

Manual Integration with Office 365

Scope

Office 365 Integration can work in manual mode and automated mode.

In automated mode, you only need to approve the app in the Office 365 app-store on your portal and all configuration changes are applied. Additionally, any changes made to the Office 365 policies on your portal, will be automatically reflected on the Office 365 environment.

In manual mode, no changes are applied to the Office 365 environment and those changes need to be implemented manually. Furthermore, any change to the Office 365 policies on your portal, should be implemented manually on the Mail-Flow rules which are described in step #3.

This document will help you understand the interaction with Office 365 in three scenarios:

1. You want to choose automated mode but first want to learn the configuration changes that will be automatically applied to Office 365
2. You want to choose manual mode and need to know what the initial configuration should be
3. You are already in monitor mode and moving to inline mode (In this case jump to Step-2 and Step-3) or already in inline mode but changing the scope of the policy – users or groups it applies to (In this case jump to Step-3)

Note that in some configurations we refer to {portal}, this is an indication of your portal name. For example, if your portal is customer-x.checkpoint.net, then you will need to replace '{portal}' with 'customer-x'.

Finally, if you are not sure and about to apply these changes for the first time, please contact support and we will assist you in the configuration.

Step-1: Journal Rule

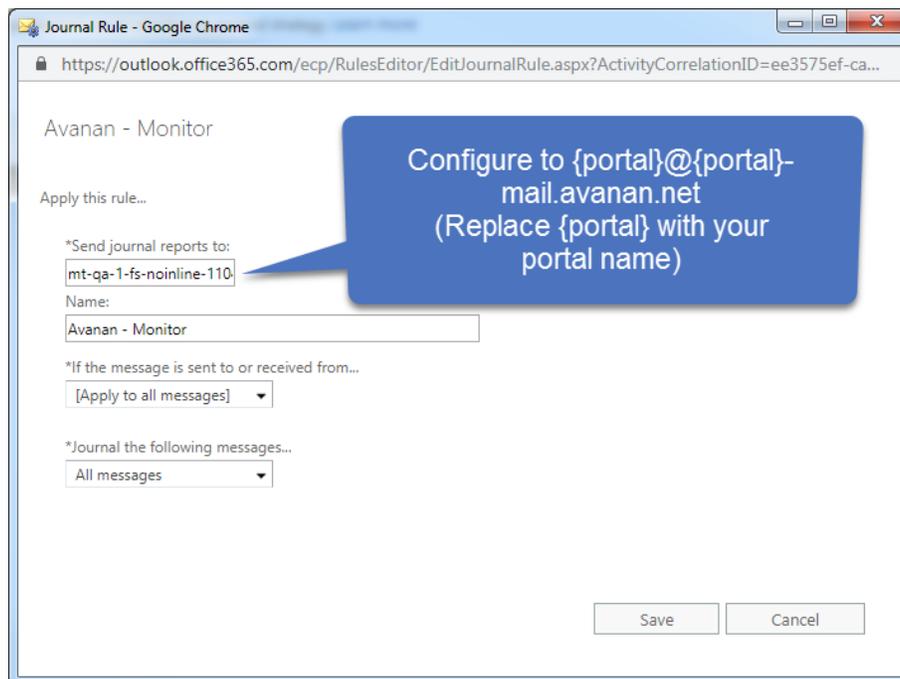
The journal rule is used for the monitoring mode. The journal rule configures Office 365 to send all emails to the system.

Note:

Before you create a journal rule, you must specify an account to receive journal reports that can't be delivered to the journal destination.

Please follow [these steps](#) to configure this mailbox.

1. The journal rule should be configured as follows:



Journal Rule - Google Chrome

https://outlook.office365.com/ecp/RulesEditor/EditJournalRule.aspx?ActivityCorrelationID=ee3575ef-ca...

Avanan - Monitor

Apply this rule...

*Send journal reports to:

Name:

*If the message is sent to or received from...

*Journal the following messages...

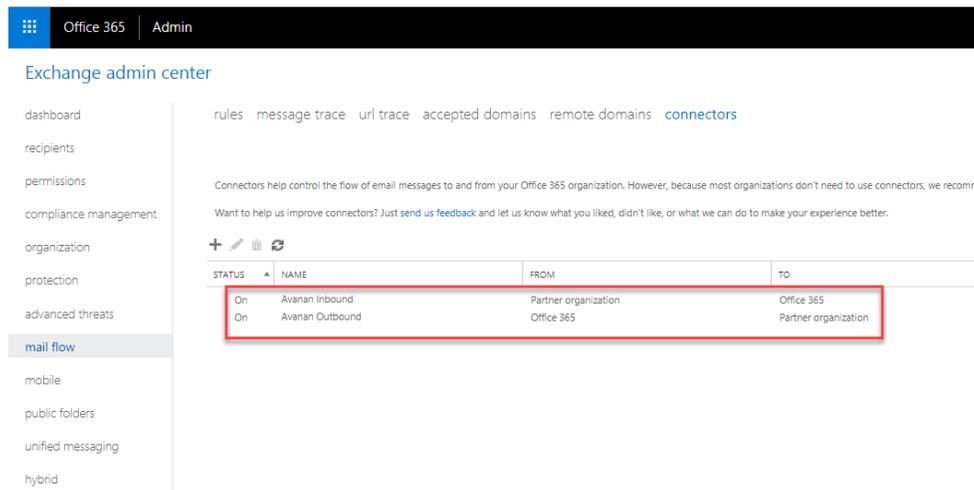
Save Cancel

Configure to {portal}@{portal}-mail.avanan.net
 (Replace {portal} with your portal name)

Step-2: Connectors

First Inbound connector is used to for the monitoring mode. Second Outbound connector and following step-3, are relevant only once you are ready to move to inline mode.

In step-2 you will define the inbound and outbound connectors that sends traffic to and receives traffic from the cloud. Under “Connectors”, you should have two connectors:

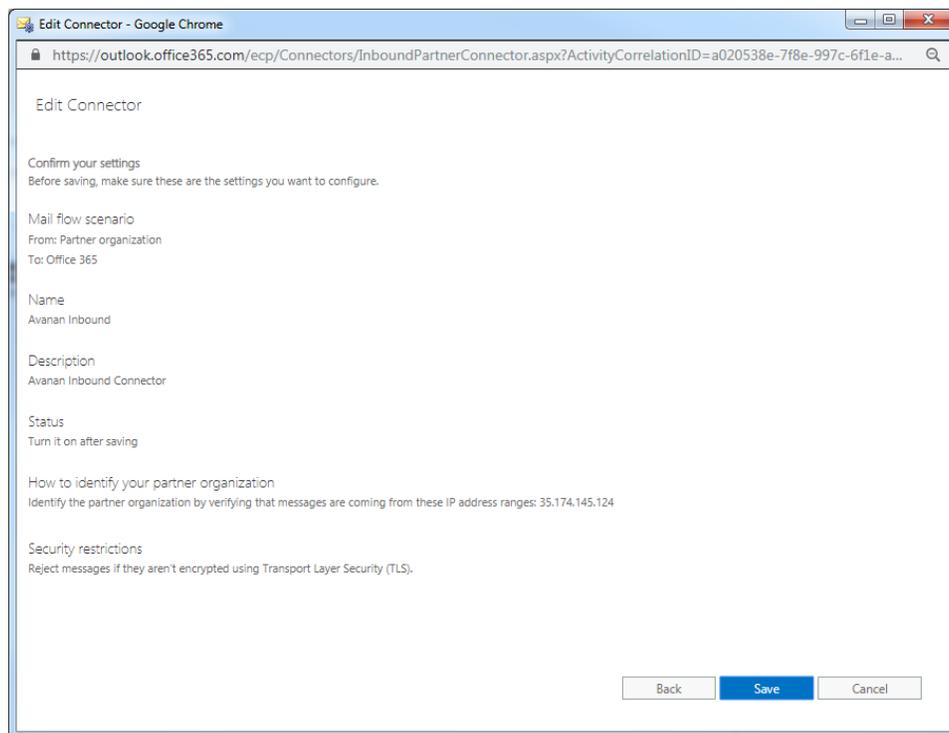


The screenshot shows the Exchange Admin Center interface. The top navigation bar includes 'Office 365' and 'Admin'. The left sidebar lists various management areas, with 'mail flow' selected. The main content area is titled 'Exchange admin center' and 'connectors'. It contains a table of connectors with the following data:

| STATUS | NAME | FROM | TO |
|--------|-----------------|----------------------|----------------------|
| On | Avanan Inbound | Partner organization | Office 365 |
| On | Avanan Outbound | Office 365 | Partner organization |

Create the two connectors based on the following configuration.

2. "Avanan Inbound" – should be configured as follows:



Edit Connector - Google Chrome

https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx?ActivityCorrelationID=a020538e-7f8e-997c-6f1e-a...

Edit Connector

Confirm your settings
Before saving, make sure these are the settings you want to configure.

Mail flow scenario
From: Partner organization
To: Office 365

Name
Avanan Inbound

Description
Avanan Inbound Connector

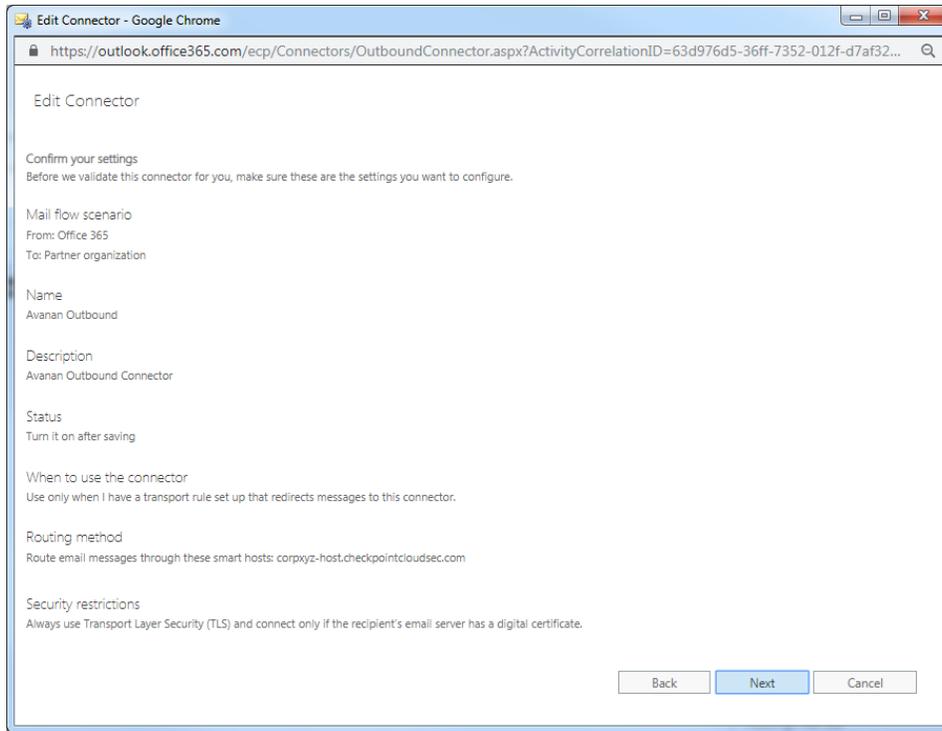
Status
Turn it on after saving

How to identify your partner organization
Identify the partner organization by verifying that messages are coming from these IP address ranges: 35.174.145.124

Security restrictions
Reject messages if they aren't encrypted using Transport Layer Security (TLS).

Back Save Cancel

3. "Avanan Outbound" – should be configured as follows:



Edit Connector - Google Chrome
https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ActivityCorrelationID=63d976d5-36ff-7352-012f-d7af32...

Edit Connector

Confirm your settings
Before we validate this connector for you, make sure these are the settings you want to configure.

Mail flow scenario
From: Office 365
To: Partner organization

Name
Avanan Outbound

Description
Avanan Outbound Connector

Status
Turn it on after saving

When to use the connector
Use only when I have a transport rule set up that redirects messages to this connector.

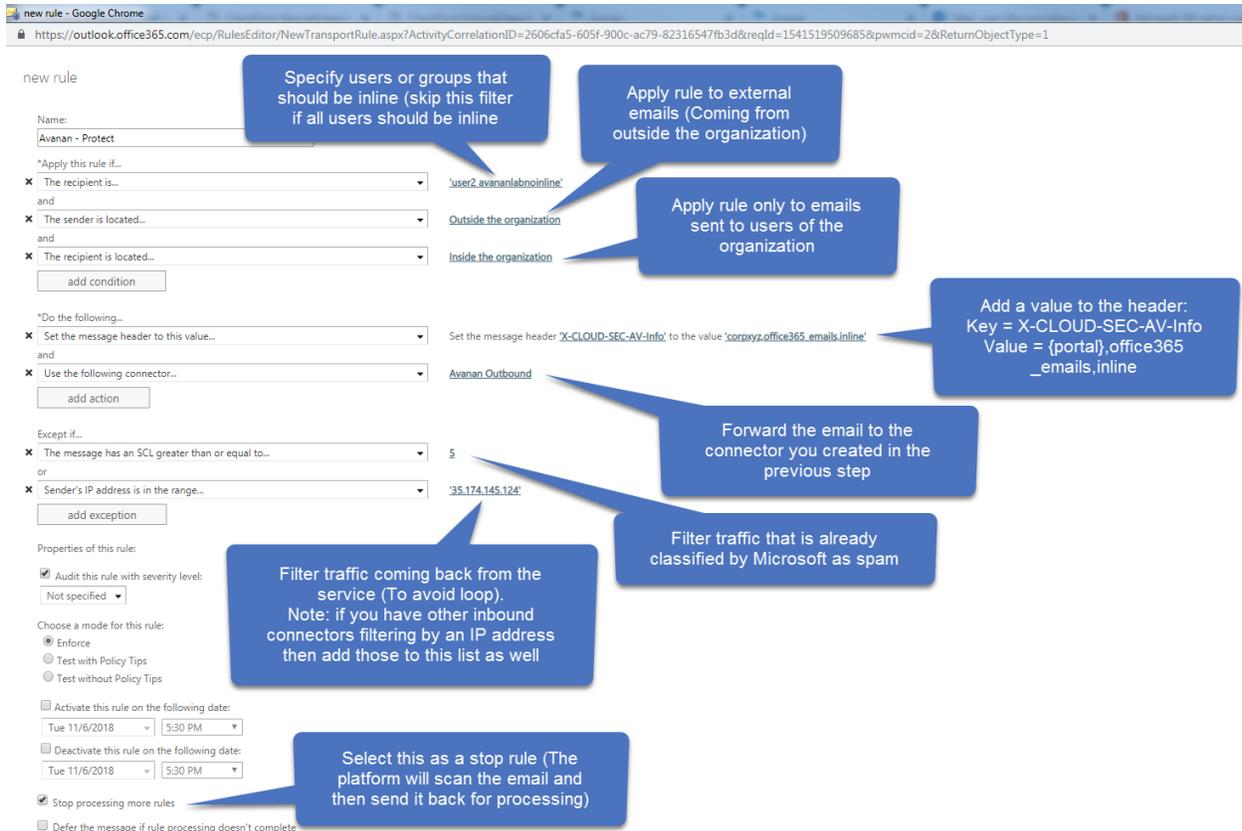
Routing method
Route email messages through these smart hosts: corpxyz-host.checkpointcloudsec.com

Security restrictions
Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

Step-3: Mail-flow Rule

The purpose of the mail-flow rule is to implement the inline mode for the users that need to be inline. Every time you change the scope of the inline policy (Add or remove users/groups) you will need to edit the section “Apply this rule if... The recipient is ...”

4. Create “Checkpoint – Protect” rule as the first mail-flow rule with the following configurations



Apply this rule if...

- The recipient is... `'user2.avananlab@online'`
 - Specify users or groups that should be inline (skip this filter if all users should be inline)
- and
- The sender is located... `Outside the organization`
 - Apply rule to external emails (Coming from outside the organization)
- and
- The recipient is located... `Inside the organization`
 - Apply rule only to emails sent to users of the organization

Do the following...

- Set the message header to this value... Set the message header 'X-CLOUD-SEC-AV-Info' to the value 'corxyz.office365_emails.inline'
 - Add a value to the header: Key = X-CLOUD-SEC-AV-Info Value = {portal},office365_emails,inline
- and
- Use the following connector... `Avanan Outbound`
 - Forward the email to the connector you created in the previous step

Except if...

- The message has an SCL greater than or equal to... `$`
 - Filter traffic that is already classified by Microsoft as spam
- or
- Sender's IP address is in the range... `'35.174.145.124'`
 - Filter traffic coming back from the service (To avoid loop). Note: if you have other inbound connectors filtering by an IP address then add those to this list as well

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 11/6/2018 5:30 PM
- Deactivate this rule on the following date: Tue 11/6/2018 5:30 PM
- Stop processing more rules
 - Select this as a stop rule (The platform will scan the email and then send it back for processing)
- Defer the message if rule processing doesn't complete