How to Configure Microsoft 365 Outbound Automatic Replies

https://campus.barracuda.com/doc/96022969/

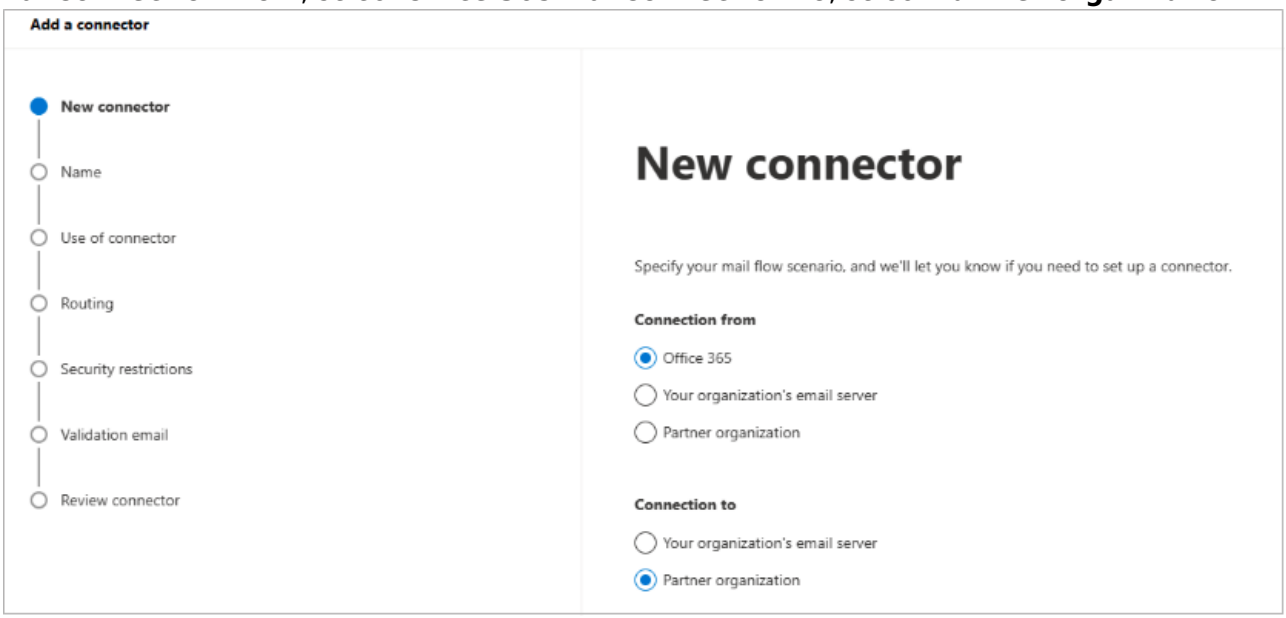
Use the steps in this article to configure outbound automatic replies that do not have an Envelope-From address or have an Envelope-From domain not in Email Gateway Defense (such as `onmicrosoft.com`) . This ensures that relayed mail and mail without an Envelope-From is sent directly to the internet bypassing Email Gateway Defense.

Note that if you are using a 3rd party signature service, such as CodeTwo or Exclaimer Cloud, click **Stop processing more rules** in your mail flow rule for your signature service. This will ensure that your mail will have the signatures applied.

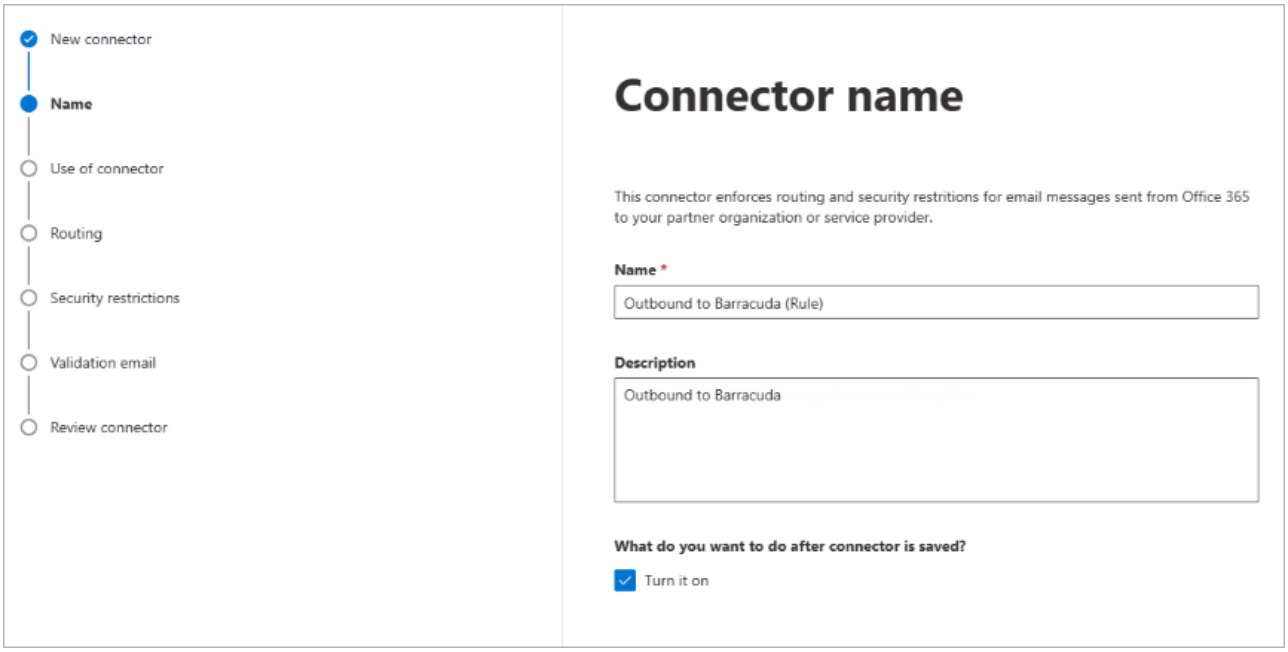
Step 1. Create the Connector

Note that the following steps use the new Exchange admin center user interface.

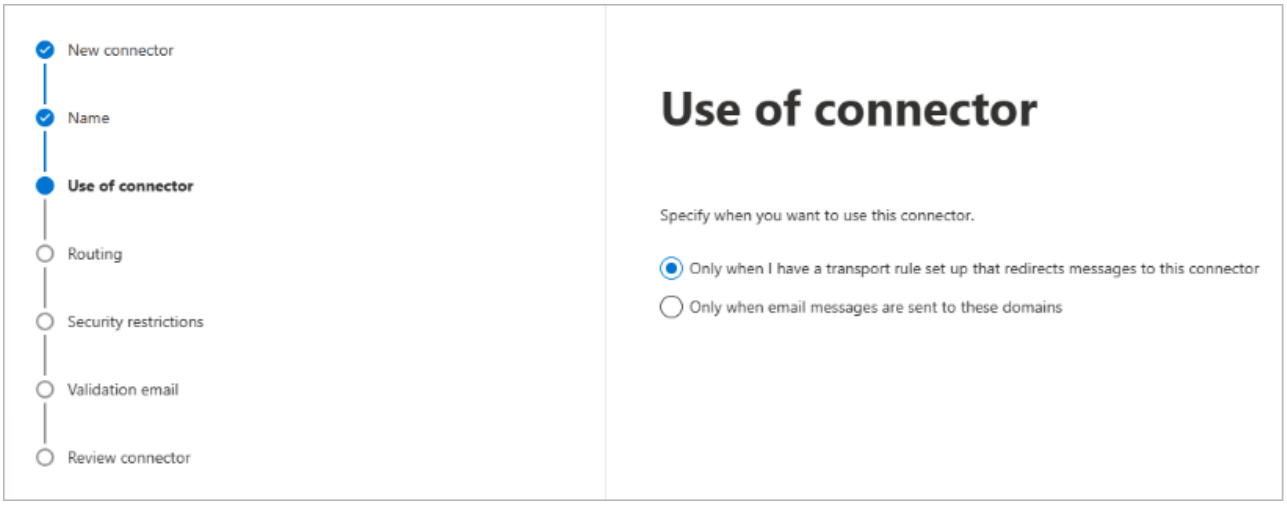
1. Log into the Microsoft 365 admin center https://admin.exchange.microsoft.com/.
2. In the left pane, click **Mail flow**, and click **Connectors**.
3. Click the **Add a connector** button, and use the wizard to create a new connector.
4. For **Connection from**, select **Office 365**. For **Connection to**, select **Partner organization**.



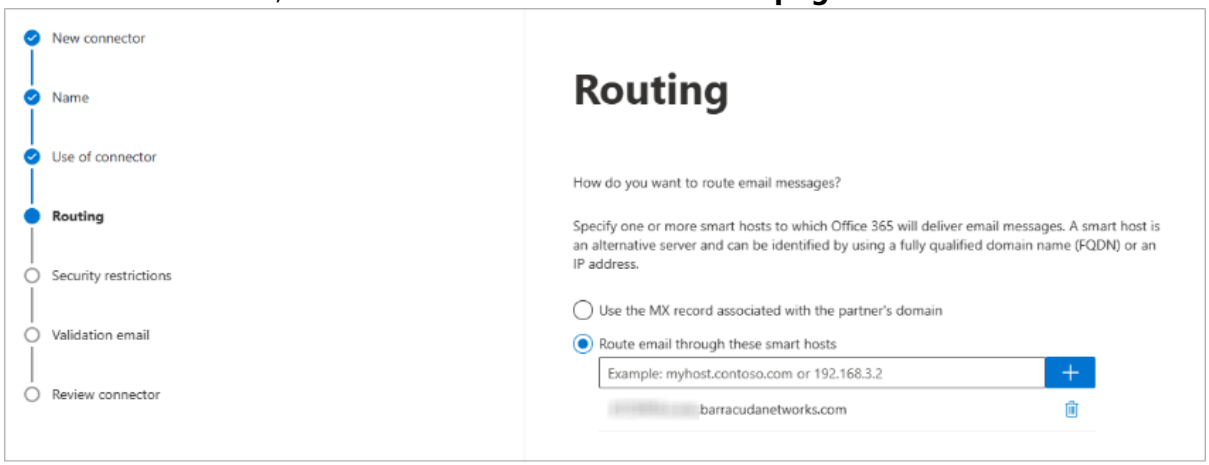
5. Click **Next**. Enter a **Name** and (optional) **Description** to identify the connector:



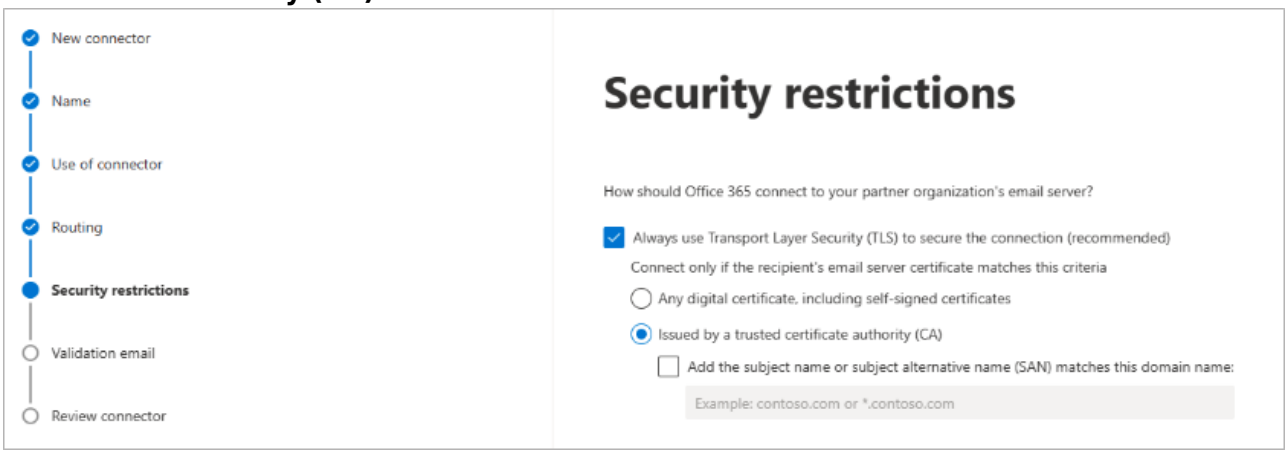
6. Click **Next**. Select **Only when I have a transport rule set up that redirects messages to this connector.**



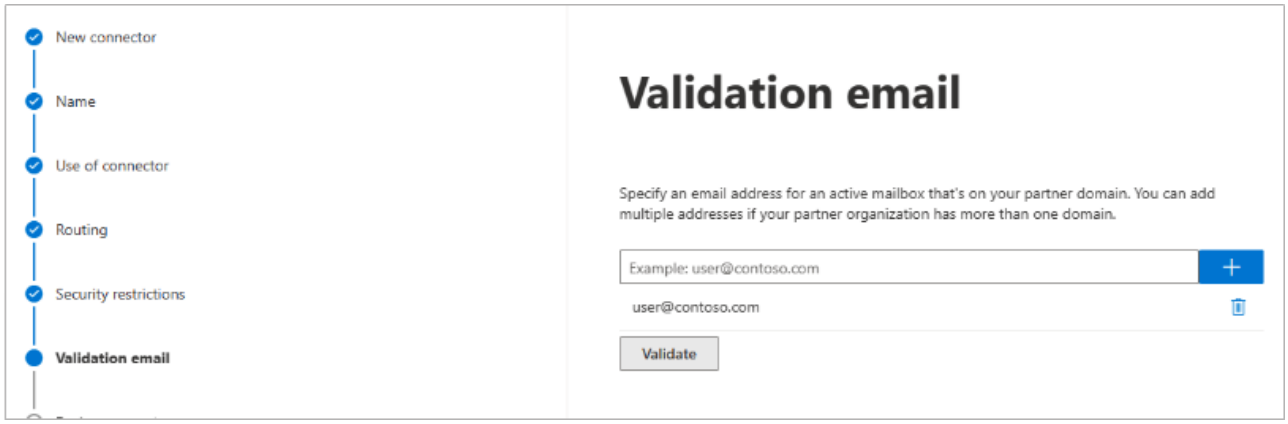
7. Click **Next**. Select **Route email through these smart host**, and click the **+** symbol.
    1. Go to Email Gateway Defense, and click the **Domains** tab. Copy your outbound hostname from the MX records, and enter it in the **add smart host page**:



8. Click **Next**. Use the default settings for the **Security restrictions:Always use Transport Layer Security (TLS) to secure the connection (recommended) > Issues by Trusted certificate authority (CA)**:



9. Enter an external email address to validate the connector. For this test, it is important to use an email address from *outside your organization* , like a gmail or yahoo email address.
   Click **Validate**.
   There are two parts of the validation:
   1. **Test Connectivity** – If this test fails, Outbound Groups is not enabled. Contact Barracuda Networks Technical Support and request that Outbound Groups be enabled on your Email Gateway Defense account.
   2. **Send Test Email** – If the test fails, there is no cause for concern. The test email comes from a Microsoft domain, not from your domain, so it is rejected. If you changed your domain away from `onmicrosoft.com`, the test should work. Note that you might still receive the email even if the test failed.

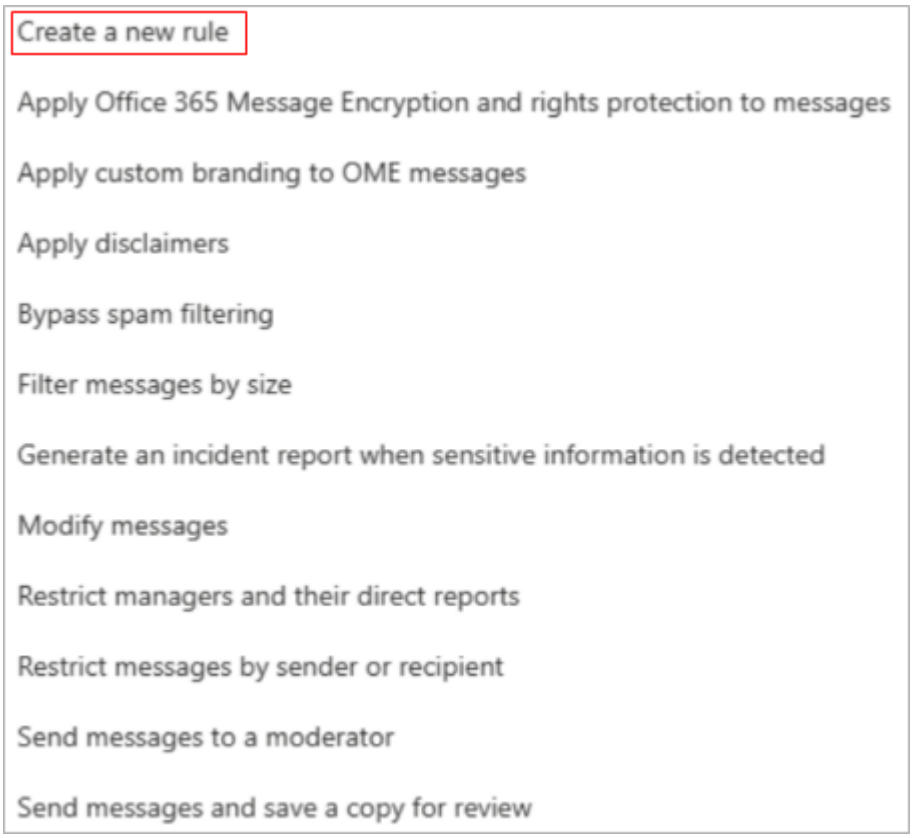


10. Once the validation process is complete, click **Next**. Review your settings and then click **Create connector**.

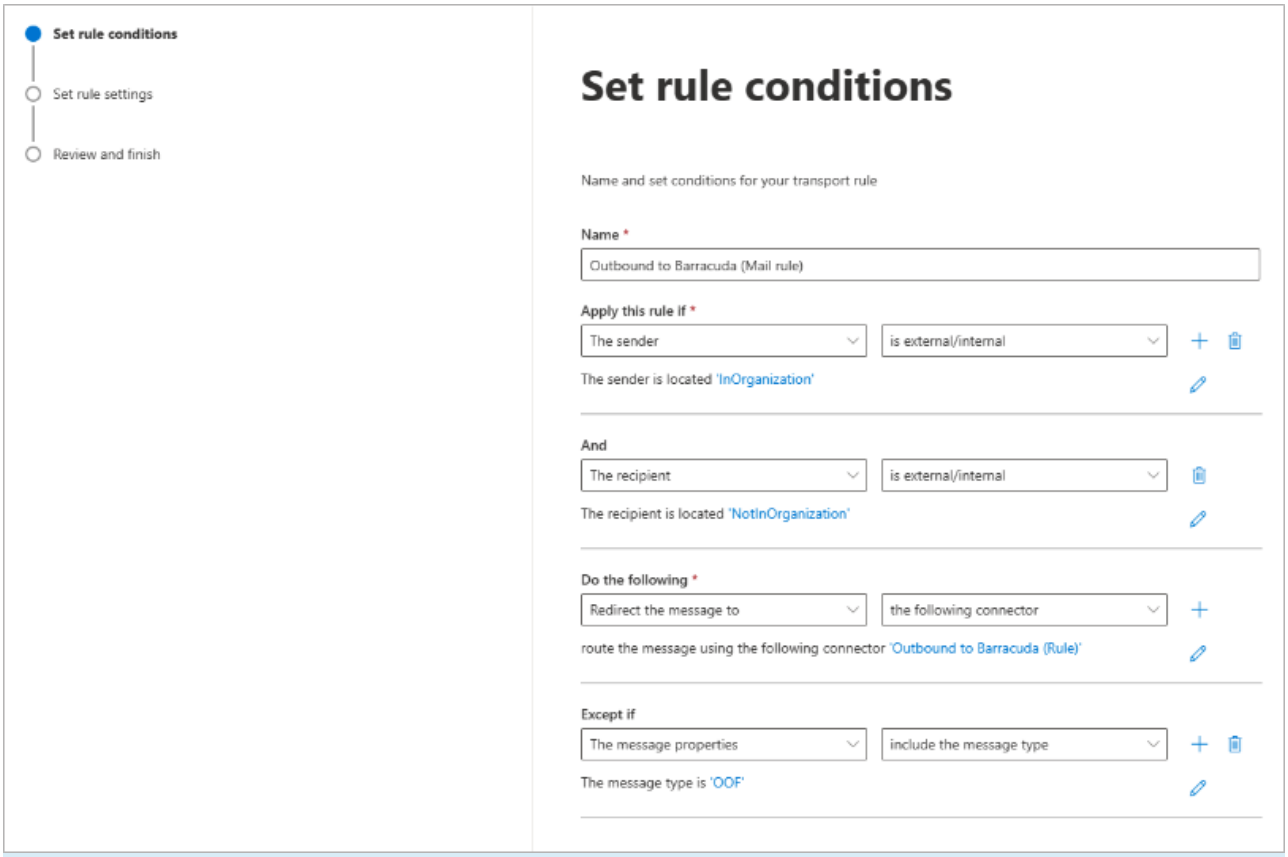
Step 2. Create Transport Rule

1. Log into the Microsoft 365 admin center https://admin.exchange.microsoft.com/.
2. In the left pane, click **mail flow**, and click **rules**.
3. Click **Add a rule**.

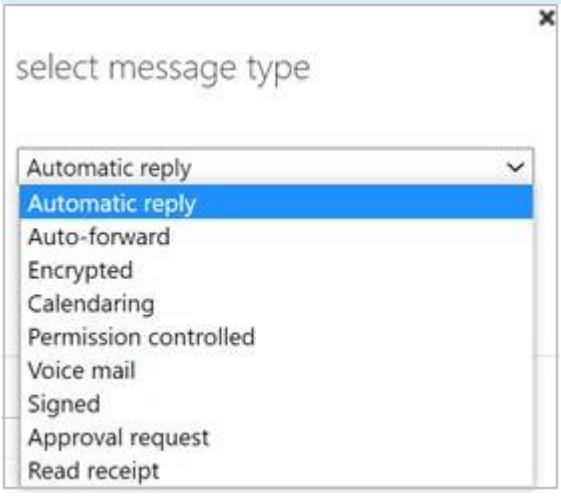
4. Select **Create a new rule**.



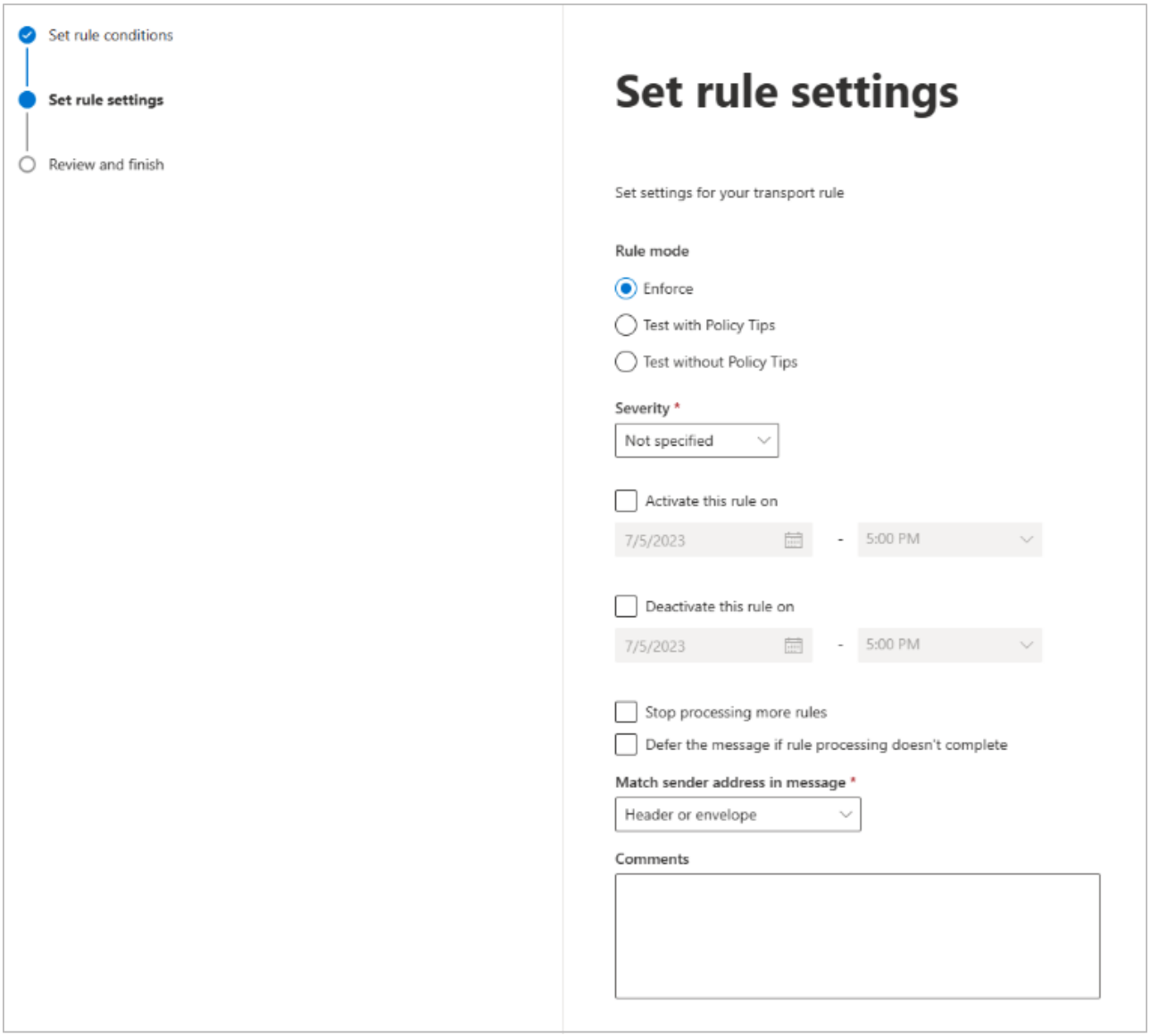
5. In the **new rule** page, enter a **Name** to represent the rule.
6. Under **Apply this if**, select **The sender > is external/internal > Inside the organization**.
7. Click the + to add a new condition.
8. From the drop-down menu, select **The recipient > is external/internal > Outside the organization**.
9. Under **Do the following**, select **Redirect the message to > the following connector**, and select the connector you defined above in *Step 1. Create the Connector.*
10. Under **Except if**, select **The message properties > include the message type > Automatic reply**.



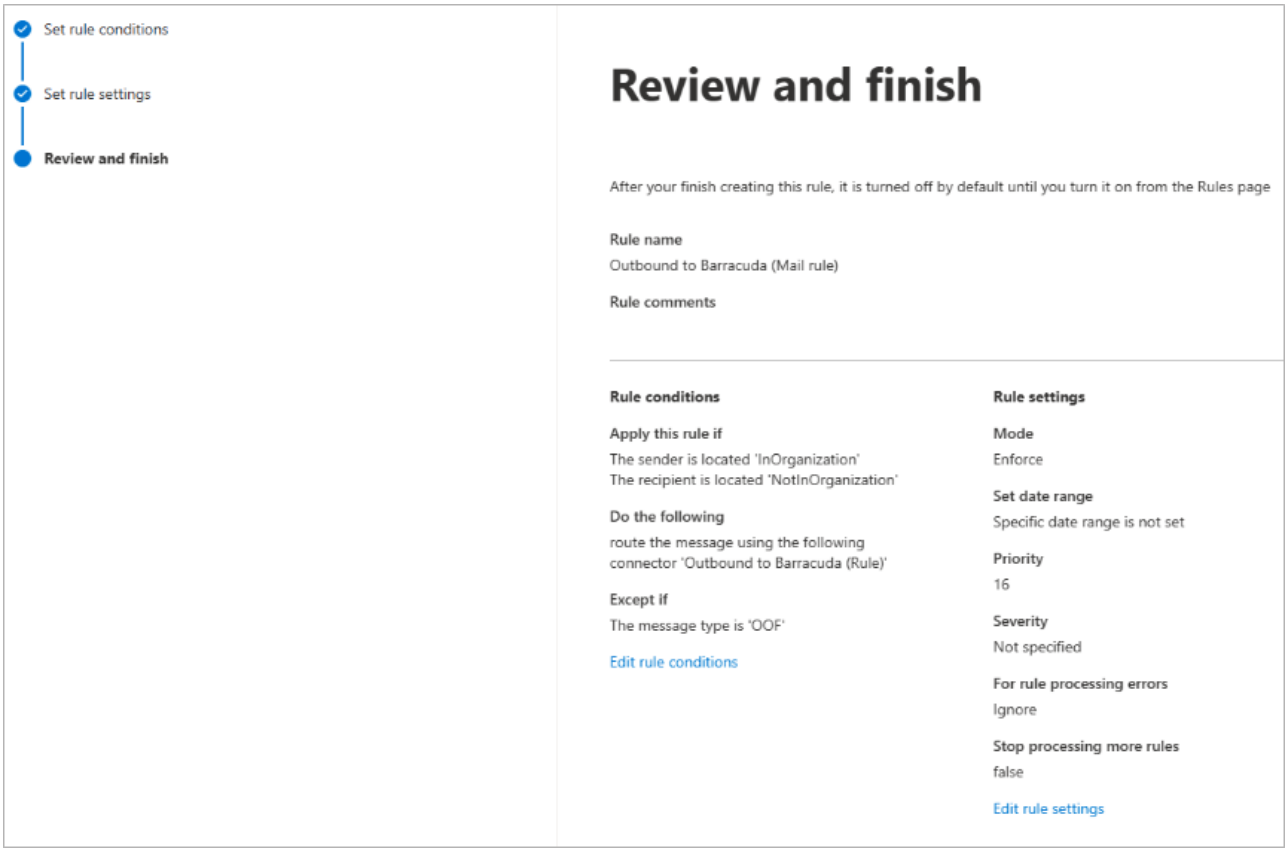
You can only set one message type exception per rule. You must create multiple mail flow rules for different message types, for example, one for **Automatic reply** and one for **Auto-forward**.



11. Click **Next**.
12. Under **Match sender address in message**, select **Header or envelope**.



13. Click **Next**.
14. Review the settings and then click **Finish**.



Step 3. Disable Existing Barracuda Networks Send Connector

1. Log into the Microsoft 365 admin center https://admin.exchange.microsoft.com/.
2. In the left pane, click **mail flow**, and click **connectors**.
3. Select the send connector you created during Step 2 - Configure Microsoft 365 for Inbound and Outbound Mail, *Step 7. Configure Outbound Mail* section.
4. Disable the send connector.

Your system will now use the new send connector you created in Step 1 above.

Figures

1. ms_newConnector.png
2. ms_ConnectorName1.png
3. ms_UseofConnector.png
4. ms_ConnectorRouting.png
5. ms_SecurityRestrictions1.png
6. ms_validateEmail1.png
7. ms_CreateNewRule.png
8. ms_ruleConditions.png
9. messageType01.png
10. ms_ruleSettings.png
11. ms_ruleReview.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.