

How to Configure Microsoft 365 Outbound Automatic Replies

https://campus.barracuda.com/doc/16885/

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.

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
	Your organization's email server
	Partner organization

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



New connector	
Name	Connector name
Use of connector	
Routing	This connector enforces routing and security restritions for email messages sent from Office 36 to your partner organization or service provider.
	Name *
O Security restrictions	Outbound to Barracuda (Rule)
O Validation email	Description Outbound to Barracuda
O 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	
	Name	Use of connector
	Use of connector	Specify when you want to use this connector.
0	Routing	 Only when I have a transport rule set up that redirects messages to this connector
	Security restrictions	Only when email messages are sent to these domains
	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 +
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 connector	Security restrictions	
Name		
Use of connector		
Routing	How should Office 365 connect to your partner organization's email server?	
Security restrictions	Connect only if the recipient's email server certificate matches this criteria O Any digital certificate, including self-signed certificates	
Validation email	 Issued by a trusted certificate authority (CA) Add the subject name or subject alternative name (SAN) matches this domain name: 	
O Review connector	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
	Routing	multiple addresses if your partner organization has more than one domain.
		Example: user@contoso.com +
	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.

Create a new rule
Apply Office 365 Message Encryption and rights protection to messages
Apply custom branding to OME messages
Apply disclaimers
Bypass spam filtering
Filter messages by size
Generate an incident report when sensitive information is detected
Modify messages
Restrict managers and their direct reports
Restrict messages by sender or recipient
Send messages to a moderator
Send messages and save a copy for review

- 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.

Email Gateway Defense



Set rule conditions		
Set rule settings	Set rule conditions	
Review and finish		
	Name and set conditions for your transport rule	
	Name *	
	Outbound to Barracuda (Mail rule)	
	Apply this rule if *	
	The sender V is external/internal V	+
	The sender is located 'InOrganization'	0
	And	
	The recipient \checkmark is external/internal \checkmark	۲ 🗎
	The recipient is located 'NotInOrganization'	0
	Do the following *	_
	Redirect the message to \sim the following connector \sim	+
	route the message using the following connector 'Outbound to Barracuda (Rule)'	0
	Except if	_
	The message properties \sim include the message type \sim	+
	The message type is 'OOF'	0
	ge type exception per rule. You must create multiple ma types, for example, one for Automatic reply and one fo	
select message type	×	
Automatic reply	~	
Automatic reply		
Auto-forward		
Encrypted		
Calendaring		
Calendaring Permission controlled		
Calendaring Permission controlled Voice mail		
Calendaring Permission controlled Voice mail Signed		
Calendaring Permission controlled Voice mail		

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

Email Gateway Defense



	Set rule settings
Set rule settings	Set rule settings
Review and finish	
	Set settings for your transport rule
	Rule mode
	Enforce
	Test with Policy Tips
	Test without Policy Tips
	Severity *
	Not specified 🗸
	Activate this rule on
	7/5/2023 🛗 - 5:00 PM 🗸
	Deactivate this rule on
	7/5/2023
	F S COLO Inc.
	Stop processing more rules
	Defer the message if rule processing doesn't complete
	Match sender address in message * Header or envelope
	Comments

13. Click Next.

14. Review the settings and then click **Finish**.



Set rule settings	Review and fi	nish
Review and finish	After your finish creating this rule, it is turned Rule name Outbound to Barracuda (Mail rule) Rule comments	off by default until you turn it on from the Rul
	Rule conditions	Rule settings
	Apply this rule if The sender is located 'InOrganization' The recipient is located 'NotInOrganization' Do the following route the message using the following connector 'Outbound to Barracuda (Rule)' Except If The message type is 'OOF' Edit rule conditions	Mode Enforce Set date range Specific date range is not set Priority 16 Severity Not specified For rule processing errors Ignore Stop processing more rules false

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 <u>Step 2 Configure Microsoft 365 for Inbound and</u> <u>Outbound Mail</u>, *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.