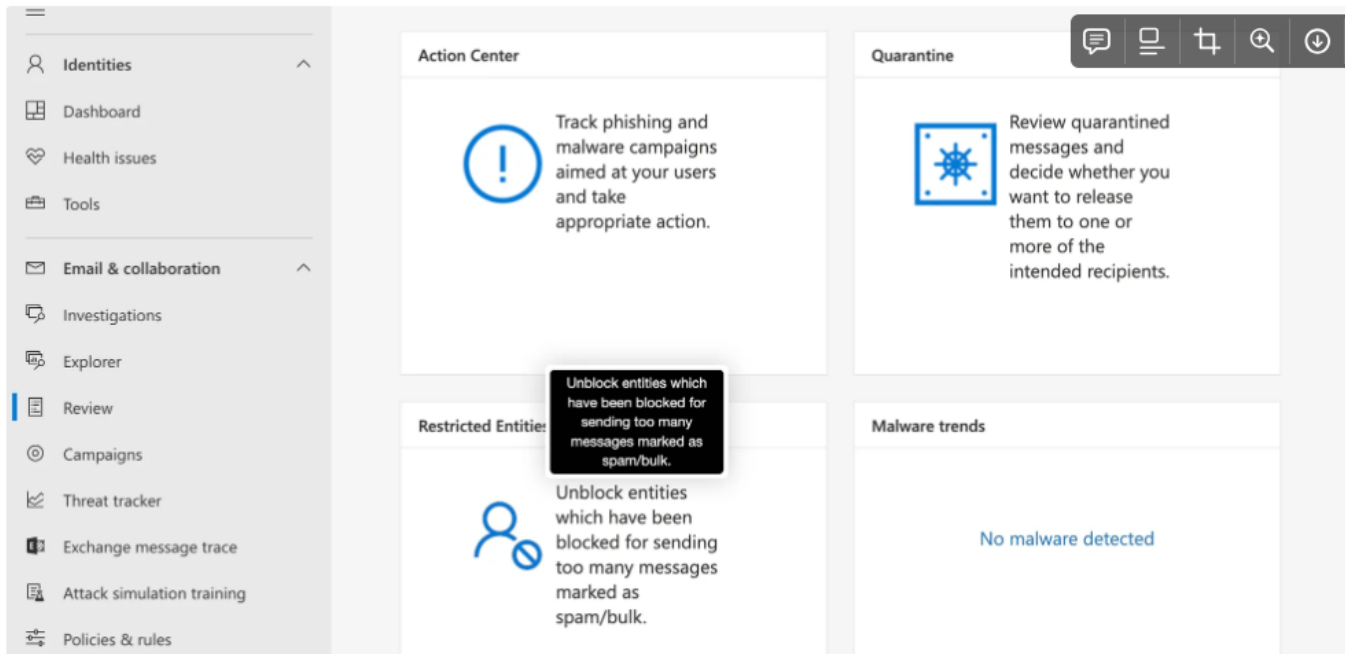
“ «Votre message n'a pas pu être remis parce que vous n'avez pas été reconnu comme expéditeur valide. Le plus souvent, il est possible que votre adresse de messagerie soit susceptible d'envoyer du courrier indésirable et qu'elle ne soit plus autorisée à envoyer du courrier électronique. Contactez votre administrateur de courrier pour obtenir de l'aide. Le serveur distant a renvoyé' 550 5.1.8 accès refusé, expéditeur sortant incorrect».

## SOLUTION

# Supprimer un utilisateur de la page Entités restreintes dans le portail Microsoft Defender

Dans le portail Microsoft Defender à l'adresse <https://security.microsoft.com>, accédez à **Email & collaboration>Examiner les>entités restreintes**. Ou, pour accéder directement à la page **Entités restreintes**, utilisez <https://security.microsoft.com/restrictedentities>.

1. Dans la page **Entités restreintes**, identifiez le compte d'utilisateur à débloquer. La valeur **de l'entité** est **Mailbox**. Pour modifier la liste des entités d'un espacement normal à un espacement compact, sélectionnez **Modifier l'espacement de liste en compact ou normal**, puis sélectionnez **Liste compacte**. Utilisez la zone **De recherche** et une valeur correspondante pour rechercher des utilisateurs spécifiques. Sélectionnez un en-tête de colonne à trier en fonction de cette colonne.



2. Sélectionnez l'utilisateur à débloquer en sélectionnant la zone case activée de l'entité, puis en sélectionnant l'action **Débloquer** qui apparaît sur la page.
3. Dans le menu volant **Débloquer l'utilisateur** qui s'ouvre, lisez les détails du compte restreint dans la page **Vue d'ensemble**. Vérifiez que vous avez suivi les suggestions de la section **Recommandations** pour confirmer que le compte n'est pas compromis ou pour reprendre le contrôle du compte. Lorsque vous avez terminé dans la page **Vue d'ensemble**, sélectionnez **Suivant**.
4. Dans la **page Débloquer l'utilisateur**, tenez compte des recommandations et utilisez les liens dans les sections **Authentification multifacteur** et **Modifier le mot de passe** pour **Activer l'authentification multifacteur** et **Réinitialiser le mot de passe de l'utilisateur** si vous n'avez pas déjà effectué ces étapes. L'activation de l'authentification multifacteur et la réinitialisation du mot de passe constituent une bonne défense contre la compromission future du compte. Lorsque vous avez terminé d'accéder à la **page Débloquer l'utilisateur**, sélectionnez **Envoyer**.
5. Sélectionnez **Oui** dans la boîte de dialogue d'avertissement qui s'ouvre.

# Les connecteurs 365

Le connecteur, permet d'authentifier les mails qui lui parviendrait d'une IP précise, comme étant des mails du tenant.

On peut mettre n'importe quoi comme adresse en Sender, vu que c'est l'IP qui sert d'authentification.

Il faut juste avoir une adresse avec un domaine accepté du tenant.

[Comment configurer un appareil ou une application multifonctions pour envoyer des e-mails à l'aide de Microsoft 365 ou Office 365](#)

L'envoi direct est recommandé pour les logiciels ERP

## Paramètres de l'envoi direct

Entrez les paramètres suivants directement sur l'appareil ou dans l'application :

### Agrandir le tableau

Paramètre du périphérique ou de l'application	Valeur
Hôte du serveur/hôte actif	Votre point de terminaison MX, par exemple contoso-com.mail.protection.outlook.com
Port	Port 25
TLS/StartTLS	Facultatif
Adresse e-mail	N'importe quelle adresse de messagerie de l'un de vos domaines Microsoft 365 ou Office 365 acceptés. Cette adresse e-mail n'a pas besoin d'avoir de boîte aux lettres.

Nous vous recommandons d'ajouter un enregistrement SPF (Sender Policy Framework) pour éviter d'avoir des messages marqués comme courrier indésirable. Si vous envoyez à partir d'une adresse IP statique, ajoutez-la à votre enregistrement SPF dans les paramètres DNS de votre bureau d'enregistrement de domaines comme suit :

### Agrandir le tableau

Entrée DNS	Valeur
SPF	<code>v=spf1 ip4:&lt;Static IP Address&gt; include:spf.protection.outlook.com ~all</code>

## EXEMPLE

Création d'un connecteur Akanea pour autoriser les mail en provenance de 194.30.173.12 comme étant des mails du tenant

Mail flow scenario

From: Your organization's email server

To: Office 365

Name

Akanea

Status

On

Edit name or status

How to identify email sent from your email server

Identify incoming messages from your email server by verifying that the sending server's IP address is within these IP address ranges: IP ADDRESS, and the sender's or recipient's email address is an accepted domain for your organization.

Edit sent email identity

Création d'une règle de transport pour générer une copie cci à destination de Patricia pour les mails envoyés depuis exploitation + adresse ADRESSE IP Expéditeur.

Rule description

Apply this rule if

sender ip addresses belong to one of these ranges: 'IP ADDRESS'

and Includes these patterns in the From address: 'ADRESSE EXPEDITEUR'

Do the following

Blind carbon copy(Bcc) the message to 'ADRESSE BCC'

# Activer le transfert automatique sur une BAL Exchange 365

## Depuis le centre d'administration O365

- Connexion tenant O365 > trouver l'utilisateur
- Dans l'onglet Mail > vérifier si un transfert est actif.

### Mailbox storage

[Learn more about mailbox storage quotas](#)

#### Mailbox permissions

[Read and manage permissions \(1\)](#)

[Send as permissions \(0\)](#)

[Send on behalf of permissions \(0\)](#)

#### Show in global address list

Yes

[Manage global address list visibility](#)

#### Automatic replies

On

[Manage automatic replies](#)

#### Email apps

Other email apps allowed

[Manage email apps](#)

#### Email forwarding

None

[Manage email forwarding](#)

#### More actions

[Edit Exchange properties](#)

- Manage email Forwarding > décocher la case.
- Tester un envoi de mail et faire un message TRACE pour vérifier que le transfert est bien actif.
- Dans la console Exchange ADMIN > Mail Flow > message trace > on peut voir les flux de mail et constater le transfert de mail.





# Mise en place d'une nouvelle stratégie d'archivage automatique

## Stratégie de rétention auto

Tout mail de plus de 2 ans > archive en ligne stratégie par défaut (dossier système)

FAIRE UNE CAPTURE D'ECRAN DE LA STRATEGIE

Dans le centre d'administration Partner > microsoft 365 compliance

## Faire une nouvelle Balise.

Dans data lifestyle management > exchange (legacy) > MRM retention tags> New tag

- Choix du nom
- Choisir **automatique** pour que la balise concerne l'intégralité de la BAL. On peut aussi cibler un dossier.
- Choix du nombre de jours

**Choisir Move item to archive (attention delete par défaut).**

## Nouvelle politique de rétention

Dans MRM retention policies > new policy

Si c'est une stratégie par défaut, sélectionner les TAGS de la stratégie par défaut et ajouter le TAG précédemment créé.

- La stratégie est créée.

## Rattacher la stratégie créée à l'utilisateur souhaité.

Dans le tenant Exchange admin center > cliquer sur l'utilisateur > Mailbox > retention policy > manage

Changer la retention policy pour celle qui a été créée.

- Il faudra attendre quelques jours pour qu'elle s'applique.

## Forcer l'application de la stratégie de rétention.

- Connexion à l'échange online

Connect-ExchangeOnline -DelegatedOrganization DOMAINE DE MESSAGERIE

- Forcer la stratégie à s'appliquer

Start-ManagedFolderAssistant -Identity COMPTE 365 USER

Lancer la commande plusieurs fois pour forcer l'application de la stratégie.

## Copie référence de la "Default MRM Policy"

1 Month Delete 1 Week Delete 1 Year Delete 5 Year Delete 6 Month Delete Default 2 year move to archive Junk Email Never Delete Personal 1 year move to archive Personal 5 year move to archive Personal never move to archive Recoverable Items 14 days move to archive

On peut appliquer une politique sur le dossier ARCHIVE qui est un dossier système sans passer par le web mail et l'utilisateur

# Modification du quota d'une BAL Exchange.

- Par défaut 50Go
- On peut mettre en place des quotas appliqués depuis le serveur
- Se fait en ligne de commande avec POWERSHELL.

[Configuration de quotas de stockage pour une boîte aux lettres](#)

[Increase or customize Exchange Online mailbox size - Exchange](#)

## Télécharger les packages.

```
Install-Module ExchangeOnlineManagement
```

## Connexion au tennent de l'entreprise

```
Connect-ExchangeOnline -DelegatedOrganization DOMAINE DE MESSAGERIE
```

## Récupérer les quotas du compte

```
Get-Mailbox BAL USER | Format-List  
IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDatabaseQuotaDefaults
```

## Définir de nouveaux quotas

```
Set-Mailbox BAL USER -ProhibitSendQuota 7GB -ProhibitSendReceiveQuota 7.1GB -IssueWarningQuota 6.75GB
```

## Se deconnecter !

exit

[Augmenter ou personnaliser la taille de la boîte aux lettres Exchange Online - Exchange](#)

# La quarantaine Exchange

## 365

On peut accéder à la zone de quarantaine via le centre de sécurité Defender > email et collaboration > Review > Quarantine

- Les mails sont stockés 30 jours
- On peut les prévisualiser, les autoriser si besoin ou les supprimer > il faut être administrateur.
- C'est une responsabilité d'autoriser les mails dans cette interface.
- Si un mail part d'une adresse contact vers cette même adresse > mail enregistré dans un site internet > peut se retrouver en mail reçu même si c'est du SPAM.

[Anti-spam message headers](#)

# Forward des mails vers l'extérieur - Pour tout le tenant (non recommandé).

Configurer au niveau de la BAL utilisateur le forward vers une adresse mail est possible.

Cependant par défaut et pour des raisons de sécurité cette option n'est pas active par défaut dans le tenant.

Connexion à Defender > Email & Collaboration > Policies and rules > Threat Policies > Anti-Spam policies > anti-spam out bound policy

The image shows two side-by-side screenshots from the Microsoft Defender portal. The left screenshot is titled "Anti-spam policies" and displays a table of policies. The right screenshot is titled "Protection settings" and shows configuration options for message limits, forwarding rules, and notifications.

**Anti-spam policies**

We recommend enabling preset security policies to stay updated with new security controls and our recommended settings. [View preset security policies](#)

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, and outbound spam filter.

+ Create policy   Refresh

Name	Status
<input type="checkbox"/> Anti-spam inbound policy (Default)	Always on
<input type="checkbox"/> Connection filter policy (Default)	Always on
<input checked="" type="checkbox"/> Anti-spam outbound policy (Default)	Always on

**Protection settings**

**Message limits**

Set an external message limit

Set an internal message limit

Set a daily message limit

Restriction placed on users who reach the message limit

Restrict the user from sending mail until the following day

**Forwarding rules**

Automatic forwarding rules

Automatic - System-controlled

**Notifications**

☐ Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

☐ Notify these users and groups if a sender is blocked due to sending outbound spam

**Save**   **Cancel**

Changer le mode automatic par on - forwarding is enable

# Forward des mails vers l'extérieur - Pour un compte du tenant

Création d'une nouvelle stratégie outbound

## Name your policy



Add a name and description for your custom anti-spam policy.

Name \*

Description

Sélectionner l'utilisateur



# Protection settings



Set your outbound anti-spam settings for this policy.

## Message limits

Set an external message limit

Set an internal message limit

Set a daily message limit

Restriction placed on users who reach the message limit

No action, alert only

▼

## Forwarding rules

Automatic forwarding rules

On - Forwarding is enabled

▼

## Notifications

- ☐ Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups
- ☐ Notify these users and groups if a sender is blocked due to sending outbound spam

Notification en cas d'alerte + Forward sur ON

# Vérifier les règles de courrier cachées d'une BAL

`Get-InboxRule -mailbox BAL USER -IncludeHidden`

[Get-InboxRule \(ExchangePowerShell\) | Microsoft Learn](#)

# Gestion des réponses automatiques (Shell)

```
Get-MailboxAutoReplyConfiguration -identity service.gestion1@abdgestion.com
```

```
set-MailboxAutoReplyConfiguration -identity service.gestion1@abdgestion.com -AutoReplyState disabled
```

[Set-MailboxAutoReplyConfiguration \(ExchangePowerShell\)](#)

# Publier un calendrier 365

[Enable External Users for booking and adding Exchange Room Calendars - .matrixpost.net](#)

Get-MailboxCalendarFolder Room1:\Calendar | Select *publish*

Set-MailboxCalendarFolder Room1:\Calendar -PublishEnabled **\$true**

# Partage d'un calendrier de ressource vers l'extérieur

Les boîtes aux lettres de ressources ne doivent en aucun cas être gérées de cette manière, car les événements ne doivent pas être créés directement dans le calendrier de la salle, mais la salle doit être ajoutée en tant que ressource à la réunion, ce qui peut être réalisé via le partage fédéré.

Cela permettra d'accéder aux informations F/B, par conséquent, lorsque les utilisateurs de Tenant B réserve une salle de Tenant A, ils peuvent voir s'il est disponible ou non. De plus, pour que la salle puisse traiter les réunions externes, ils devront configurer les paramètres de la salle pour permettre le traitement des demandes externes.

[Relations d'organisation dans Exchange Online | Microsoft Learn](#)

Et en ce qui concerne [l'organisation mutualisée](#), il existe une fonctionnalité dans Microsoft Entra ID et Microsoft 365 qui vous permet de définir une limite autour des locataires Microsoft Entra que votre organisation possède. Dans l'annuaire, il prend la forme d'un groupe de locataires qui représente votre organisation. Chaque paire de locataires du groupe est régie par des paramètres d'accès interlocataire que vous pouvez utiliser pour configurer la collaboration B2B.

Voici les principaux avantages d'une organisation mutualisée :

1. Différencier les utilisateurs externes internes et externes à l'organisation
2. Amélioration de l'expérience collaborative dans le nouveau Microsoft Teams
3. Amélioration de l'expérience collaborative dans Viva Engage

# Problème de Time Zone lors des invitations Teams

Get-MailboxCalendarConfiguration -Identity <user> | FL WorkingHoursTimeZone

Set-MailboxCalendarConfiguration -Identity<user> -WorkingHoursTimeZone "Romance Standard Time"

<https://learn.microsoft.com/en-us/powershell/module/exchange/set-mailboxcalendarconfiguration?view=exchange-ps>

Règle de courrier pour SPAM  
d'adresses au niveau du  
tenant








Norm <sup>★</sup>

Appliquer cette règle si \*

l'adresse correspond à l'un des mo... 



Effectuer les opérations suivantes \*

quarantaine hébergée



Sauf si

Sélectionnez un

### Paramètres de règle

## Mode

## Enforce

### Définir la plage de dates

La plage de dates spécifique n'est pas définie

## Priorité

1

## Non spécifié

Ignore

false

[Modifier les paramètres des règles](#)[Modifier les conditions de règle](#)



# Règle de courrier whitelist

## (exemple d'un formulaire de contact)

Whitelist Mails site Web formulaire de contact

Conditions

Paramètres

Nom \*

Whitelist Mails site Web formulaire de contact

Appliquer cette règle si \*

Le destinataire

est externe/interne

+

Le destinataire se trouve 'inOrganization'

Et

Objet ou corps

L'objet correspond à ces modèles de texte 'Formulaire de contact'

+

Et

L'expéditeur

L'adresse correspond à l'un des modèles de texte suivants

+

L'adresse de l'expéditeur correspond à l'un de ces modèles de texte 'inOrganization'

Et

L'expéditeur

est externe/interne

+

L'expéditeur se trouve 'NotInOrganization'

Effectuer les opérations suivantes \*

Modifier les propriétés du message

définir le seuil de probabilité de courrier indésirable (SCL)

+

Définir le niveau de probabilité de courrier indésirable (SCL) sur '-1'

# Configurer l'envoi direct (via le MX)

<https://learn.microsoft.com/fr-fr/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365#option-2-send-mail-directly-from-your-printer-or-application-to-microsoft-365-or-office-365-direct-send>

# Procédure mail frauduleux

## USURPATION ET MAIL FRAUDULEUX PROCEDURE

1. Reset MDP.
2. Déconnexion des sessions via le centre Admin 365. Révoquer les sessions
3. Vérifier le MFA.
4. Ouvrir l'OWA, checker les règles Inbox.
5. Déconnecter depuis l'OWA els appareils mobiles ( Tous, pas de social).
6. Scan AV.
7. Vérification de la délégation sur la BAL en question.

## Centre d'administration Identité

1. Vérification des journaux de connexion
2. Vérification des applications (autorisations accordées) et exécution d'un script graph si besoin de les supprimer proprement.

<https://www.it-connect.fr/obtenir-la-liste-des-nouveaux-domaines-fr-potentiellement-malveillants/>

## Echange téléphonique avec le client

Bonjour

Ce mail fait suite à notre conversation téléphonique.

Concernant la sécurité de vos boîtes aux lettres, il y a quelques réflexes à avoir et des bonnes pratiques, comme celles décrites par l'ANSSI : <https://www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/>

1. Vérifier que l'expéditeur affiché est bien l'expéditeur réel du mail : Vos Outlook affichent, entre parenthèses à droite du nom/prénom de l'auteur, l'adresse mail d'envoi
2. Passer votre curseur de souris sans cliquer, sur les expéditeurs, liens contenus dans les mails, images, pour voir le chemin réel. Si la destination vous semble douteuse ou frauduleuse, ne faites pas confiance à ce mail.
3. En cas de doute sur un mail, n'hésitez pas à contacter l'auteur présumé par un autre moyen, comme le téléphone, pour vérifier s'il est bien à l'origine de ce mail. Surtout si vous n'attendiez pas de communication de leur part.

Malgré toutes ces recommandations, des éléments peuvent passer outre votre vigilance, car nous relevons effectivement une forte recrudescence de mails malveillants ou tentatives de piratages. Je vous invite à nous signaler tout mail frauduleux qui vous aurait été adressé et remis en boîte de

réception, et non en indésirable, pour amélioration du filtrage.

Je reste à votre disposition pour tout complément d'informations. Vous pouvez me recontacter au 05 .. ou en répondant à ce mail. Dans l'attente de votre retour, je vous souhaite une excellente journée.

# Calendrier exchange > suppression délégation obsolète

***Get-InboxRule -Mailbox "DelegatorUserEmailaddress" -IncludeHidden***

***Get-InboxRule -Mailbox "DelegatorUserEmailaddress" -IncludeHidden -identity (rule identity)***

***Get-InboxRule -Mailbox "DelegatorUserEmailaddress" -IncludeHidden -identity (rule identity) | FL***

Suppression de la règle de courrier

***Get-InboxRule -Mailbox "DelegatorUserEmailaddress" -IncludeHidden -identity (rule identity) | remove-inboxrule***

# Voir les abonnements auquel un utilisateur est abonné

```
Get-Mailbox | % { Get-MailboxFolderPermission (($_).PrimarySmtpAddress.ToString())+":\Calendar")  
-User xxxx@xxxx.xxx -ErrorAction SilentlyContinue} | select Identity,User,AccessRights
```

ou

```
Get-Mailbox | % { Get-MailboxFolderPermission (($_).PrimarySmtpAddress.ToString())+":\Calendar")  
-User xxxx@xxxx.xxx -ErrorAction SilentlyContinue} | select Identity,User,AccessRights
```

# Salles de réunion

Attribuer des droits sur une salle de réunion /shell

**Placer le nom de la personne ayant fait la réservation, dans l'objet, et rend le détail de l'évènement, visible sur les Outlook des autres utilisateurs**

```
Set-CalendarProcessing -Identity FQDN SALLE -AddOrganizerToSubject $true -DeleteComments $false -DeleteSubject $false
```

**Donner le rôle REVIEWER à tous les utilisateurs sur une salle de réunion.**

```
set-MailboxFolderPermission -identity FQDN SALLE:\calendar -user default -AccessRights reviewer
```

(ne jamais supprimer l'autorisation par défaut)

# En shell - vérifier les droits sur un calendrier

- Se connecter à Exchange On-line

```
Connect-ExchangeOnline -DelegatedOrganization [medef-gironde.fr](http://medef-gironde.fr/)
```

- Vérifier les droits donnés à des utilisateurs sur le calendrier de madame CHESNE

```
Get-MailboxFolderPermission -identity [cchesne@medef-gironde.fr](mailto:cchesne@medef-gironde.fr):\calendrier
```

- Attribuer un droit REVIEWER a Monsieur Ducos sur le calendrier de Madame Chesne

```
add-MailboxFolderPermission -identity [cchesne@medef-gironde.fr](mailto:cchesne@medef-gironde.fr):\calendrier -user [jducos@medef-gironde.fr](mailto:jducos@medef-gironde.fr) -AccessRights reviewer
```

- Cela fonctionnerait de la même façon avec une salle de réunion.

Après application du code >

- Attendre minimum 1 heure pour que les droits s'appliquent (idéalement le lendemain matin).
- Supprimer le calendrier > le rappeler de nouveau depuis la GAL
- ne surtout pas utiliser l'option depuis un calendrier partagé.
- Remplacer l'autorisation par défaut sur un calendrier

```
Set-MailboxFolderPermission -Identity twingo@ccbi.fr:calendar -user 'par défaut' -AccessRights Editor
```



# En Shell > activer l'archivage à extension automatique

## [Enable auto-expanding archiving](#)

- Connecter à exchange On Line (attention en temps que partenaire nous n'aurons les droits pour activer ce paramètre.

```
Connect-ExchangeOnline -Organization [cabcourtois.com](http://cabcourtois.com/)
```

- Obtenir les informations sur le paramètre

```
Get-Mailbox [vcourtois@cabcourtois.com](mailto:vcourtois@cabcourtois.com) | FL  
AutoExpandingArchiveEnabled
```

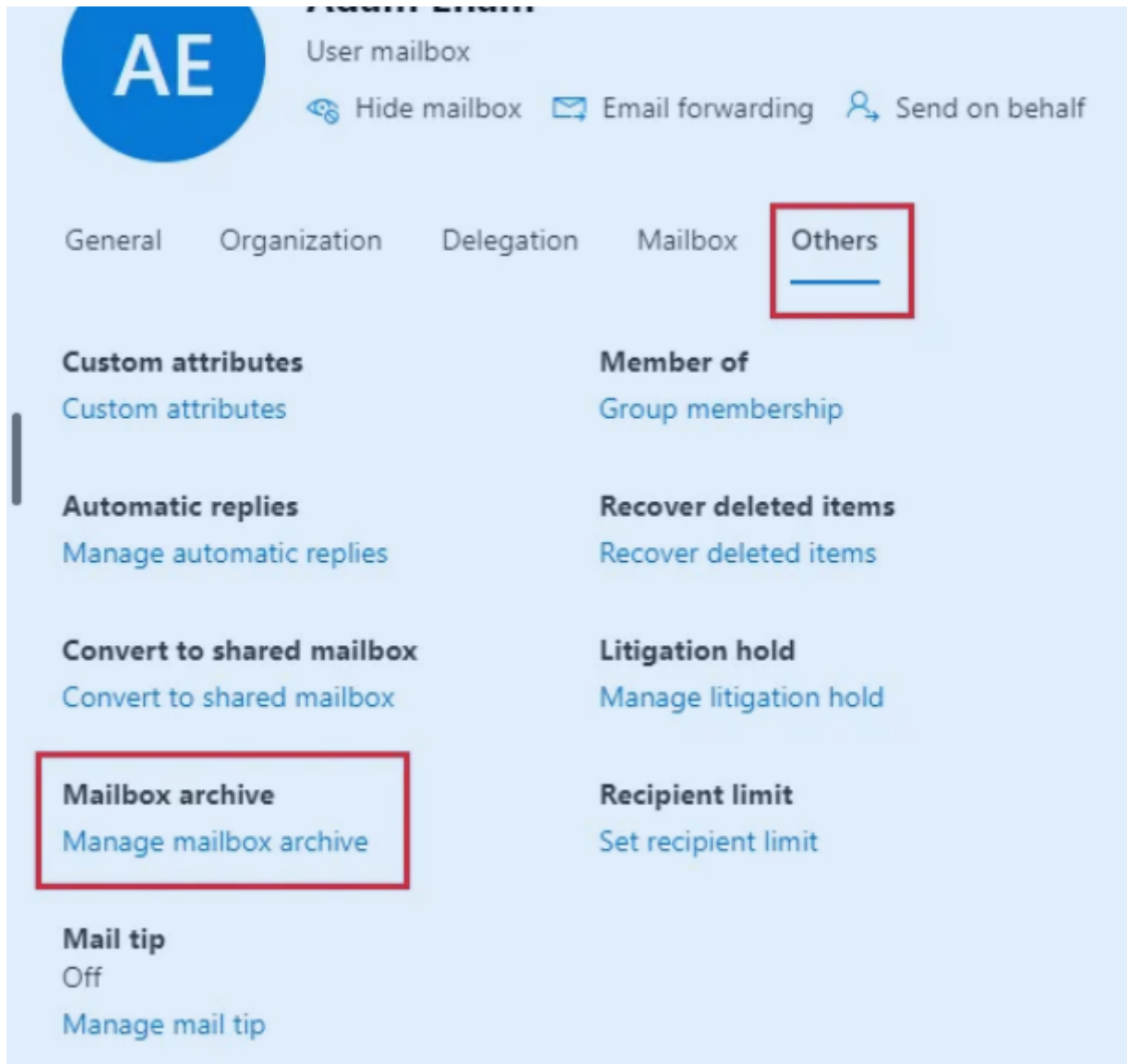
- Activer le paramètre pour l'utilisateur.

```
Enable-Mailbox [vcourtois@cabcourtois.com](mailto:vcourtois@cabcourtois.com) -AutoExpandingArchive
```

# Activer l'archivage en ligne !

[Activer les boîtes aux lettres d'archivage pour Microsoft 365](#)

Depuis le centre d'administration Exchange



En SHELL :

- Connexion exchange Online
- Activer l'archivage

```
Enable-Mailbox -Identity <username> -Archive
```

- Pour tous les utilisateurs ! Vérifier que ce n'est pas activé et l'activer dans ce cas).

```
Get-Mailbox -Filter {ArchiveGuid -Eq "00000000-0000-0000-0000-000000000000" -AND RecipientTypeDetails -  
Eq "UserMailbox"}} | Enable-Mailbox -Archive
```