

How to Configure Office 365 Outbound Automatic Replies

<https://campus.barracuda.com/doc/93880353/>

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 the Barracuda Email Security Service (such as onmicrosoft.com). This ensures that relayed mail and mail without an Envelope-From is sent directly to the internet bypassing the Barracuda Email Security Service.

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 Office 365 admin center.
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**.

New connector

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

Connection from

☒ Office 365

☐ Your organization's email server

☐ Partner organization

Connection to

☐ Your organization's email server

☒ Partner organization

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

Connector name

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

Name *

Outbound to BESS

Description

Route Outbound mail to Barracuda

What do you want to do after connector is saved?



Turn it on

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

Use of connector

Specify when you want to use this connector.



Only when I have a transport rule set up that redirects messages to this connector



Only when email messages are sent to these domains

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



*



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

Routing

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.

☐ Use the MX record associated with the partner's domain

☒ Route email through these smart hosts

Example: myhost.contoso.com or 192.168.3.2



d123456@ess.barracudanetworks.com



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)**:

Security restrictions

How should Office 365 connect to your partner organization's 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:

Example: contoso.com or *.contoso.com

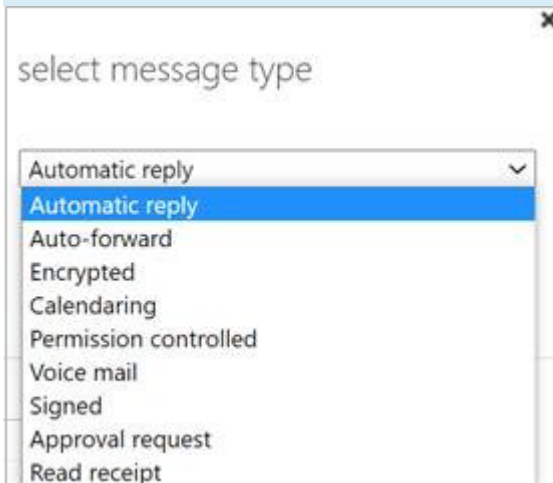
9. Click **Next**. In the confirmation page, verify your settings and click **Next**. Office 365 runs a test to verify your settings.
10. When the verification page displays, enter a test email address, and click **Validate**. Once the verification is complete, your mail flow settings are added.

Step 2. Create Transport Rule

1. Log into the Office 365 admin center, and go to **Admin centers > Exchange**.
2. In the left pane, click **mail flow**, and click **rules**.
3. Click the + symbol, and click **Create new rule**.

4. In the **new rule** page, enter a **Name** to represent the rule.
5. Click **more options** towards the bottom of the page.
6. From the **Apply this rule** drop-down menu, select **The sender is located > is external/internal > Inside the organization**.
7. Click **Add Condition**. From the drop-down menu, select **The recipient is located > is external/internal > Outside the organization**.
8. From the **Do the following** drop-down menu, select **Redirect the message to > the following connector**, and select the connector you defined above in *Step 1. Create the Connector*.
9. Click **Ok**.
10. Click **Add Exception**. From the drop-down menu, 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 **Save**.

new rule

Name:

*Apply this rule if...

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

and

✕ The recipient is located... [Outside the organization](#)

*Do the following...

Use the following connector... [Outbound \(selected domain\)](#)

Except if...

✕ The message type is... [Automatic reply](#)

Step 3. Disable Existing Barracuda Send Connector

1. Log into the Office 365 admin center.
2. In the left pane, click **Mail flow**, and click **Connectors**.
3. Select the send connector you created during [Step 2 - Configure Office 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. new_connector.png
2. connector_name.png
3. connector_use1.png
4. connector_routing1.png
5. connector_security_restrictions.png
6. messageType01.png
7. oooRule01.png

© Barracuda Networks Inc., 2024 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.