Bypassing External Mail Forwarding Restrictions with Power Automate

written by Karl Fosaaen | June 25, 2020

During a recent Office 365 assessment, we ran into an interesting situation where Exchange was configured to disallow any external domain forwarding rules. This configuration is intended to prevent attackers from compromising an account and setting up forwarding for remote mail access and persistence. Part of this assessment was to validate that these configurations were properly implemented, and also to look for potential bypasses for this configuration.

Power Automate

As part of the Office 365 environment, we had access to the Power Automate application. Formerly known as Microsoft Flow, Power Automate is a framework for gluing together multiple services for automation tasks within Office 365.

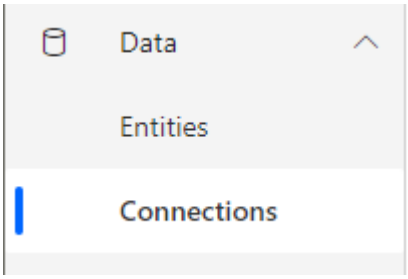
Want to get an email every time someone uploads a file to your shared OneDrive folder? Connect Outlook and OneDrive in Power Automate and set up a flow. I like to think of it as IFTTT for the Microsoft ecosystem.

Forwarding Email

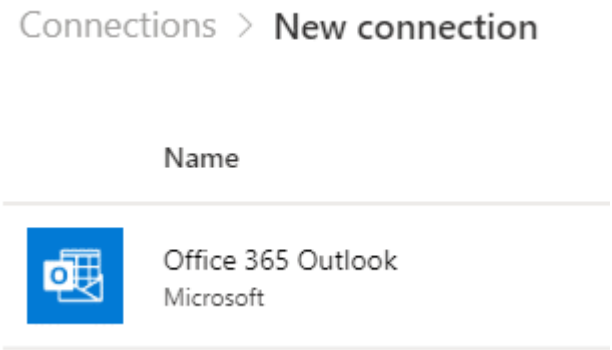
Since we were able to create connections and flows in Power Automate, we decided to connect Power Automate to Office 365 Outlook and create a flow for forwarding email to a NetSPI email address.

You can use the following process to set up external mail forwarding with Power Automate:

1. Under the Data menu, select “Connections”.

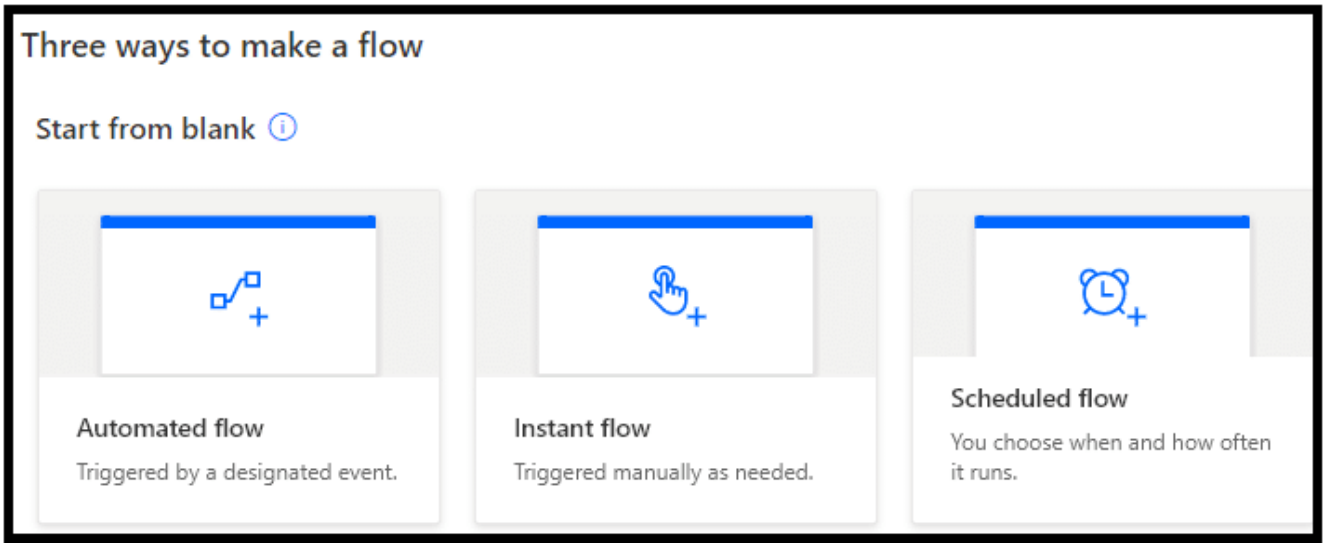


2. Select “New Connection” at the top of the window, and find the “Office 365 Outlook” connection.

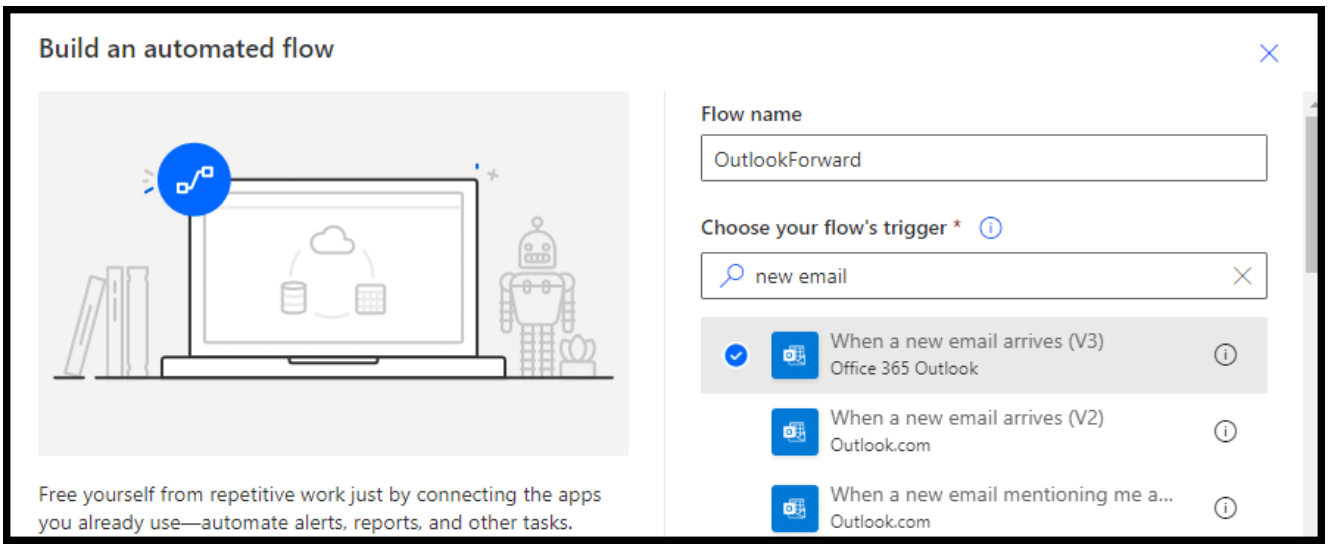


3. Select “Create” on the connection and authorize the connection under the OAuth pop-up.

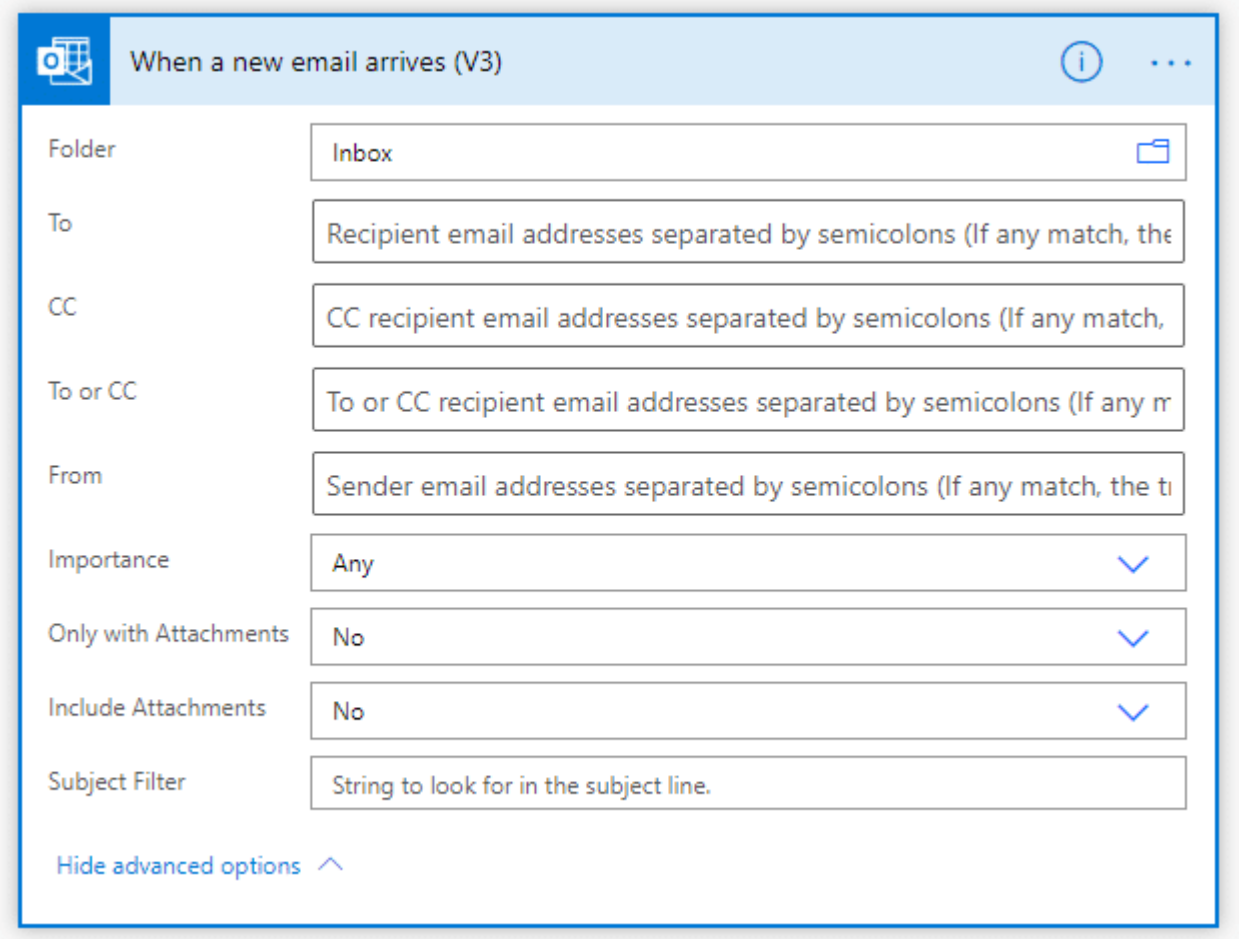
4. Navigate to the “Create” section from the left navigation menu, and select “Automated flow”.



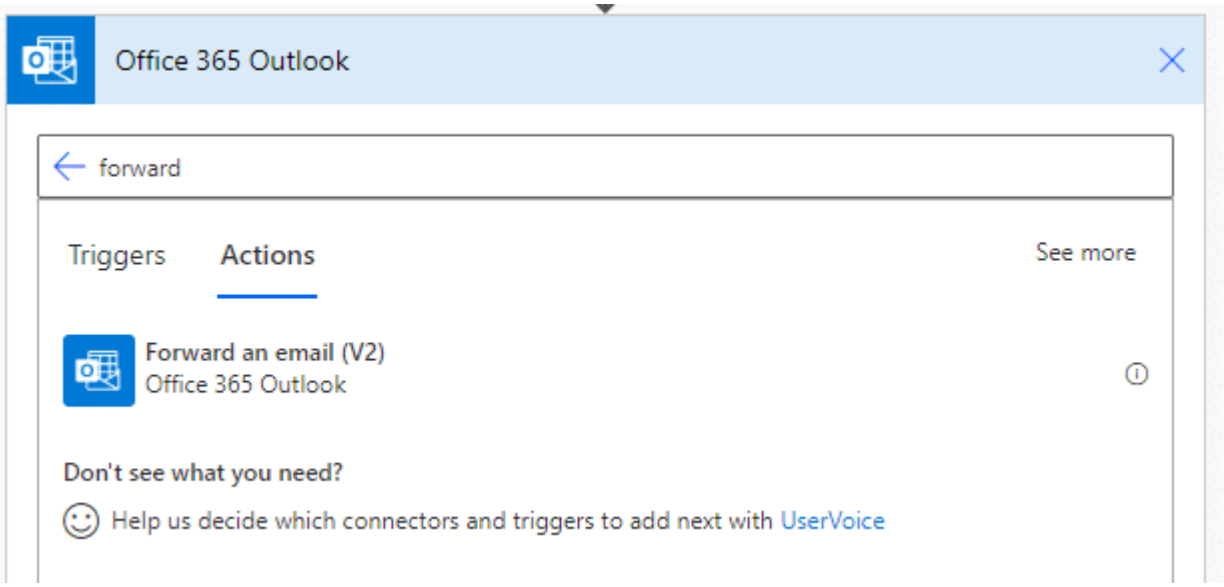
5. Name the flow (OutlookForward) and search for the “When a new email arrives (V3)” Office 365 Outlook trigger.



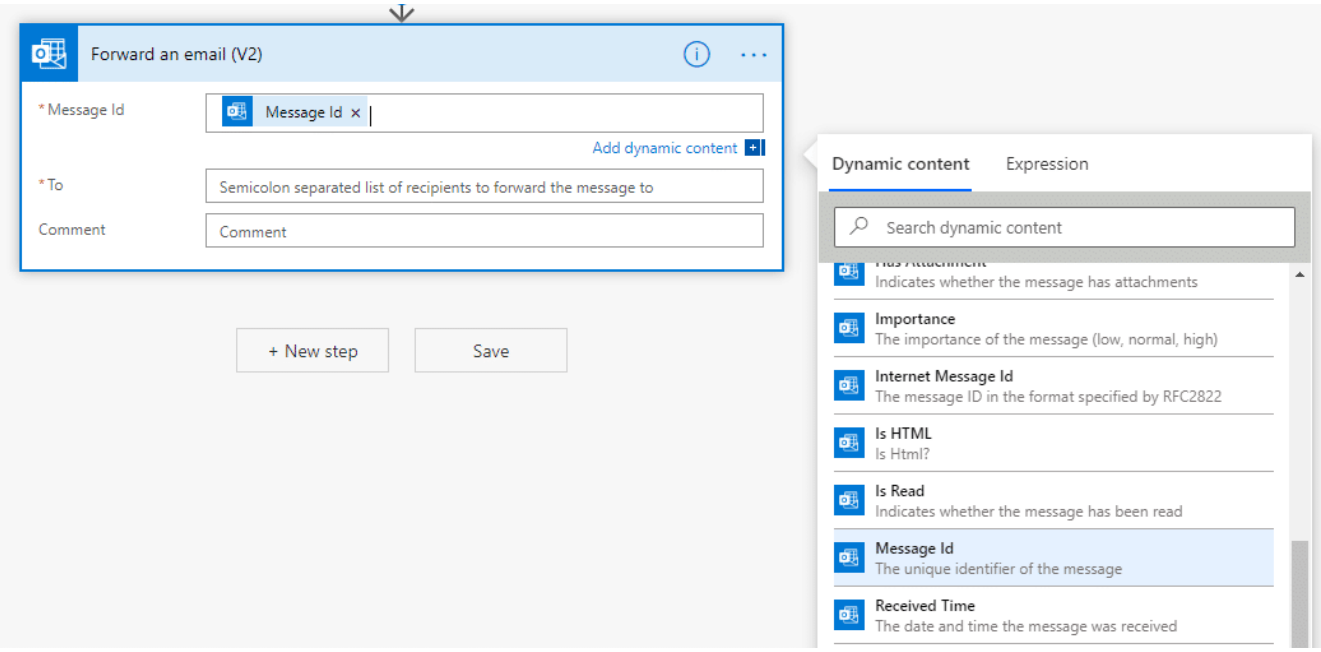
6. Select any advanced options and add a new step.



7. In the added step, search for the Office 365 Outlook connection, and find the “Forward an email (V2)” action.

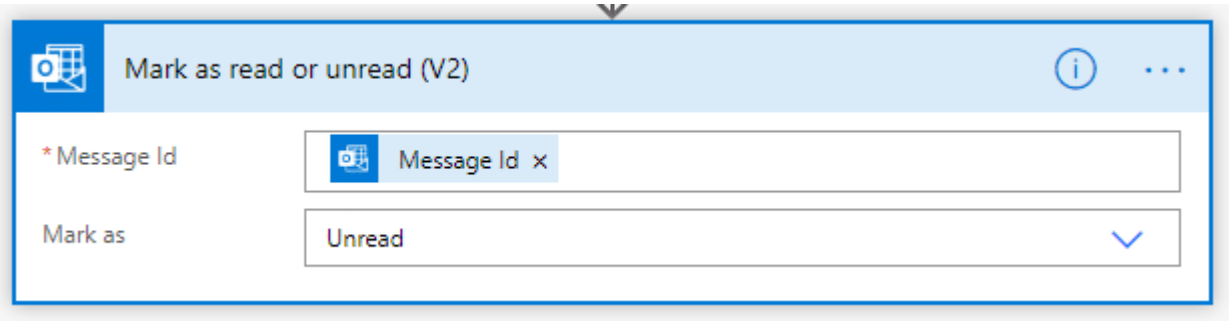


8. From the “Add dynamic content” link, find “Message Id” and select it for the Message Id.



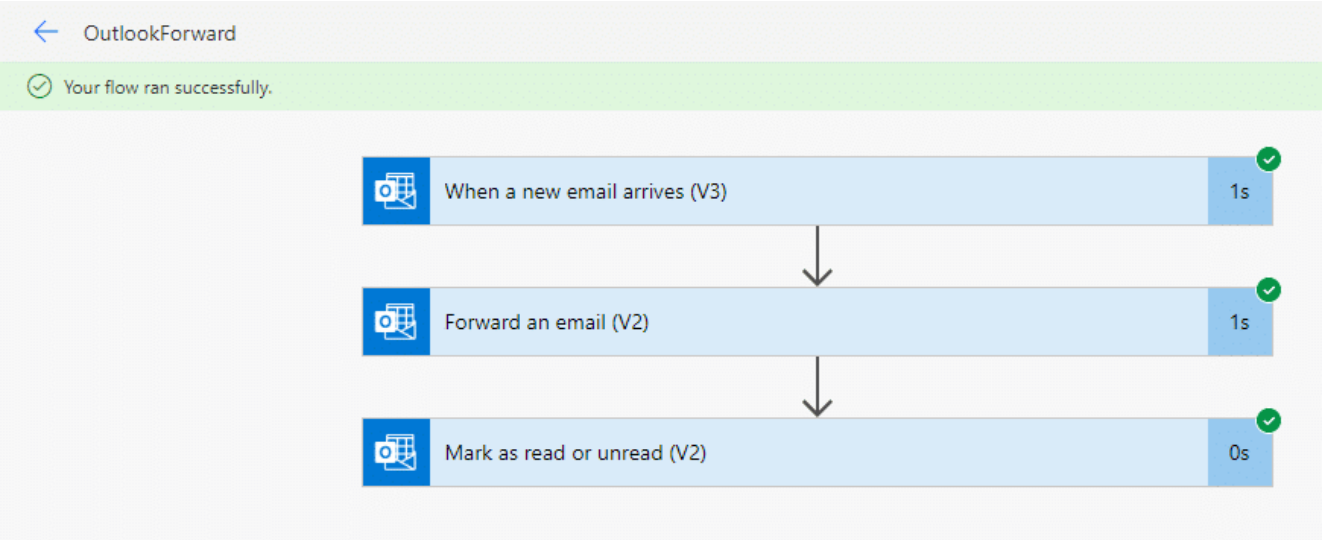
9. Set your “To” address to the email address that you’d like to forward the message to.

10. Optional, but really recommended – Add one more step “Mark as read or unread (V2)” from the Office 365 Outlook connection, and mark the message as Unread. This will hopefully make the forwarding activity less obvious to the compromised account.



11. Save the flow and wait for the emails to start coming in.

You can also test the flow in the editor. It should look like this:



Taking it further

While forwarding email to an external account is handy, it may not accomplish the goal that we're going for.

Here are a few more ideas for interesting things that could be done with Power Automate:

- Use "Office 365 Users – Search for users (V2)" to do domain user enumeration
    - Export the results to an Excel file stored in OneDrive
- Use the enumerated users list as targets for an email phishing message, sent from the compromised account
    - Watch an inbox for the template message, use the message body as your phishing email

- Connect “OneDrive for Business” and an external file storage provider (Dropbox/SFTP/Google Drive) to mirror each other
    - When a file is created or modified, copy it to Dropbox
- Connect Azure AD with an admin account to create a new user
    - Trigger the flow with an email to help with persistence.

Fixing the Issue

It looks like it is possible to disable Power Automate for users, but you may have legitimate reasons for using it. Alternatively, Microsoft Flow audit events are available in the Office365 Security & Compliance center, so you can at least log and alert on the creation of new flow.

For anyone looking to map these activities back to the Mitre ATT&CK framework, check out these links:

- https://attack.mitre.org/beta/techniques/T1087/003
- https://attack.mitre.org/beta/techniques/T1114
- https://attack.mitre.org/beta/techniques/T1114/001
- https://attack.mitre.org/beta/techniques/T1114/002
- https://attack.mitre.org/beta/techniques/T1114/003

Prior Work

Some related prior Microsoft Flow related research was presented at DerbyCon in 2019 by Trent Lo – https://www.youtube.com/watch?v=80xUTJPlhZc