

How to Configure Microsoft 365 for Inbound and Outbound Mail

<https://campus.barracuda.com/doc/39822576/>

This article addresses configuring Microsoft 365 with the Barracuda Email Security Gateway as your inbound and/or outbound mail gateway.

See also: [Step 3 - Initial Configuration](#)

Important

Microsoft 365 addresses and user interfaces can change, so please refer to Microsoft documentation for details on configuration. To prepare your Barracuda Email Security Gateway deployment to connect with Microsoft 365, see [Prerequisites for your email server environment](#) in [Set up connectors to route mail between Microsoft 365 and your own email servers](#).

You can specify the Barracuda Email Security Gateway as an *inbound mail gateway* through which all incoming mail for your domain passes before reaching your Microsoft 365 account. The Barracuda Email Security Gateway filters out spam and viruses, and then passes the mail on to the Microsoft 365 mail servers. Use the **Inbound Configuration** instructions below to configure.

You can likewise specify the Barracuda Email Security Gateway as the *outbound mail gateway* through which all mail is sent from your domain via your Microsoft 365 account to the recipient. As the outbound gateway, the Barracuda Email Security Gateway processes the mail by filtering out spam and viruses and applying any outbound policies (blocking, encrypting, etc.) before final delivery. By using the configuration described in *Outbound Configuration* below, you instruct the Microsoft 365 mail servers to pass all outgoing mail from your domain to the Barracuda Email Security Gateway.

Inbound Configuration

To restrict all mail sent to your organization to only that which is sent from the Barracuda Email Security Gateway:

1. Create a connector for MS Exchange in Microsoft 365. You will need the IP address of the Barracuda Email Security Gateway. Once you configure the connector, any Internet mail that does not originate from this IP address range will be rejected by Microsoft 365.
2. Optionally add the requirement for TLS encryption. If you do so, then all mail from your partner organization sent from the IP address or address range you specify must be sent using TLS. Any mail that does not meet this restriction will be rejected.

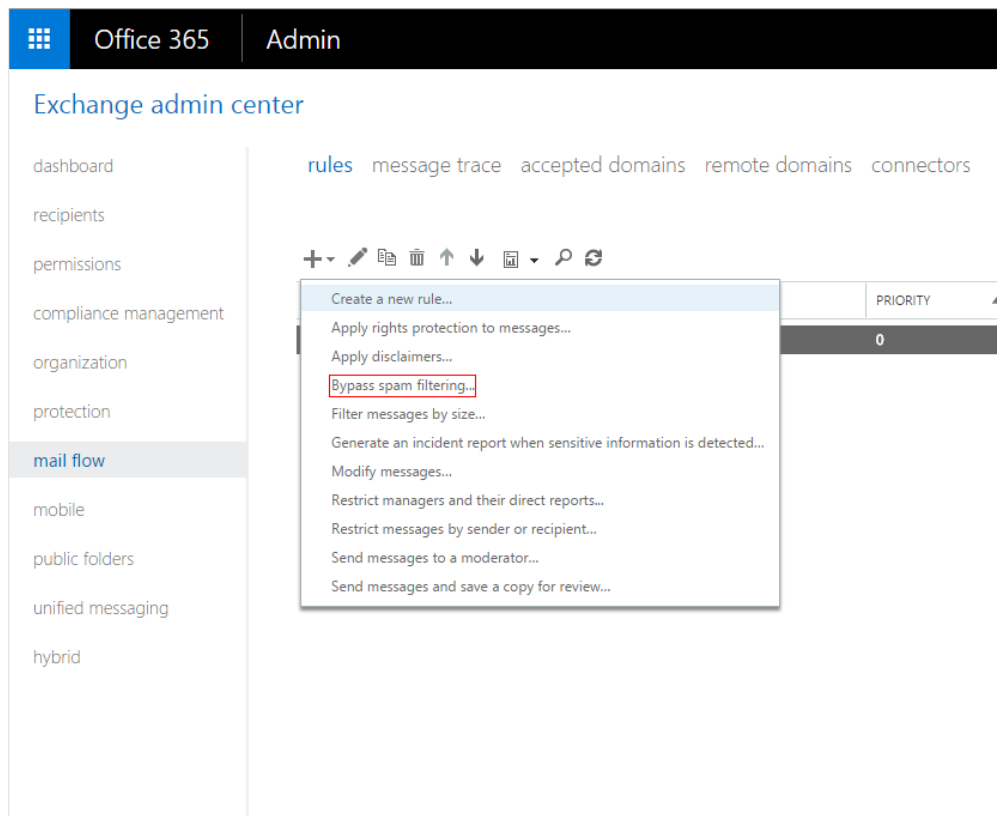
Important: When TLS is selected for the inbound connector, the Barracuda Email Security Gateway needs to have a trusted certificate, not the default certificate. In this

case, SMTP recipient verification will not work, so you need to either set up [explicitly accepted users](#), or use LDAP recipient verification.

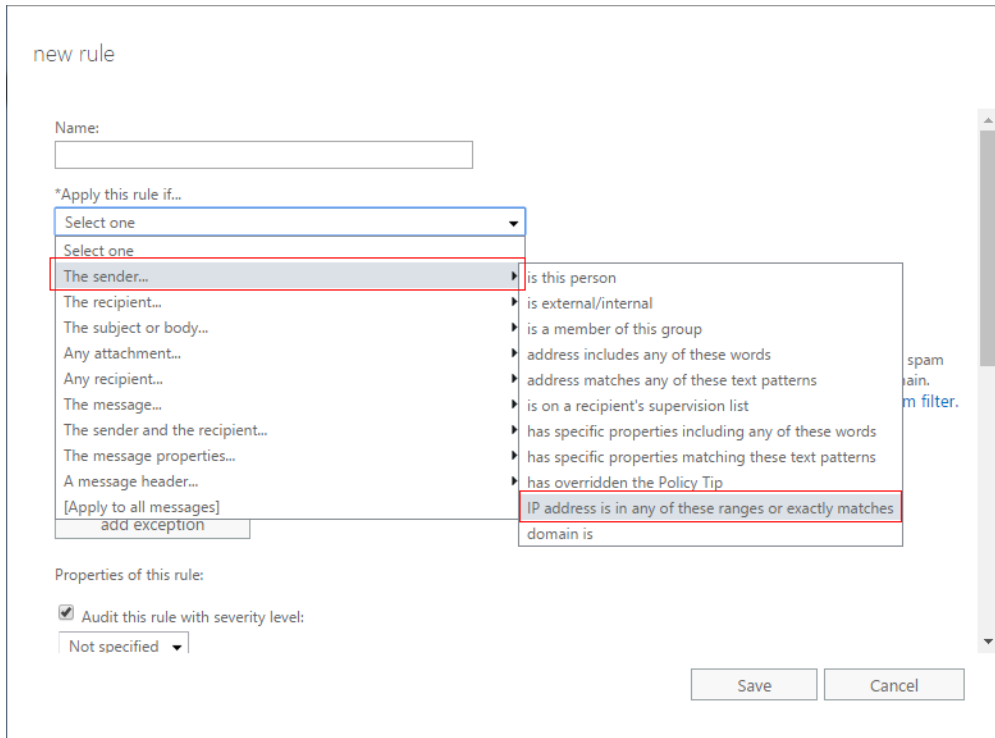
For further details about configuring Microsoft 365 with connectors, see [Set up connectors for secure mail flow with a partner organization](#) in Microsoft documentation.

Inbound Configuration - Create Transport Rule to Bypass Spam Filtering

1. Log into the Microsoft 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 **Bypass spam filtering**:



4. In the **new rule** page, enter a **Name** to represent the rule.
5. From the **Apply this rule** drop-down menu, select **The sender > IP address is in any of these ranges or exactly matches**:



new rule

Name:

*Apply this rule if...

Select one

The sender... is this person

The recipient... is external/internal

The subject or body... is a member of this group

Any attachment... address includes any of these words

Any recipient... address matches any of these text patterns

The message... is on a recipient's supervision list

The sender and the recipient... has specific properties including any of these words

The message properties... has specific properties matching these text patterns

A message header... has overridden the Policy Tip

[Apply to all messages] IP address is in any of these ranges or exactly matches

add exception domain is

Properties of this rule:

Audit this rule with severity level:

Not specified

Save Cancel

6. In the **Specify IP address ranges** page, enter the IP address/range for the Sender (your Barracuda Email Security Gateway).
7. Click **OK**, and click **Save** to create the transport rule.
8. Click the **Edit** icon for the rule, scroll to the **Properties of this rule** section, and in the **Priority** field, type 0.
9. Click **Save**.

Outbound Configuration From Microsoft 365 to the Barracuda Email Security Gateway

If you have more than one domain on your tenant (e.g., `x.com` and `y.com`) and you only want to filter one of the domains (such as `x.com`, for example), refer to [How to Configure Microsoft 365 to Scan Only Selected Domains Outbound](#). The instructions in the section below describe how to filter for *all* domains for outbound mail.

If you have multiple outgoing account domains for Microsoft 365, you only need to make one send connector in Microsoft 365. You can use any one of the outbound smarthosts to make the send connector.

Each of your domains from which you want to be able to send email *must* be added to the Barracuda Email Security Gateway. Be sure to add all of your accepted Microsoft 365 domains to the Barracuda Email Security Gateway before configuring outgoing email in this section.

1. Log into your Barracuda Email Security Gateway as *admin*. Go to the **BASIC > Outbound** page.
2. Make a note of the Outbound SMTP Host IP address and associated port.
3. Log into the Microsoft 365 [Exchange admin center](#), and go to **Admin centers > Exchange**.
4. In the left pane, click **mail flow**, and click **connectors**.
5. Click the + symbol, and use the wizard to create a new connector.
6. From the **From** drop-down menu, select **Microsoft 365**, and from the **To drop-down** menu, select **Partner organization**.

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. [Learn more](#)

From:

To:

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

7. Enter a Name and (optional) Description to identify the connector.

New connector

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

*Name:

Description:

What do you want to do after connector is saved?
 Turn it on

8. Click **Next**. Select **Only when email messages are sent to these domains**, click the + symbol, and enter an asterisk (*) in the **add domain** field.
9. Click **OK**, and click **Next**. Select **Route email through these smart hosts**, and click the + symbol.
10. Go to the Barracuda Email Security Gateway and navigate to the **BASIC > IP Configuration** page. Copy the **Default Hostname** and the **Default Domain** values from the **Domain Configuration** section of the page. Alternatively you can use the public IP address (which should be NAT'ed to the firewall). Enter the Default Hostname or IP address in the **add smart host page**:

add smart host

Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.
Example: myhost.contoso.com or 192.168.3.2

11. Click **Save** , and click **Next** . Use the default setting, **Always use Transport Layer Security (TLS) to secure the connection (recommended)** > **Issued by Trusted certificate authority (CA)** :

New connector

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

12. Click **Next**. In the confirmation page, verify your settings and click **Next**. Microsoft 365 runs a test to verify your settings:

New connector

Confirm your settings
Before we validate this connector for you, make sure these are the settings you want to configure.

Mail flow scenario
From: Office 365
To: Partner organization

Name
Outbound to Barracuda

Description
None

Status
Turn it on after saving

When to use the connector
Use only for email sent to these domains: *

Routing method
Route email messages through these smart hosts:
d91267.o.ess.barracudanetworks.com

Please wait...

Back Next Cancel

13. When the verification page displays, enter a test email address, and click **Validate**. For this test, it is important to use an email address from *outside your organization*, such as a Gmail or Yahoo email address.

There are two parts of the validation:

1. **Test Connectivity** - If this test fails, contact [Barracuda Networks Support](#).
 2. **Send Test Email** - If this 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 change your domain away from `onmicrosoft.com`, the test should work.
 3. Click **Save**. Your mail flow settings are added.
14. The Barracuda Email Security Gateway now accepts outbound traffic from Outlook 365.

Add a Connector

1. Log into the Microsoft 365 [Exchange 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 **Microsoft 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 *

Description

What do you want to do after connector is saved?

Turn it on

6. Click **Next** . Select **Only when email messages are sent to these domains** . Enter an asterisk (*) in the text box field and click the blue + .

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 hosts**.
8. Go to the Barracuda Email Security Gateway and navigate to the **BASIC > IP Configuration** page. Copy the **Default Hostname** and the **Default Domain** values from the **Domain Configuration** section of the page (ex: MyESG.barracudanetworks.com). Alternatively you can use the public **IP address** (which should be NAT'ed to the firewall). Enter it in the **Routing** 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

#123456.a.esb.barracudanetworks.com

9. 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

10. 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. There are two parts of the validation:
1. **Test Connectivity** - If this test fails, contact [Barracuda Networks Technical Support](#).
 2. **Send Test Email** - If this 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.

Validation email

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.

Example: user@contoso.com +

mgorman@barracuda.com 🗑️

Validate

⊗ Validation failed

Task	Status
> Check connectivity to https://www.barracudanetworks.com/	Succeed
> Send test email	Failed

11. Click **Next**. If the test email failed, you will need to confirm that you wish to continue without successful validation by clicking **Yes** in the pop-up dialog box. Click **Next**.
12. Verify your settings, and then click **Create connector** to complete the process.

Review connector

Mail flow scenario

From: Office 365

To: Partner organization

Name

Outbound to Barracuda

Status

Turn it on after saving

[Edit name](#)

Use of connector

Use only for email sent to these domains: *

[Edit use](#)

Routing

Route email messages through these smart hosts: `@123456.o.es.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](#)

The Barracuda Email Security Gateway now accepts outbound traffic from Microsoft Outlook 365.

Figures

1. BypassSpamFiltering.png
2. SenderIPAddress.png
3. SelectPartnerOrg.png
4. NewConnector.png
5. AddSmartHostPage.png
6. TransportLayer.png
7. ConfirmSettings.png
8. NewConnectorEAC.png
9. ConnectorNameNew.png
10. UseOfConnectorNew.png
11. RoutingNew.png
12. SecurityRestrictionsNew.png
13. ValidationEmailNew.png
14. ReviewConnectorNew.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.