

How to Configure Office 365 to Scan Only Selected Domains Outbound

<https://campus.barracuda.com/doc/53675549/>

If you make setting changes, allow a few minutes for the changes to take effect.

Use the steps in this article if you have multiple domains within your Office 365 tenant and you want to scan only certain domains outbound.

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 on your outbound hostname:

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



@123456.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) > Issued 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:

Review connector

Mail flow scenario

From: Office 365

To: Partner organization

Name

Outbound to BESS

Status

Turn it on after saving

[Edit name](#)

Use of connector

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

[Edit use](#)

Routing

Route email messages through these smart hosts: @123456@ess.barracudanetworks.com

[Edit routing](#)

Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server certificate is issued by a trusted certificate authority (CA).

[Edit restrictions](#)

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**.
8. From the drop-down menu, select **The sender's domain is...**
9. Enter the domains you want to route through the Barracuda Email Security Service.
10. From the **Do the following** drop-down menu, select **Redirect the message to... > the following connector**, and select the connector you defined in *Step 1. Create the Connector*.
11. Click **Add Exception**.
12. From the drop-down menu, select **The Recipient is located > is external/internal > Inside the organization**.
13. Towards the bottom, from the **Match sender address in message** drop-down menu, select **Header or envelope**.
14. Click **Save**.

<Rule Name>

Name:

*Apply this rule if...

☒ The sender is located...

and

☒ The sender's domain is...

*Do the following...

Except if...

☒ The recipient is located...

Properties of this rule:

Priority:

☒ Audit this rule with severity level:

Choose a mode for this rule:

☒ Enforce
☐ Test with Policy Tips
☐ Test without Policy Tips

☐ Activate this rule on the following date:

☐ Deactivate this rule on the following date:

☐ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message:

Figures

1. new_connector.png
2. connector_name.png
3. connector_use1.png
4. connector_routing.png
5. connector_security_restrictions.png
6. connector_review1.png
7. transport_Rule.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.