



## Letsignit Office 365 SMTP feature setup.

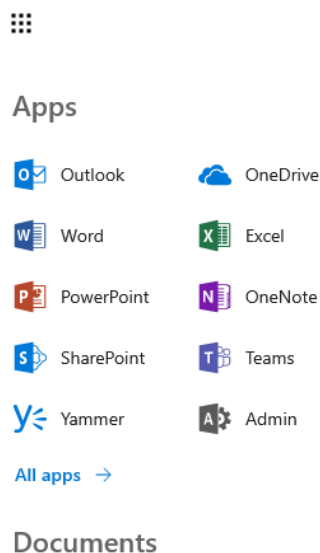
Author	Translated by	Date	Version
FCA	PMJ	06/2020	3.1
FCA	FCA	11/2020	3.2

## Contents

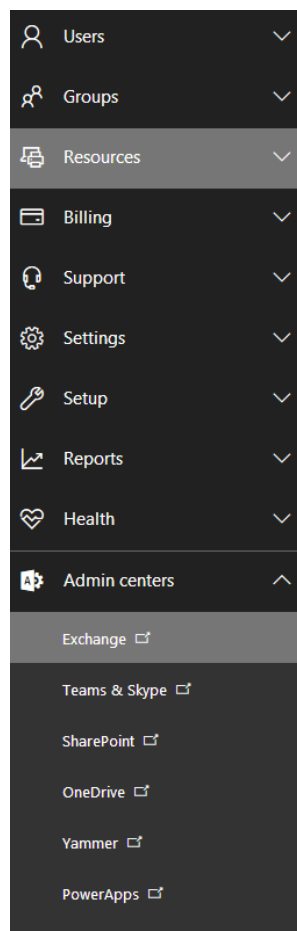
1. Defining the receiving SMTP connector .....	3
2. Create a send connector to Letsignit servers.....	7
3. Settings applied to the connector .....	10
4. The case of distributor's lists created under local Exchange .....	15
5. Automatic absence response case .....	16
6. Disclaimers configured in Exchange Online .....	19
7. Microsoft Planner and/or Teams logistics case.....	19
8. 'Enable-OrganizationCustomization' error.....	21
9. Annex: How to connect to Azure in PowerShell: .....	21
10. Annex: How to set up the App password for automatic implementation .....	23
11. Non-reception of internal user emails .....	24
12. Memento – important information .....	24

## 1. Defining the receiving SMTP connector

To do this, go to the Office 365 administrator section:



From the “**Admin Center**” App, click on “**Exchange**” tab:



## From “Exchange Admin Center” go to “mail flow”

### Exchange admin center

dashboard

recipients

permissions

compliance management

organization

protection

advanced threats

mail flow

mobile

public folders

unified messaging

hybrid

Welcome

recipients

mailboxes

groups

resources

contacts

shared

migration

organization

sharing

add-ins

## Then go to “Connectors” tab:

### Exchange admin center

dashboard

recipients

permissions

compliance management

organization

protection

advanced threats

mail flow

mobile

public folders

unified messaging

hybrid

rules message trace url trace accepted domains remote domains connectors

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we've simplified the experience. Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

+ ✎ 🗑️ ↺

STATUS	NAME	FROM
There are no items to show in this view.		

## Then click on the + sign.

rules message trace url trace accepted domains remote domains connectors

We have simplified & improved the Connectors management experience in the new Exchange admin portal. You can try to preview the experience.

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we've simplified the experience. Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

+ ✎ 🗑️ ↺

STATUS	NAME	FROM
On	to lscloud-smtp.letsignit.com	Office 365

LETSGNIT

50 rue Breteuil 13006 MARSEILLE | Tel. +33 4 88 60 02 54 | [contact@letsignit.com](mailto:contact@letsignit.com) | [www.letsignit.com](http://www.letsignit.com)  
Siret 824 622 740 000 10 | RCS Marseille Capital 16 363€ | APE 6201 Z | TVA Intracommunautaire FR 20 824 622 740

## Create a new connector:

### Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.  
[Learn more](#)

From:

Your organization's email server ▼

To:

Office 365 ▼

**You need to create a connector for this mail flow scenario.** When this connector is set up, Office 365 will accept messages from your organization's email server and send the messages to recipients on your behalf. To complete this scenario, you'll also need to configure your email server to send email messages directly to Office 365. [Learn more about configuring your email server](#)

## Name it:

### New connector

This connector lets Office 365 accept email messages from your organization's email server (also called an on-premises server).

\*Name:

LSI to O365

Description:

What do you want to do after connector is saved?

- ☒ Turn it on
- ☒ Retain internal Exchange email headers (recommended)

Authorize the Letsignit's Ip: 52.226.140.66, 104.45.169.33, 40.90.242.172, 52.226.140.254, 52.185.66.245 and 13.86.124.154

LETSIGNIT

50 rue Breteuil 13006 MARSEILLE | Tel. +33 4 88 60 02 54 | [contact@letsignit.com](mailto:contact@letsignit.com) | [www.letsignit.com](http://www.letsignit.com)  
Siret 824 622 740 000 10 | RCS Marseille Capital 16 363€ | APE 6201 Z | TVA Intracommunautaire FR 20 824 622 740

## New connector

How should Office 365 identify email from your email server?

- ☐ By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches this domain name (recommended)

Example: contoso.com or \*.contoso.com

- ☒ By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization

+ ✎ -


52.226.140.66

104.45.169.33

40.90.242.172

**52.226.140.254**

52.185.66.245

-  Office 365 will only accept messages through this connector if the sender's domain or TLS certificate domain is configured as an accepted domain for your Office 365 organization. [Learn more](#)

## 2. Create a send connector to Letsignit servers

Create new connector from the tab:



Choose this flow:

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.  
[Learn more](#)

From:  
Office 365 ▼

To:  
Your organization's email server ▼

**You need to create a connector for this mail flow scenario.** Because your domain's MX record points to Office 365, you must set up an alternative server (called a smart host) so that Office 365 can send email to your organization's email server (also called on-premises server). To complete the scenario, you might need to configure your email server to accept messages delivered by Office 365. [Learn more about configuring your email server](#)

In the next step name the connector at your convenience:

\*Name:

Description:

What do you want to do after connector is saved?

- ☒ Turn it on
- ☒ Retain internal Exchange email headers (recommended)

***We advise you to name the mail flow: 'smtp-us.letsignit.com'.***

The next step asks you “when” the connector should be activated. If you wish to use the SMTP connector for internal and external emails, follow the steps below:

## New connector

When do you want to use this connector?

- ☒ Only when I have a transport rule set up that redirects messages to this connector
- ☐ For email messages sent to all accepted domains in your organization
- ☐ Only when email messages are sent to these domains

+ ✎ -

Select  
you c  
redire  
this o  
[Learn](#)

In the next step, indicate “who” Office 365 will send your mail flow to (you should enter: **smtp-us.letsignit.com**):

## New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

+ ✎ -

smtp-us.letsignit.com

You can add more smart hosts at your convenience to ensure a continuity of service.



In this next step, you should activate the TLS connector, like shown below:

### New connector

How should Office 365 connect to your email server?

- ☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)
- Connect only if the recipient's email server certificate matches this criteria
- ☐ Any digital certificate, including self-signed certificates
- ☒ Issued by a trusted certificate authority (CA)
- ☒ And the subject name or subject alternative name (SAN) matches this domain name:

smtp-us.letsignit.com

Finally, Office 365 will ask you to validate the scenario you have defined as well as to test the validation of the connection between Office 365 and your Letsignit solution. For this step, you must have done step 1 of this document.

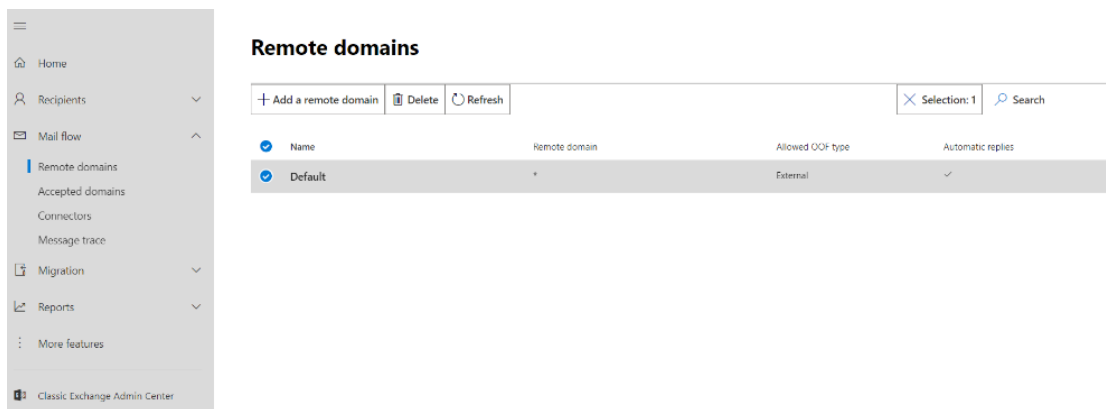
## 3. Settings applied to the connector

### a) Modify the messaging format

In order for Letsignit to read the content of the emails received from Office 365, email communications from winmail.dat should be avoided: <https://support.microsoft.com/en-us/kb/2487954>

To do this

Go to the 'Domain' section of your Exchange Online and then to the 'RemoteDomain' section of your 'Mail flow' tab. Then, edit the 'Default' rule.



Then, put the 'User RTF format' value to 'Never'

Remote Domain: - Google Chrome  
outlook.office365.com/ecp/RemoteDomain/NewRemoteDomain.as...

new remote domain

Specify a domain that will be considered remote when mail is received.

\*Name:  
Default

\*Remote Domain:  
\*

Out of Office automatic reply types:  
☐ None  
☒ Allow only external Out of Office replies  
☐ Allow internal Out of Office replies

Automatic replies:  
☒ Allow automatic replies  
☒ Allow automatic forwarding

Message reporting:  
☒ Allow delivery reports  
☒ Allow non-delivery reports  
☐ Allow meeting forward notifications

Use rich-text format:  
☐ Always  
☒ Never  
☐ Follow user settings

Supported Character Set  
MIME character set:  
None

Non-MIME character set:  
None

Choose to always or never send messages using rich-text format. Use Follow user settings to send email messages that use the rich-text settings specified by the Outlook user.

Save Cancel

## b) Implement a connection filter

Go to the connection filter interface:

## Exchange admin center

[dashboard](#)
[recipients](#)
[permissions](#)
[compliance management](#)
[organization](#)
[protection](#)
[advanced threats](#)
[mail flow](#)
[mobile](#)
[public folders](#)
[unified messaging](#)
[hybrid](#)

### Welcome

We're updating the Exchange admin center and need your expert feedback to make it even better. Give it a try, and share your thoughts. [Try it now](#)

**recipients**
[mailboxes](#)
[groups](#)
[resources](#)
[contacts](#)
[shared](#)
[migration](#)

**permissions**
[admin roles](#)
[user roles](#)
[Outlook Web App policies](#)

**compliance management**
[in-place eDiscovery & hold](#)
[auditing](#)
[data loss prevention](#)
[retention policies](#)
[retention tags](#)
[journal rules](#)

**organization**
[sharing](#)
[add-ins](#)




**protection**
[malware filter](#)
[connection filter](#)
[spam filter](#)
[outbound spam](#)
[quarantine](#)
[action center](#)
[dkim](#)

**advanced threats**
[safe attachments](#)
[safe links](#)

Then, choose the filter connection:

[dashboard](#)
[recipients](#)
[permissions](#)
[compliance management](#)
[organization](#)
[protection](#)
[advanced threats](#)
[mail flow](#)
[mobile](#)
[public folders](#)
[unified messaging](#)
[hybrid](#)

malware filter **connection filter** spam filter outbound spam quarantine action center dkim

NAME	
Default	<div>Default</div> <div>Scoped to: All domains</div> <div>Summary</div> <div>IP Allow list: Configured</div> <div>IP Block list: Not configured</div> <div>Safe list: Disabled</div>

Using the + sign, add the following IP, one by one: 52.226.140.66, 104.45.169.33, 40.90.242.172, 52.226.140.254, 52.185.66.245 and 13.86.124.154. Save.

Default

general

• connection filtering

connection filtering

IP Allow list

Always accept messages from the following IP addresses.

+ ✎ -

Allowed IP Address
192.168.1.1
192.168.1.2
192.168.1.3

IP Block list

Always block messages from the following IP addresses.

+ ✎ -

Blocked IP Address

☐ Enable safe list

### c) Add a rule

Now the connector is activated and configured, you must create a rule that will redirect the emails to it.

To do this, go to “rules” (tab on the left):

[rules](#) [message trace](#) [url trace](#) [accepted domains](#) [remote domains](#) [connectors](#)

Next, add one and define it like shown below:

LETSIGNIT

50 rue Breteuil 13006 MARSEILLE | Tel. +33 4 88 60 02 54 | [contact@letsignit.com](mailto:contact@letsignit.com) | [www.letsignit.com](http://www.letsignit.com)  
Siret 824 622 740 000 10 | RCS Marseille Capital 16 363€ | APE 6201 Z | TVA Intracommunautaire FR 20 824 622 740

## new rule

Name:  
Route to LSI

\*Apply this rule if...

☒ The sender is located... [Inside the organization](#)

and

☒ The sender's domain is... ['admin@...'](#)

add condition

\*Do the following...

Use the following connector... [to lsicloud-smtp.letsignit.com](#)

add action

Except if...

☒ A message header includes... ['X-LSI-Version' header includes '1.0'](#)

or

☒ The message type is... [Calendaring](#)

or

☒ The sender address matches... ['<>'](#)

add exception

Properties of this rule:

☒ Audit this rule with severity level:  
Not specified

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

☐ Activate this rule on the following date:  
Tue 6/9/2020 1:30 AM

☐ Deactivate this rule on the following date:  
Tue 6/9/2020 1:30 AM

☒ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message:  
Envelope

Comments:

Where the name is chosen by you. The rule applies to the “recipient” which is “internal/external” then choose “in the organization”.

You must add the following 4 exceptions:

- The first and most important one is to detect if the email has already passed through Letsignit (choose “a message header...” then “corresponds to these text examples”) the values to be set are to be kept as they are.
- The second consists of limiting the size of the email, according to the RFC. We ask you not to exceed 29 MB.
- The third to exclude calendar notifications (choose “the message properties” then “includes the message type”).
- The fourth which excludes empty senders (choose “the sender” then “the address corresponds to one of the following templates”).
- Set the value "Envelope" in the "Match sender's address in the message" option at the bottom of the rule options.

## 4. The case of distributor's lists created under local Exchange

If you have a list of distributors or share mailboxes created under local Exchange and synchronized with Azure, Microsoft recognizes the potential problem in the delivery of mails to it.

This is linked to the attribute that is modified. You must modify this value like explained below.

The Microsoft link: <https://support.microsoft.com/en-us/help/2723654/external-recipients-don-t-receive-email-messages-that-are-sent-to-a-di>

Here are the values that must be changed if your infrastructure is local and not Azure:

**ReportToOriginatorEnabled : False**

>Must replace the value 'true'

This attribute will put the email in the distribution list in the return-path of expedited email.  
*If you choose to modify the second attribute (**ReportToManagerEnabled**) it will ensure you that each distribution list to a declared manager because their email list will be in the Return-Path.*

### Procedure to follow:

Execute this command on your Powershell connected to your Azure tenant:

**Get-DistributionGroup -Filter {ReportToOriginatorEnabled -eq \$false} | Format-Table Name**

If the result is different from 'null', please continue according to the origins of the distribution list concerned.

### Several cases:

- The distribution list was created in a local Exchange, please execute this command on the Powershell connected to your local Exchange.

**Set-DistributionGroup -Identity "Nom\_de\_la\_liste" -ReportToOriginatorEnabled \$true**

- The distribution list was created directly in Azure. We have noticed that certain distribution lists can have this behavior.

**Set-DistributionGroup -Identity "Nom\_de\_la\_liste" -ReportToOriginatorEnabled \$true**

- The distribution list was created on a local AD, without the presence of Exchange. → This case will be the subject of an ancillary procedure requiring a schema extension to create these attributes.

## 5. Automatic absence response case

If you have automatic responses activated, it is necessary to add a rule with a higher priority than the created transport rule for the redirection of emails.

This rule should be configured as follows:

Go to your Exchange Administration center.

Click on the **“Mail flow”** menu and then, **“Rules”**

Exchange admin center

dashboard rules message trace accepted domains remote domains connectors

recipients permissions compliance management organization protection **mail flow** mobile public folders unified messaging hybrid

ON	RULE	PRIORITY
<input checked="" type="checkbox"/>	Route email to Letsignit signature service (devlsi.fr)	0

Route email to Letsignit signature service (devlsi.fr)

If the message...

sender's address domain portion belongs to any of these domains: 'devlsi.fr' and is received from: 'Inside the organization'

Do the following...

Route the message using the connector named 'Office 365 to Letsignit signature service (devlsi.fr)' and Stop processing more rules

Except if...

Is message type 'Calendar' or 'X-LSI-Version' header contains '1.0' or Includes these patterns in the From address: '<>'

Rule mode

Enforce

Additional properties

Sender address matches: Envelope

Version: 15.0.5.2

You will find the previously created Letsignit transport rule, click on the '+' to create a new rule.



Then, fill in the **‘Name’** with the value that you wish to give.

Click on the blue link **“More options”** at the bottom of the screen.



In the section “Apply the rule if...” choose “The message Properties” and then, “include the message type”.

Choose “**Automatic Reply**” and validate.

new rule - Google Chrome

https://outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=c6a58...

new rule

Name:  
Automatic response

\*Apply this rule if...

Select one

Select one

The sender...

The recipient...

The subject or body...

Any attachment...

Any recipient...

The message...

The sender and the recipient...

The message properties...

A message header...

[Apply to all messages]

include the message type

include this classification

don't include any classification

include an SCL greater than or equal to

include the importance level

Properties of this rule:

☒ Audit this rule with severity level:

Not specified

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

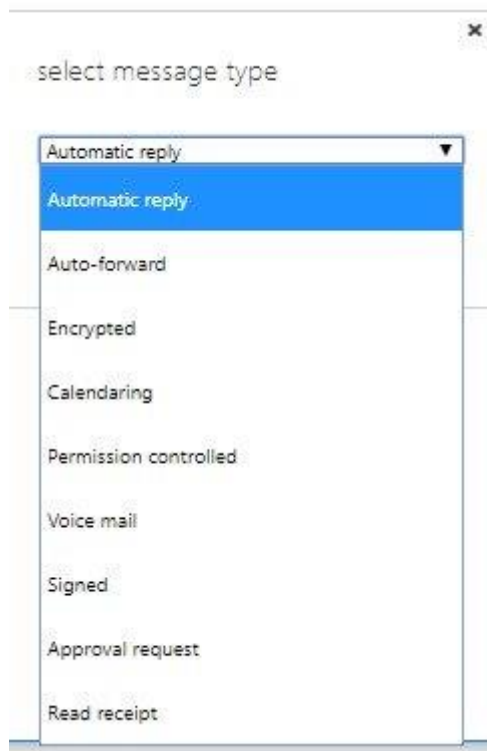
☐ Activate this rule on the following date:

Thu 18/07/2019 10:00

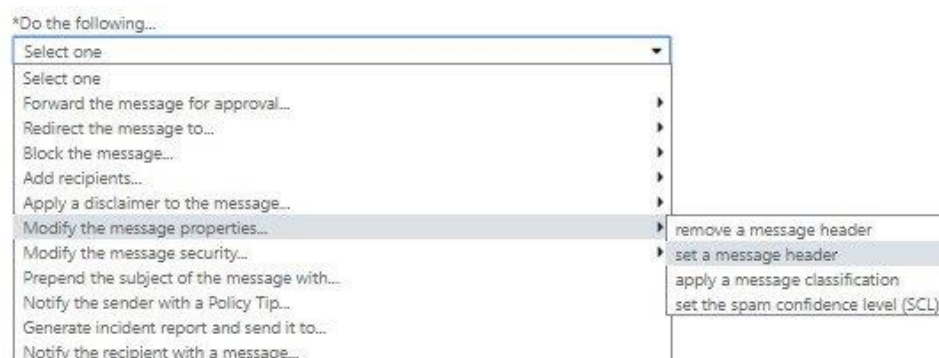
☐ Deactivate this rule on the following date:

Thu 18/07/2019 10:00

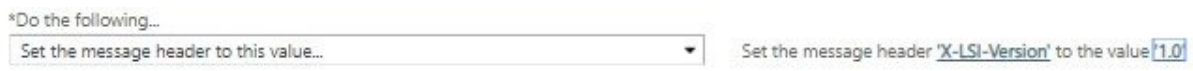
Save Cancel



In the section “Proceed as follows” choose “Modify the message properties” and then, “Set a message header”



Enter the follow value in “enter the text”: X-LSI-Version and ‘version’: 1.0



Then, save by clicking on the button at the bottom of the screen.



Reassemble the auto reply rule over the Letsignit transport rule with the up-arrow icon.



## 6. Disclaimers configured in Exchange Online

If you have a disclaimer, you can use it from Letsignit and deactivate it from your Exchange Online.

To find out if you are using a disclaimer from Exchange Online, please type the following command in a Powershell connected to your O365 holder as administrator:

**Get-TransportRule | fl Name,ApplyHtmlDisclaimerLocationIf**

The result indicates that the disclaimer function is being used, we advise you to deactivate it and use the disclaimer function of the Letsignit Cloud provided for this purpose.

## 7. Microsoft Planner and/or Teams logistics case

By default, all the messages from Planner or Teams can be sent by mail and can be signed.

To avoid this behavior, you must exclude the flow by adding an exception to the Letsignit transport rule that sends the emails to the outgoing connector.

Here are the steps to take after you have connected your Exchange control panel, from the “mail flow” section and then, the “transport rule” section.

[rules](#) [message trace](#) [url trace](#) [accepted domains](#) [remote domains](#) [connectors](#)

Select the existing Letsignit transport rule and edit it.

Then, click on “Add exception”.

new rule

Name:

Apply this rule if...

☒ The sender is located... [inside the organization](#)

and

☒ The sender's domain is... [admin@letsignit.com](#)

Do the following...

Use the following connector... [to letsignit-remote.letsignit.com](#)

Except if...

☒ A message header includes... [X-LSI-Version header includes '1.0'](#)

or

☒ The message type is... [Calendar](#)

or

☒ The sender address matches... ["x"](#)

Properties of this rule:

☒ Audit this rule with severity level: [Not specified](#)

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

☐ Activate this rule on the following date: [Tue 6/9/2020 1:30 AM](#)

☐ Deactivate this rule on the following date: [Tue 6/9/2020 1:30 AM](#)

☒ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message: [Envelope](#)

Comments:

Select from the scroll menu, “A message header...” then “matches these text patterns”

Select one

Select one

The sender...

The recipient...

The subject or body...

Any attachment...

Any recipient...

The message...

The sender and the recipient...

The message properties...

A message header...

☐ includes any of these words

☐ matches these text patterns

☐ Test without Policy Tips

☐ Activate this rule on the following date:

Complete the respective name in the header and the value with the following:

Header name: **X-MS-Exchange-UnifiedGroup-SubmittedViaGroupAddress**

Header value: **/o=ExchangeLabs/ou=Exchange Administrative Group**

specify header name

X-MS-Exchange-UnifiedGroup-SubmittedViaGroupAddress

OK Cancel

specify words or phrases

/o=ExchangeLabs/ou=Exchange Administrative Group

OK Cancel

Then, save.

Save Cancel

## 8. 'Enable-OrganizationCustomization' error

If during the automatic procedure (via the website cloud.letsignit.com) or during a manual procedure you encounter the error:

The command you tried to run is not currently allowed in your organization. To run this command, you first need to run the command: Enable-OrganizationCustomization.

+ CategoryInfo: NotSpecified: (Default:String) [Set-HostedConnectionFilterPolicy],

InvalidOperationInD\u2026tedContextException

+ FullyQualifiedErrorId: [Server=YQBPR0101MB2241,RequestId=2465bb42-aacb-4cc7-8911-562e93ed8940,TimeStamp=9/20/2019 8:32:50 PM] [FailureCategory=Cmdlet-InvalidOperationInDehydratedContextException]

158D1C75,Microsoft.Exchange.Management.SystemConfigurationTasks.SetHostedConnectionFilterPolicy

+ PSComputerName: outlook.office365.com

The type in the following command in a Powershell connected to your O365 and administrator tenant:

**Get-OrganizationConfig | Select -ExpandProperty IsDehydrated**

If the result indicates that the feature is 'disabled' or 'False' then we advise you to activate the feature with the following command:

**Enable-OrganizationCustomization**

## 9. Annex: How to connect to Azure in PowerShell:

Connect in Powershell to your Office 365 server: [see the procedure here](#)

If not, you can follow the steps below:

```
PS C:\Windows\system32> $UserCredential = Get-Credential | $UserCredential = Get-Credential
```

**\$UserCredential = Get-Credential**

Then, authenticate it with the Office 365 administrator account

Next, enter the following command:

```
PS C:\Windows\system32> $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
PS C:\Windows\system32> $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
```

`$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential *UserCredential -Authentication Basic -AllowRedirection`

Finally, to finish the command, do the following:

```
PS C:\Windows\system32> Import-PSSession $Session
AVERTISSEMENT : Les noms de certaines commandes importées du module « tmp_tdmvvhdx.r5r » contiennent des
approuvés qui peuvent les rendre moins détectables. Pour trouver les commandes comportant des verbes non
réexécutez la commande Import-Module avec le paramètre Verbose. Pour obtenir la liste des verbes approuvés
Get-Verb.
```

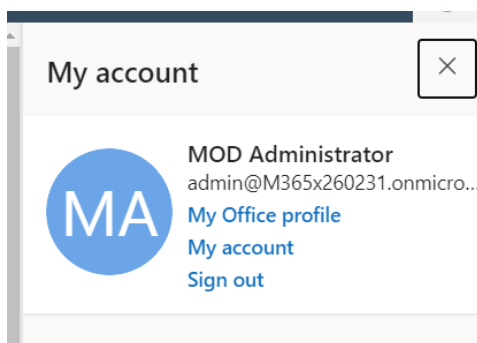
`Import-PSSession $Session`

It is possible to validate the connection by going through the Get-Mailbox command.

## 10. Annex: How to set up the App password for automatic implementation

This paragraph refers to the Microsoft Office support article: <https://support.office.com/en-gb/article/create-an-app-password-for-microsoft-365-3e7c860f-bda4-4441-a618-b53953ee1183?ui=en-US&rs=en-GB&ad=GB>

If you use multiple authentications for the authentication of your user accounts, this may cause a problem when activating the feature. To solve this, you can create an application password on your Office Holder that will be used to authenticate without using the MFA (Multiple Factor Authentication), in this case go to the "My Account" section of your Office 365 Holder.



In the **"Security and Privacy"** section go to **"create and manage app passwords"**.

You can create the app passwords in this section and use it when the app is connected via SMTP connector to your Office tenant.

To use the newly created password, you must enter it in, instead of entering the original password for the account used.

Example:

Login: exemple@exemple.fr

password: mdp123456

Identifiers with the app password =

Login: [exemple@exemple.fr](mailto:exemple@exemple.fr)

password: apppassword123456

## 11. Non-reception of internal user emails

Context: In certain cases, the tenant user does not receive any emails coming from the same domain as theirs and that are directly addressed to them, but they do receive external emails or emails they are copied into.

To correct this, you must apply the following Powershell steps, connected to your Office 365/Exchange:

Retrieve the 'TransportConfig' settings to see the settings for JournalingReportNdrTo

Get-TransportConfig | fl JournalingReportNdrTo\*

Then force the value of the email delivery, by changing the value of this attribute.

Set-TransportConfig – JournalingReportNdrTo "<>"

At this stage, you must wait one hour or two for the modification to really be taken into account.

You can do the test: write to the person concerned directly with the person as the only addressee.

Microsoft sources:

<https://support.microsoft.com/en-us/help/2829319/transport-and-mailbox-rules-in-exchange-online-or-in-on-premises-excha>

## 12. Memento – important information

Here you can find all the important information for the annex operations.

- User type for creating the connector & rules on Exchange Online:

Exchange Administrator

- SPF value to include in your existing SPF

Include: spfcloud.letsignit.com

- The Letsignit server DNS value to point to when sending your emails

Isicloud-smtp.letsignit.com

- Letsignit IP seen when email is returned (once passed through Letsignit)

40.66.63.89, 40.66.63.90, and 40.66.63.91 for EMEA

52.226.140.66, 104.45.169.33, 40.90.242.172, 52.226.140.254, 52.185.66.245 and 13.86.124.154 for US east and central