

How to Configure Office 365 to Scan Only Selected Domains Outbound

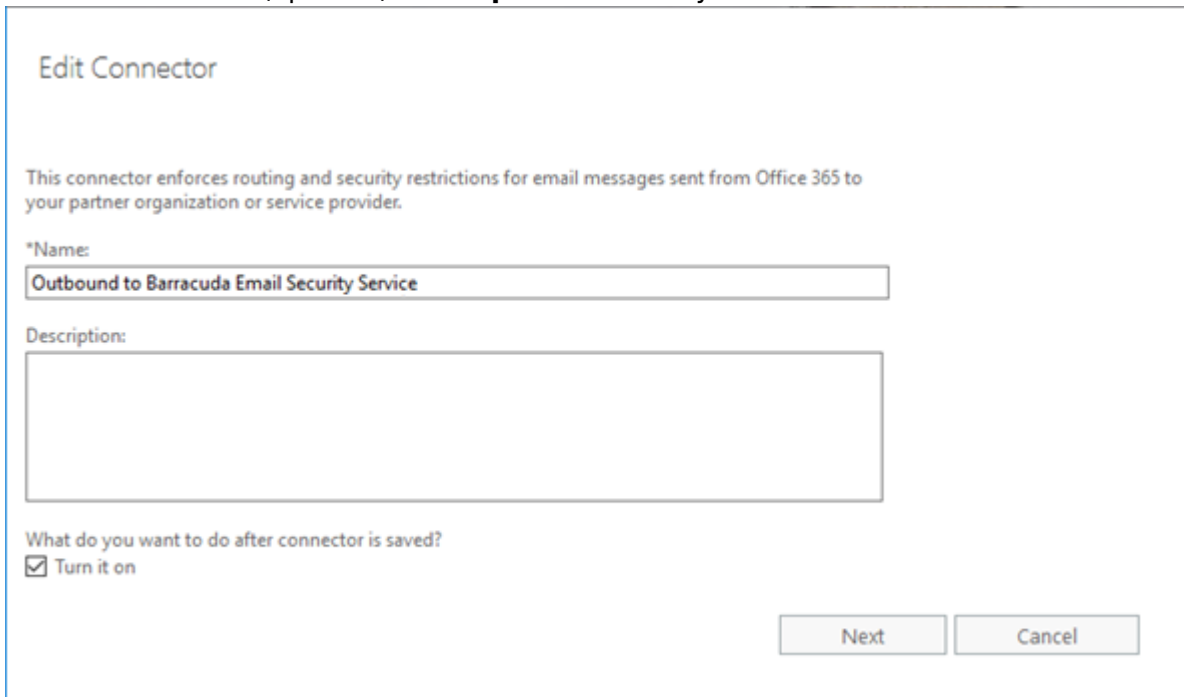
<https://campus.barracuda.com/doc/53675549/>

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

1. Log in to the Office 365 admin center, and go to **Admin centers > Exchange**.
2. In the left pane, click **mail flow**, and click **connectors**.
3. Click the **+** symbol and use the wizard to create a new connector.
4. From the **From** drop-down menu, select **Office 365**, and from the **To** drop-down menu, select **Partner organization**.
5. Enter a **Name** and (optional) **Description** to identify the connector:



Edit Connector

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

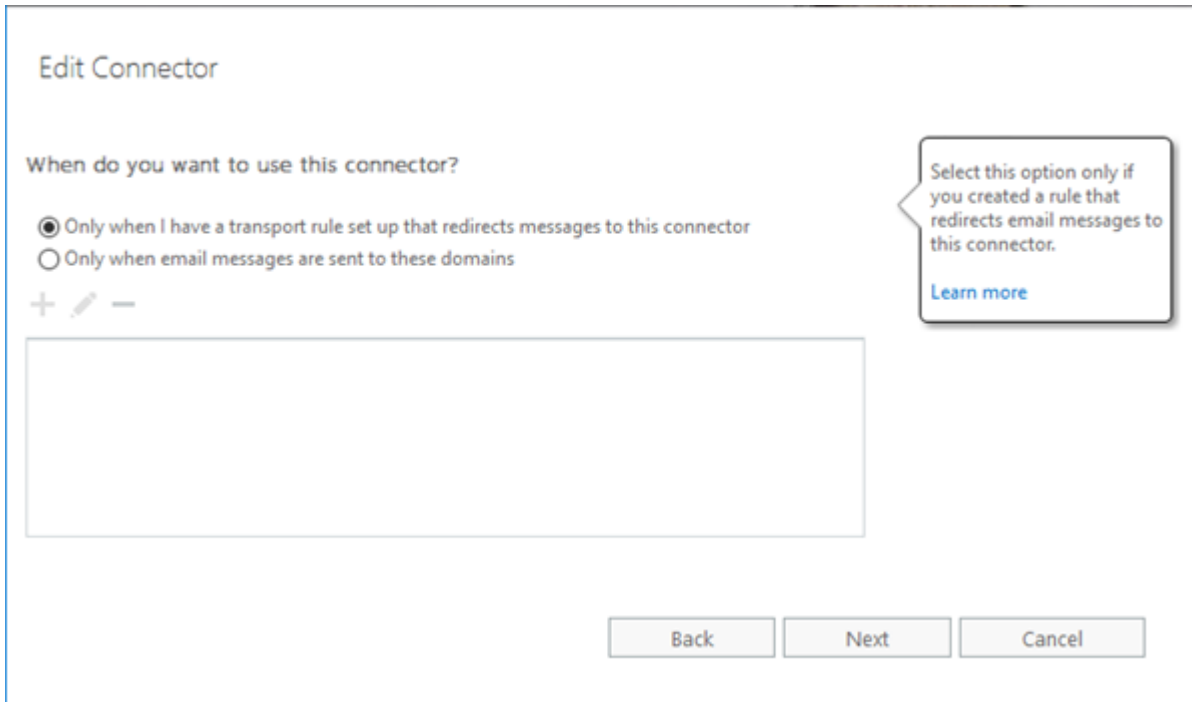
*Name:
Outbound to Barracuda Email Security Service

Description:

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

Next Cancel

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



Edit Connector

When do 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

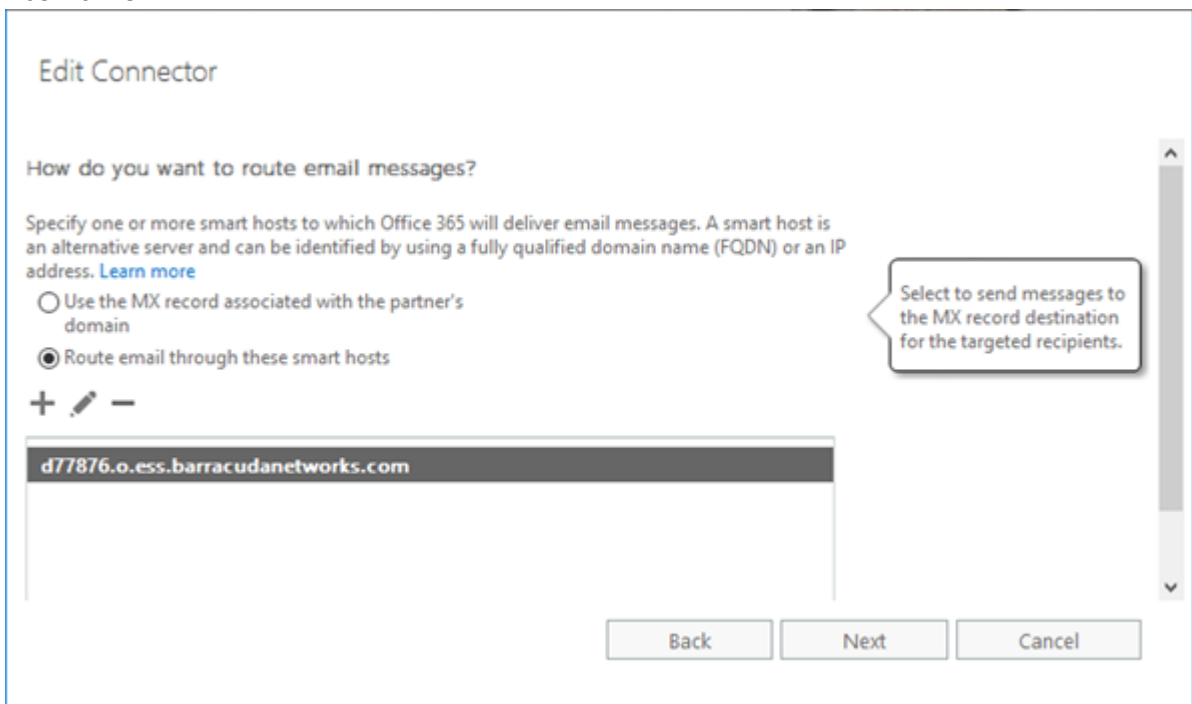
+ ✎ -

Select this option only if you created a rule that redirects email messages to this connector.

[Learn more](#)

Back Next Cancel

7. Click **Next**. Select **Route email through these smart host**, and click on your outbound hostname:



Edit Connector

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. [Learn more](#)

Use the MX record associated with the partner's domain

Route email through these smart hosts

+ ✎ -

Select to send messages to the MX record destination for the targeted recipients.

d77876.o.ess.barracudanetworks.com

Back Next Cancel

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

Edit 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

TLS is a security protocol that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be rejected if the TLS connection isn't successful.

Back Next Cancel

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

Edit 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 Email Security Service

Description
None

Status
Turn it on after saving

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

Routing method
Route email messages through these smart hosts: d77876.o.ess.barracudanetworks.com

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).

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

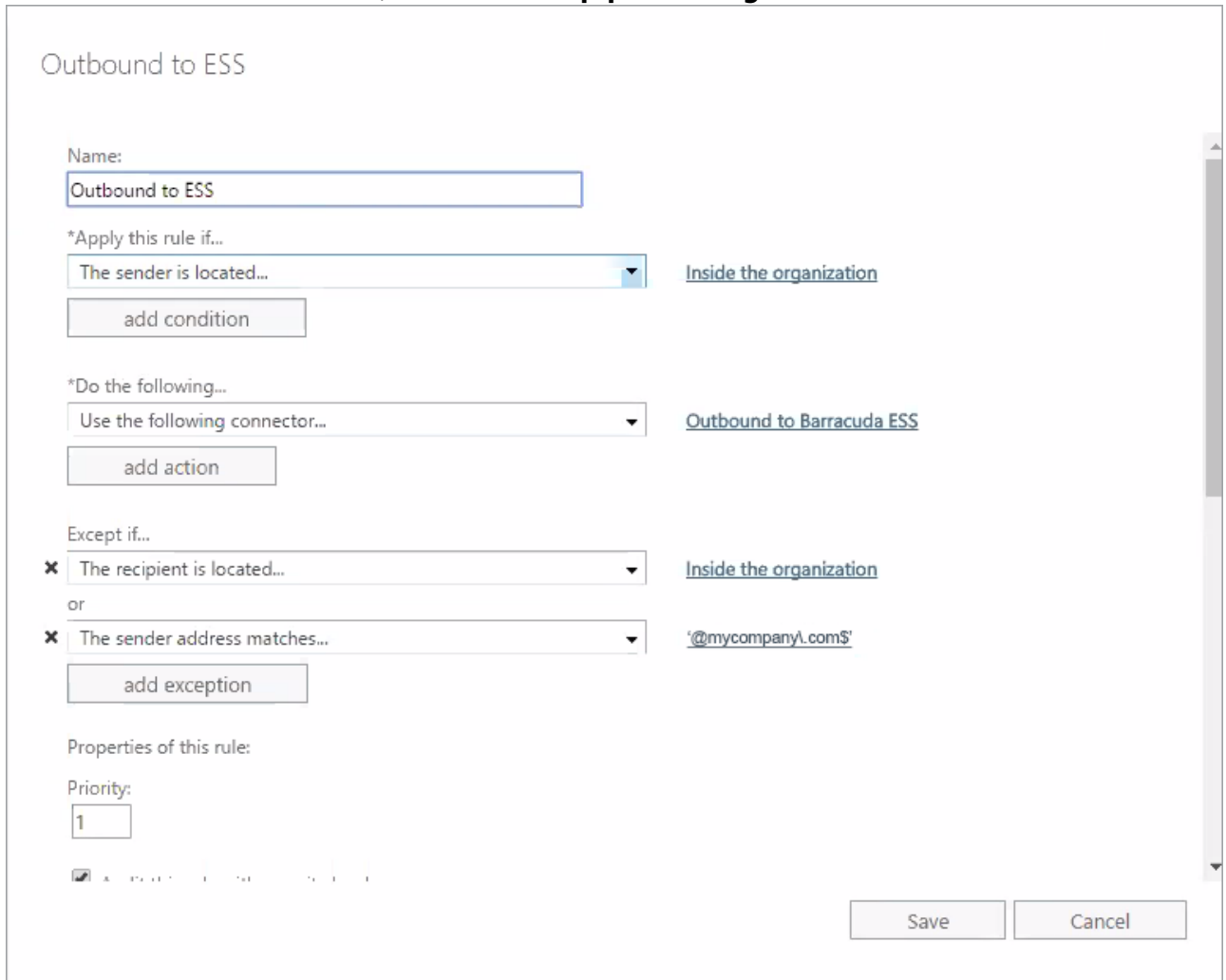
1. Log in to the Office 365 admin center, and go to **Admin centers > Exchange**.
2. In the left pane, click **mail flow**, and click **rules**.
3. Click the **+** symbol, and click **Create new rule**.
4. In the **new rule** page, enter a **Name** to represent the rule.
5. Click **more options** towards 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. 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*.

8. Click **Add Exception**.
9. From the drop-down menu, select **The Recipient is located > is external/internal > Inside the organization**.
10. Click **Add Exception**.
11. From the drop-down menu, select **The sender address matches > address matches any of these text patterns**, and enter the domain(s) you want to exclude from outbound scanning.

You must use regular expressions when entering the domain. For example, if you want to exclude the domain *mycompany.com*, you would type: '@mycompany\.com\$'

Contact [Barracuda Networks Support](#) if you need assistance.

12. Choose **Enforce** as the mode, and select **Stop processing more rules**:



Outbound to ESS

Name:
Outbound to ESS

*Apply this rule if...
The sender is located... [Inside the organization](#)
add condition

*Do the following...
Use the following connector... [Outbound to Barracuda ESS](#)
add action

Except if...
× The recipient is located... [Inside the organization](#)
or
× The sender address matches... '@mycompany\.com\$'
add exception

Properties of this rule:
Priority:
1

Enforce

Save Cancel

13. Click **Save**.

Figures

1. MyCoOutboundConnector01.png
2. OutboundConnector02.png
3. OutboundConnector03.png
4. OutboundConnector04.png
5. MyCoOutboundConnector05.png
6. bess_exclude_domain_outbound.png

© Barracuda Networks Inc., 2019 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.