

How to Configure Microsoft 365 to Scan Only Selected Domains Outbound

https://campus.barracuda.com/doc/96022966/

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 Microsoft 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 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.

Add a connector	
New connector	
O Name	New connector
Use of connector	Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
O Routing	Connection from
Security restrictions	Office 365 Your organization's email server
Validation email	O Partner organization
O Review connector	Connection to O Your organization's email server
	Partner organization

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



Name	Connector name
Use of connector	
Routing	This connector enforces routing and security restritions for email messages sent from Office 3 to your partner organization or service provider.
	Name *
Security restrictions	Outbound to Barracuda (Rule)
> Validation email	Description
	Outbound to Barracuda
Review connector	
	What do you want to do after connector is saved?
	V Turn it on

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

•	New connector	
0	Name	Use of connector
	Use of connector	
0	Routing	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
	Security restrictions	
	Validation email	
0	Review 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**:

New connector	
Name	Routing
Use of connector	
	How do you want to route email messages?
Routing Security restrictions	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
O Validation email	Route email through these smart hosts
	Example: myhost.contoso.com or 192.168.3.2 +
O Review connector	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):

New connecto	r	
Name		Security restrictions
Use of connect	or	
		How should Office 365 connect to your partner organization's email server?
Routing	Routing	Always use Transport Layer Security (TLS) to secure the connection (recommended)
	Security restrictions	Connect only if the recipient's email server certificate matches this criteria
Security restriction		 Any digital certificate, including self-signed certificates
) Validation email	 Issued by a trusted certificate authority (CA)
Validation ema 		Add the subject name or subject alternative name (SAN) matches this domain name:
Review connect	tor	Example: contoso.com or *.contoso.com

 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:

- Test Connectivity If this test fails, Outbound Groups is not enabled. Contact <u>Barracuda</u> <u>Networks Technical Support</u> and request that Outbound Groups be enabled on your Email Gateway Defense account.
- 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.

•	New connector	
	Name	Validation email
•	Use of connector	
		Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.
9	Routing	······································
		Example: user@contoso.com +
9	Security restrictions	user@contoso.com
	Validation email	Validate

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 sender's domain is....
- 9. Enter the domains you want to route through Email Gateway Defense.
- 10. Under **Do the following**, select **Redirect the message to... > the following connector**, and select the connector you defined in *Step 1. Create the Connector*.
- 11. Under Except if, select The Recipient > is external/internal > Inside the organization.
- 12. Click Next.
- 13. Under Match sender address in message, select Header or envelope.
- 14. Click Next.
- 15. Review the settings and then click **Finish**.



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

© 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.