

Step 2 - Configure Microsoft 365 for Inbound and Outbound Mail

<https://campus.barracuda.com/doc/96022752/>

You can configure Microsoft 365 with Email Gateway Defense as your inbound and/or outbound mail gateway.

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

Microsoft 365 IP addresses and user interfaces can change; refer to Microsoft documentation for configuration details.

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

You can also specify Email Gateway Defense 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, Email Gateway Defense processes the mail by filtering out spam and viruses before final delivery. By configuring Microsoft 365 as described in **Configure Outbound Mail Flow** below, you instruct the Microsoft 365 mail servers to pass all outgoing mail from your domain to Email Gateway Defense (the gateway server).

Step 1. Launch the Email Gateway Defense Setup Wizard

Before you launch the wizard, verify you have the following:

- Microsoft 365 admin credentials
- Credentials to run a PowerShell script or terminal to manually execute PowerShell scripts

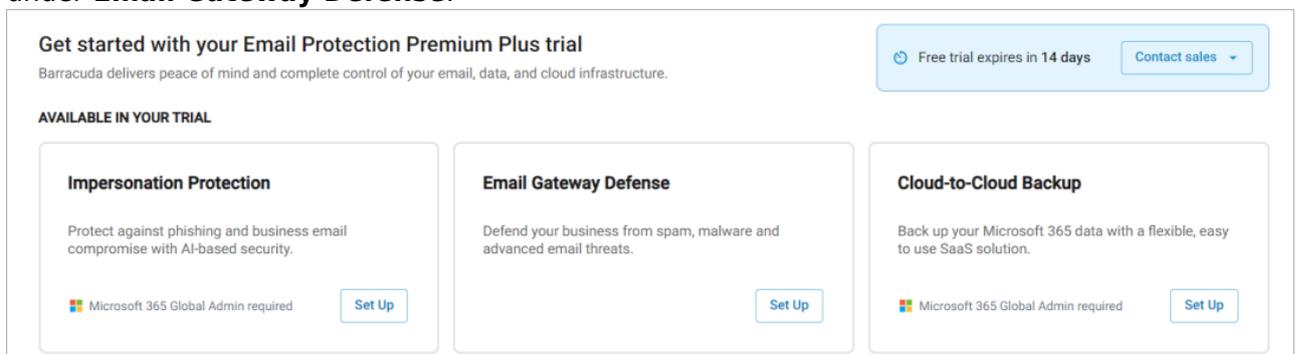
Note that you cannot reopen the wizard after you have completed the wizard. If you have started the wizard but did not complete it, log into Barracuda Cloud Control, select **Email Gateway Defense** on the left side. In the top banner, click **Set Up Now** to relaunch the wizard.

The setup wizard includes steps to identify your email server, add MX records, and remove MX records. Each of the domains where you want to filter email must be verified by Email Gateway

Defense for proof of ownership; Email Gateway Defense does not process email for a domain until the verification process is complete.

Note that after verifying your domain, any mail sent to your domain from another Barracuda Email Gateway Defense customer will be processed normally by your Email Gateway Defense account and not delivered via MX records.

1. Log into Barracuda Cloud Control. If this is your first time launching the Email Gateway Defense setup wizard, you will be redirected to the Barracuda Trials Hub page. Click **Set Up** under **Email Gateway Defense**.



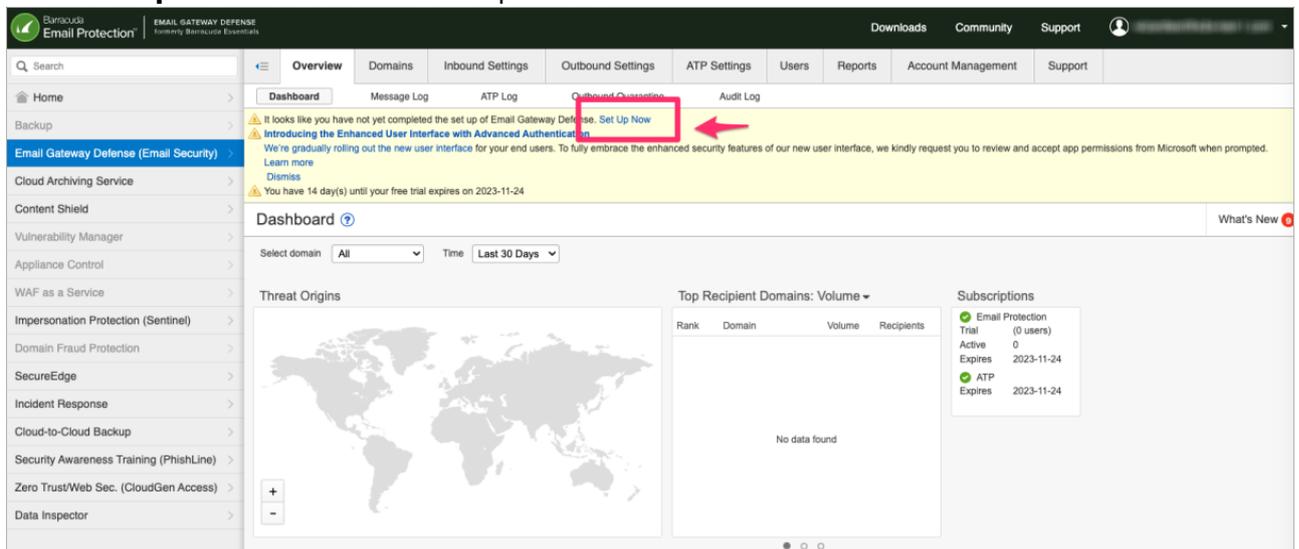
Get started with your Email Protection Premium Plus trial
Barracuda delivers peace of mind and complete control of your email, data, and cloud infrastructure.

AVAILABLE IN YOUR TRIAL

- Impersonation Protection**
Protect against phishing and business email compromise with AI-based security.
Microsoft 365 Global Admin required [Set Up](#)
- Email Gateway Defense**
Defend your business from spam, malware and advanced email threats. [Set Up](#)
- Cloud-to-Cloud Backup**
Back up your Microsoft 365 data with a flexible, easy to use SaaS solution.
Microsoft 365 Global Admin required [Set Up](#)

Free trial expires in 14 days [Contact sales](#)

Alternatively, if you have started the setup wizard but did not complete it, after logging into Barracuda Cloud Control, select **Email Gateway Defense** on the left side. In the top banner, click **Set Up Now** to launch the setup wizard.



Set Up Now

Dashboard

Select domain: All Time: Last 30 Days

Threat Origins

Top Recipient Domains: Volume

Rank	Domain	Volume	Recipients
No data found			

Subscriptions

- Email Protection Trial (0 users)
Active: 0
Expires: 2023-11-24
- ATP
Expires: 2023-11-24

The Email Gateway Defense wizard launches.

2. Select the **Region** for your data center. Then click **Confirm region**.

After you select your region, you cannot change it.

Email Gateway Defense Setup

Defend your business from spam, malware and advanced email threats.

Select data center region

Store your messages, logs and settings securely. Your data will comply with the privacy policies in the region you select.

⚠ Data center region cannot be changed after confirming

Region ▼

Confirm region

3. Enter a valid email address from the email server domain you want to protect with Email Gateway Defense. Click **Detect email server**.
4. The system automatically auto-fills your destination mail server. If this is not the correct server, click **Edit**, enter the correct details, and then click **Update**.
5. After you have determined that the settings are correct, click **Verify server**.

1. Specify email server

2. Add new MX records

3. Remove old MX records

Email Gateway Defense Setup

Defend your business from spam, malware and advanced email threats.

1 **Specify email server**
 To verify the email server you want to protect, enter a valid email address from that domain. More servers can be added in the product settings once this initial setup process is completed.

Your domain email address

Detect email server

Mail server	Port	Action	Status
test@domain.com	25	Edit	⊘ Unverified

Verify server

ⓘ Note: Mail servers can take up to 48 hours to be discoverable for new domains.

Note that mail servers can take up to 48 hours to be discoverable for new domains.

6. Once your email server is verified, a green check mark ✔ will appear at Step 1 and the **Status** will show ✔ **Verified**. You can now move on to *Step 2 Add new MX records*.
7. To add new MX records:
 1. Log into your DNS hosting account.
 2. Add the primary and backup MX records shown in the **Add new MX records** section. Instructions for your DNS hosting provider will vary; you can use search terms such as *add, edit, manage, or MX records*.

Step 2 - Configure Microsoft 365 for Inbound and Outbound Mail

3 / 27

2 Add new MX records
To confirm domain ownership, add the Primary and Backup MX records below through your DNS Hosting Provider website. Setting priority 99 for the new MX records will ensure your current inbound email flow isn't disrupted.

We detected the following information about your DNS Hosting Provider.

DNS Hosting Provider	Link
Hostinger International, Ltd	Hostinger website

[How to manage MX records | Hostinger International, Ltd](#)

MX Record	Priority	Domain	Status
Primary	99	d302338a.ess.barracudanetworks.com	Unverified
Backup	99	d302338b.ess.barracudanetworks.com	Unverified

Note: MX record updates can take up to 48 hours to take effect

3. Add the MX records with a low priority, for example, 99. Adding the new MX records to your existing list should look similar to this:

Name	TTL	Class	Record Type	Priority	Record	
mydomain.com	21600	IN	MX	10	mailserver1.mydomain.com	} Examples of existing MX records
mydomain.com	21600	IN	MX	15	mailserver2.mydomain.com	
mydomain.com	21600	IN	MX	99	dxxxxxxa.ess.barracudanetworks.com	} Examples of new Barracuda MX records
mydomain.com	21600	IN	MX	99	dxxxxxxb.ess.barracudanetworks.com	

After updating your MX records, allow at least 24-48 hours before completing the next step to allow time for your changes to propagate

4. Verify that the new Email Gateway Defense MX records have been added by clicking on the **Verify records** button.

5. Once your MX records are added, a green check mark  will appear at Step 2 and the **Status** will show  **Verified**. You can now move on to *Step 3 Remove old MX records*.

8. To remove old MX Records:

1. Log into your DNS hosting account.
2. Remove the existing MX records shown in the **Remove old MX records** section. Instructions for your DNS hosting provider will vary; you can use search terms such as *add, edit, manage, or MX records*.

3 Remove old MX records

After the new MX records are verified in Step 2, you will need to remove your old MX records through your DNS hosting provider site so that all of your inbound email will be filtered and protected by Email Gateway Defense.

[How to manage MX records | Hostinger International, Ltd](#)

Priority	Domain	Status	
25	test.natureandbirds.com	Unverified	Verify update

Note: MX record updates can take up to 48 hours to take effect

[Save & exit](#)
[Complete setup](#)

After updating your MX records, allow at least 24-48 hours before completing the next step in the setup wizard to allow time for your changes to propagate.

3. Verify that your non-Barracuda Networks MX records have been removed by clicking on the **Verify update** button.
4. Once your MX records are removed, a green check mark  will appear at Step 3 and the **Status** will show  **Verified**.
9. After you have successfully completed all the steps in the Email Gateway Defense setup wizard, click the **Complete setup** button. To exit the wizard and come back at a later time, click **Save & exit**.

Step 2. Add Additional Email Domains (Optional)

You configured your primary email domain in Step 3 of the wizard, above. Use the steps in the following section if you want to protect additional domains with Email Gateway Defense. If you are only protecting one domain, continue below with Step 3.

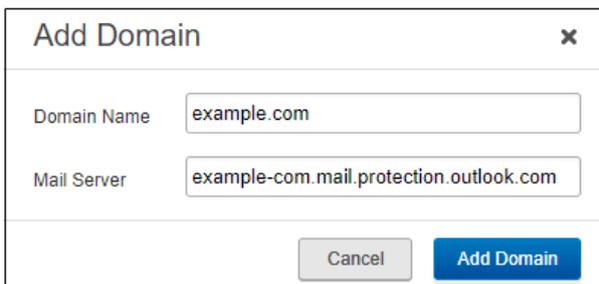
Obtain the hostname:

1. Log into the Microsoft 365 admin center.
2. In the left pane, click **Settings > Domains**.
3. In the **Domains** table, click on your domain.
4. Take note of the hostname. This is the address of your destination mail server, for example, *cuaware-com.mail.protection.outlook.com*

Enter the hostname:

Barracuda Networks recommends using a hostname rather than an IP address so that you can move the destination mail server and update DNS records without making changes to the Email Gateway Defense configuration. This address indicates where Email Gateway Defense should direct inbound mail from the Internet to your Microsoft 365 Exchange server. For example, your domain displays to the Internet as: *bess-domain.mail.protection.outlook.com*

1. Log into the Barracuda Cloud Control as administrator. In the left panel, click **Email Gateway Defense**. Select the **Domains** tab, then click **Add Domain**.
2. Enter the domain name and destination mail server hostname obtained from your Microsoft 365 account:



The screenshot shows a dialog box titled "Add Domain" with a close button (X) in the top right corner. It contains two input fields: "Domain Name" with the value "example.com" and "Mail Server" with the value "example-com.mail.protection.outlook.com". At the bottom, there are two buttons: "Cancel" and "Add Domain".

3. Click **Add Domain**; the **Domain Settings** page displays, listing the new domain.
4. Verify that the domain is yours. Follow the instructions in [How to Set Up MX Records for Domain Verification](#). Make sure that you see that the domain is successfully verified, then return to this page.

Repeat these steps, as needed, for additional Microsoft 365 domains before continuing with Step 3 below.

Step 3. Create Transport Rule to Bypass Spam Filtering

Barracuda Networks recommends using powershell commands to create a transport rule to bypass spam filtering.

1. Install Exchange Online module.
 - If you have already installed Exchange Online module, proceed to the next step.
 - To install Exchange Online module, open Windows PowerShell as an administrator and enter the following command:
`Install-Module -Name ExchangeOnlineManagement`
2. Connect to Exchange Online Powershell and log in with your Microsoft 365 administrator account using the following command:
 - `Connect-ExchangeOnline`

For more information on connecting to Exchange Online Powershell, see the Microsoft article

<https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online->

[powershell?view=exchange-ps.](#)

If you encounter issues running the PowerShell scripts, you can temporarily change the Windows PowerShell script execution policy. For more information, see the Microsoft article

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.3.](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.3)

3. Find the correct IP range based on the region selected when setting up your Barracuda Networks instance. Refer to the [Email Gateway Defense IP Ranges Used for Configuration](#) for the IP ranges corresponding to your region.
4. After you connect to Exchange Online PowerShell, run the appropriate PowerShell script based on your region:

PowerShell Script for the Australia Region

```
New-TransportRule -Name "Barracuda spam bypass" -SenderIpRanges 3.24.133.128/25 -SetSCL -1 -Enabled $true -Priority 0
```

PowerShell Script for the Canada Region

```
New-TransportRule -Name "Barracuda spam bypass" -SenderIpRanges 15.222.16.128/25 -SetSCL -1 -Enabled $true -Priority 0
```

PowerShell Script for the German Region

```
New-TransportRule -Name "Barracuda spam bypass" -SenderIpRanges 35.157.190.224/27 -SetSCL -1 -Enabled $true -Priority 0
```

PowerShell Script for the India Region

```
New-TransportRule -Name "Barracuda spam bypass" -SenderIpRanges 13.200.136.128/25 -SetSCL -1 -Enabled $true -Priority 0
```

PowerShell Script for the UK Region

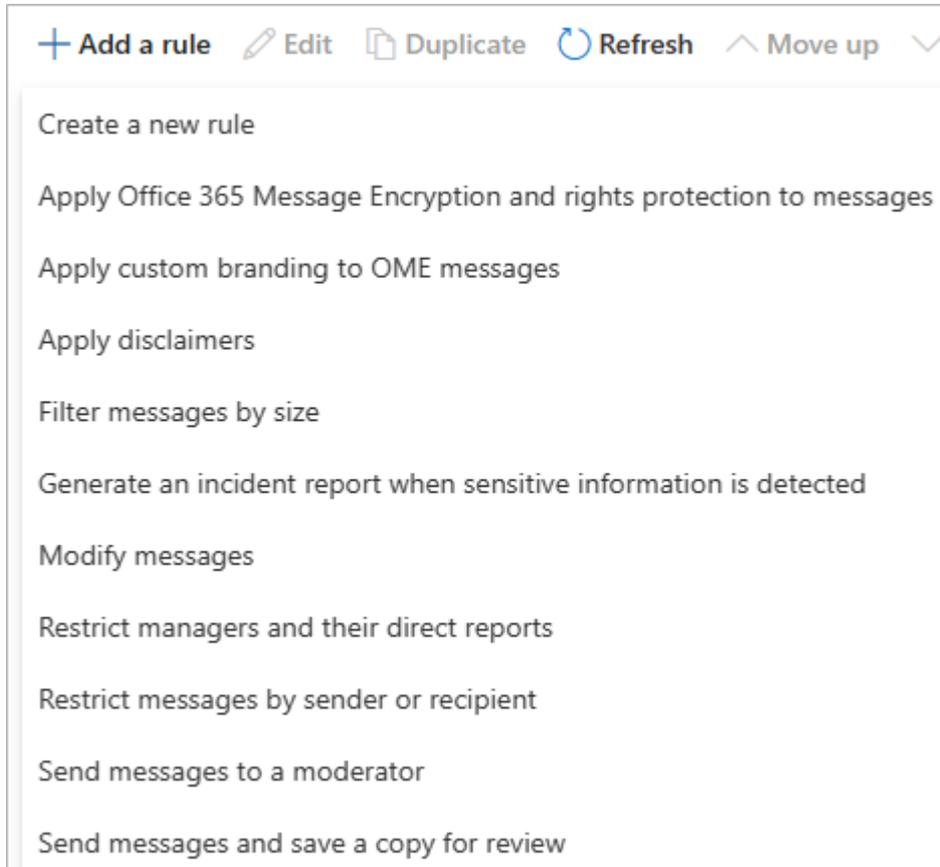
```
New-TransportRule -Name "Barracuda spam bypass" -SenderIpRanges 35.176.92.96/27 -SetSCL -1 -Enabled $true -Priority 0
```

PowerShell Script for the US Region

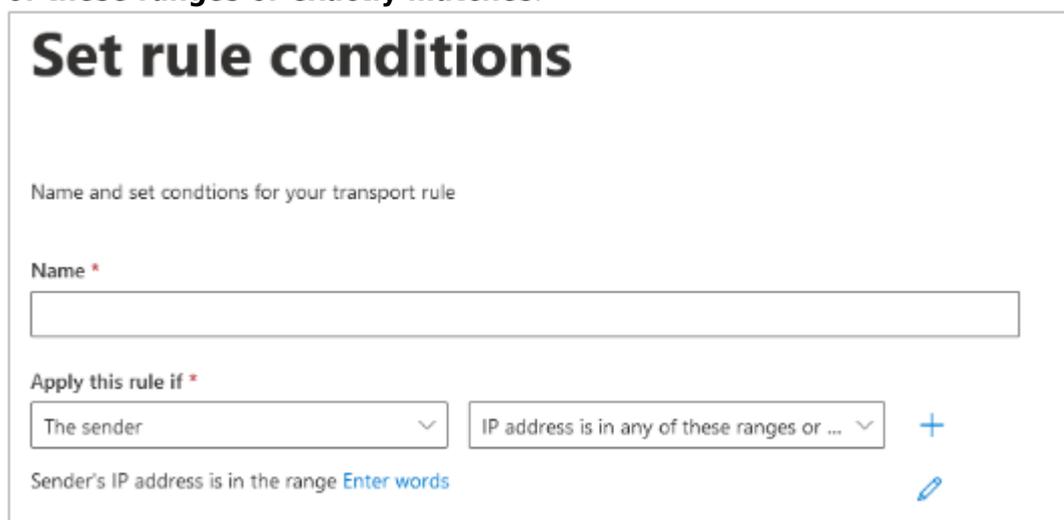
```
New-TransportRule -Name "Barracuda spam bypass" -SenderIpRanges 209.222.80.0/21 -SetSCL -1 -Enabled $true -Priority 0
```

Alternatively, you can use the Microsoft 365 admin center to create a 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 **Add a rule**, and select **Create a new rule**:



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



6. In the **specify IP address ranges** page, enter the IP address/range for the Sender (Email Gateway Defense). Refer to the IP addresses listed in [Email Gateway Defense IP Ranges Used for Configuration](#).

specify IP address ranges

Add

Edit
 Delete
1 item

○
209.222.80.0/21

7. From **Do the following** drop-down menus, select **Modify the message properties** and **set the spam confidence level (SCL)**.

Set rule conditions

Name and set conditions for your transport rule

Name *

Barracuda spam bypass

Apply this rule if *

The sender

IP address is in any of these ranges or...

+

Sender's IP address is in the range '209.222.80.0/21'

Do the following *

Modify the message properties

set the spam confidence level (SCL)

+

Set the spam confidence level (SCL) to '-1'

Except if

Select one

Select one

+

🗑️

8. Click **Next**.
9. For **Set rule settings**, leave the default options and click **Next**.

Set rule settings

Set settings for your transport rule

Rule mode

Enforce

Test with Policy Tips

Test without Policy Tips

Severity *

Not specified

Activate this rule on

8/28/2023 - 3:30 PM

Deactivate this rule on

8/28/2023 - 3:30 PM

Stop processing more rules

Defer the message if rule processing doesn't complete

Match sender address in message *

Header

Comments

10. Review the rule conditions, then click **Next**.
11. Click **Next**, then click **Finish** to create the transport rule.
12. When the rule is finished creating, click **Done**.
13. Click on the new created rule, found at the bottom of the mail flow rules.
14. Enable the rule now. By default, your newly created rule is disabled.

Barracuda spam bypass

[Edit rule conditions](#) [Edit rule settings](#)

Status: Enabled

Enable or disable rule
 Enabled

Rule settings

Rule name	Mode
Barracuda spam bypass	Enforce
Severity	Set date range
Not specified	Specific date range is not set
Senders address	Priority
Matching Header	20

For rule processing errors
Ignore

Rule description

Apply this rule if

sender ip addresses belong to one of these ranges: '209.222.80.0/21'

Do the following

Set the spam confidence level (SCL) to '-1'

Rule comments

15. Click **Edit rule settings**.

Barracuda spam bypass

[Edit rule conditions](#)
[Edit rule settings](#)

Status: Disabled

Enable or disable rule

Enabled

Rule settings

Rule name	Mode
Barracuda spam bypass	Enforce
Severity	Set date range
Not Specified	Specific date range is not set
Senders address	Priority
Matching Header	16
For rule processing errors	
Ignore	

Rule description

Apply this rule if

sender ip addresses belong to one of these ranges: '64.235.144.0/20' or '209.222.80.0/21'

Do the following

Set the spam confidence level (SCL) to '-1'

Rule comments

16. In the **Priority** field, type 0.

Barracuda spam bypass

Conditions Settings

Priority *

Rule mode

Enforce
 Test with Policy Tips
 Test without Policy Tips

Severity *

Activate this rule on
11/9/2022

Deactivate this rule on
11/9/2022

Stop processing more rules
 Defer the message if rule processing doesn't complete

Match sender address in message *

Comments

17. Click **Save**, then click **Done**.

Step 4. Deploy Partner Connector

The steps in this section enhance the security of the connection between Email Gateway Defense and Microsoft 365. Creating a partner connector will allow you to enforce security policies to ensure that all inbound email originates from Barracuda's servers.

Create Inbound Connector

To get started, create your inbound connector.

1. Install Exchange Online module.
 - If you have already installed Exchange Online module, proceed to the next step.
 - To install Exchange Online module, open Windows PowerShell as an administrator and enter the following command:
`Install-Module -Name ExchangeOnlineManagement`
2. Connect to Exchange Online Powershell and log in with your Microsoft 365 administrator account using the following command:
 - `Connect-ExchangeOnline`
For more information on connecting to Exchange Online Powershell, see the Microsoft article <https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps>.
If you encounter issues running the PowerShell scripts, you can temporarily change the Windows PowerShell script execution policy. For more information, see the Microsoft article https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.3.
3. Find the correct IP range based on the region selected when setting up your Barracuda Networks instance. Refer to the [Email Gateway Defense IP Ranges Used for Configuration](#) for the IP ranges corresponding to your region.
4. After you connect to Exchange Online PowerShell, run the appropriate PowerShell script based on your region:

PowerShell Script for the Australia Region

```
New-InboundConnector -ConnectorType Partner -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 3.24.133.128/25
```

PowerShell Script for the Canada Region

```
New-InboundConnector -ConnectorType Partner -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 15.222.16.128/25
```

PowerShell Script for the German Region

```
New-InboundConnector -ConnectorType Partner -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 35.157.190.224/27
```

PowerShell Script for the India Region

```
New-InboundConnector -ConnectorType Partner -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 13.200.136.128/25
```

PowerShell Script for the UK Region

```
New-InboundConnector -ConnectorType Partner -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 35.176.92.96/27
```

PowerShell Script for the US Region

```
New-InboundConnector -ConnectorType Partner -Name "Barracuda Inbound Connector" -RequireTls $true -SenderDomains * -SenderIPAddresses 209.222.80.0/24,209.222.81.0/24,209.222.82.0/24,209.222.83.0/24,209.222.84.0/24,209.222.85.0/24,209.222.86.0/24,209.222.87.0/24
```

Validate Mail Flow (Optional)

The new inbound partner connector you just created will be used to enforce restrictions on your Microsoft tenant to prevent emails from bypassing your Barracuda Networks gateway defenses. Prior to enforcing those restrictions, it is important to validate your inbound mail flow to ensure there are no external senders that are sending emails directly to your Microsoft tenant.

For instructions on how to validate mail flow, see [Validating Mail Flow Before Restricting Access](#).

Restrict Access**Time Requirement**

Make sure to wait at least 24 hours after updating MX records before enabling tenant restrictions. This will avoid any potential disruptions to mail delivery due to outdated MX records.

To update your Barracuda partner connector to require inbound mail to flow through Email Gateway Defense, connect to Exchange Online and run the following PowerShell command:

```
Set-InboundConnector -Identity "Barracuda Inbound Connector" -RestrictDomainstoIPAddresses $true
```

Step 5. Configure Sender Policy Framework for Outbound Mail

To ensure Barracuda Networks is the authorized sending mail service of outbound mail from Email Gateway Defense, add the following to the Sender Policy Framework (SPF) record INCLUDE line of the

SPF record for your sending mail server for each domain sending outbound mail. Select the relevant SPF INCLUDE based on the region you selected for your Barracuda Networks instance.

For more information, see [Email Gateway Defense Outbound IP Ranges](#).

AU (Australia)

```
include:spf.ess.au.barracudanetworks.com -all
```

CA (Canada)

```
include:spf.ess.ca.barracudanetworks.com -all
```

DE (Germany)

```
include:spf.ess.de.barracudanetworks.com -all
```

IN (India)

```
include:spf.ess.in.barracudanetworks.com -all
```

UK (United Kingdom)

```
include:spf.ess.uk.barracudanetworks.com -all
```

US (United States)

```
include:spf.ess.barracudanetworks.com -all
```

For more information, see [Sender Authentication](#).

- If you have an SPF record set up for your domain, edit the existing record, and add the following to the INCLUDE line for each domain sending outbound mail based on your Barracuda Networks instance. For example: `include:spf.ess.barracudanetworks.com -all`
- If you do not have an SPF record set up for your domain, use the following value to create a TXT record that creates a HARD Fail SPF for your domain based on your Barracuda Networks instance. For example: `v=spf1 include:spf.ess.barracudanetworks.com -all`

Step 6. Configure User Accounts and User Lists

Follow the steps in the appropriate links, based on your organization's setup.

[How to Configure User Authentication Using LDAP](#)[How to Configure User Authentication with Microsoft Entra ID](#)

Step 7. Configure Outbound Mail

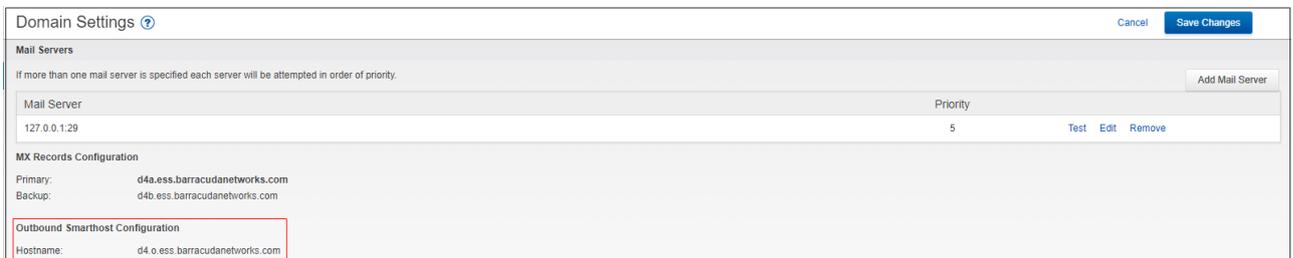
If you have more than one domain on your tenant (e.g., x.com and y.com) and you only want to filter one of the domains (like x.com), refer to [How to Configure Microsoft 365 to Scan Only Selected Domains Outbound](#). The instructions in this section below describe how to filter for *all* domains for 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 that you want to be able to send email *must* be added to Email Gateway Defense. Be sure to add all of your accepted Microsoft 365 domains into Email Gateway Defense before configuring outgoing email in this section.

Outbound Groups must be enabled on your Email Gateway Defense account. Contact [Barracuda Networks Technical Support](#) to request that Outbound Groups be enabled on your Email Gateway Defense account.

1. Log into your Barracuda Cloud Control account. On the left side, select **Email Gateway Defense**. Select the **Domains** tab. For the appropriate domain, click **Edit**.
2. On the **Domain Settings** page, locate the **Outbound Smarthost Configuration** section and make note of the **Hostname**:



Domain Settings [?](#) Cancel Save Changes

Mail Servers

If more than one mail server is specified each server will be attempted in order of priority. Add Mail Server

Mail Server	Priority	
127.0.0.1:29	5	Test Edit Remove

MX Records Configuration

Primary: d4a.ess.barracudanetworks.com
Backup: d4b.ess.barracudanetworks.com

Outbound Smarthost Configuration

Hostname: d4.o.ess.barracudanetworks.com

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 **Office 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 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**:

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

Back Next Cancel

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*, like a gmail or yahoo email address.

There are two parts of the validation:

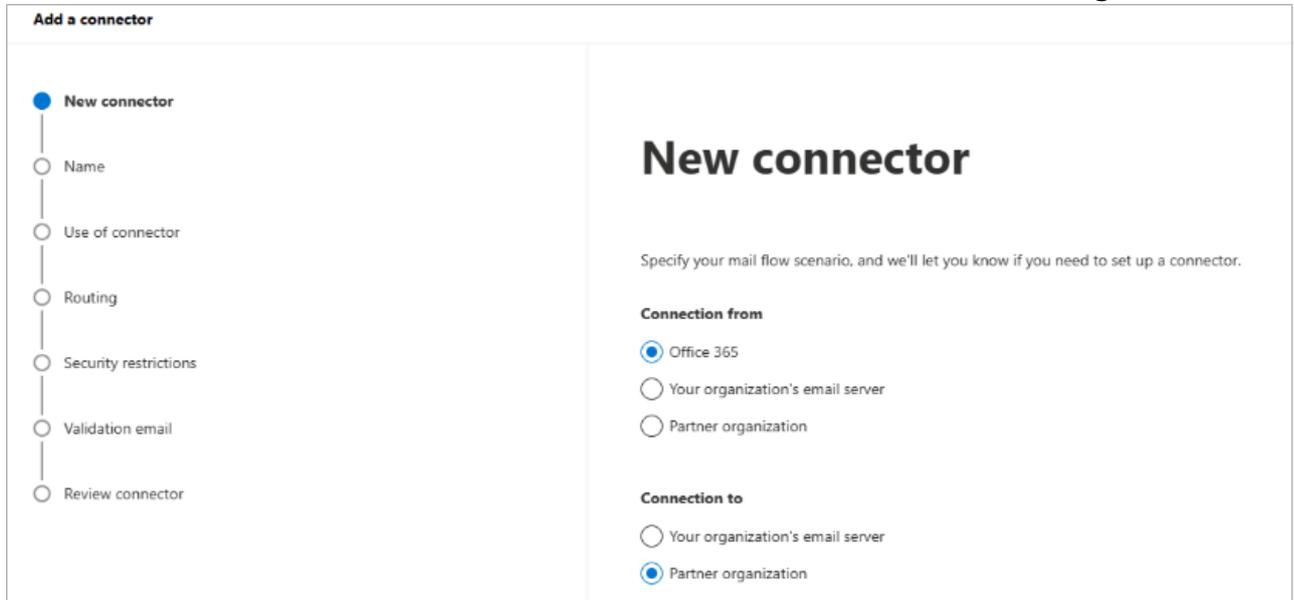
1. **Test Connectivity** - If this test fails, Outbound Groups is not enabled. Contact [Barracuda Networks Technical Support](#) and request that Outbound Groups be enabled on your Email Gateway Defense account.
2. **Send Test Email** - If the test fails, there is no cause for concern. The test email 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.

14. Click **Save**. Your mail flow settings are added.

Email Gateway Defense now accepts outbound traffic from Outlook 365.

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

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

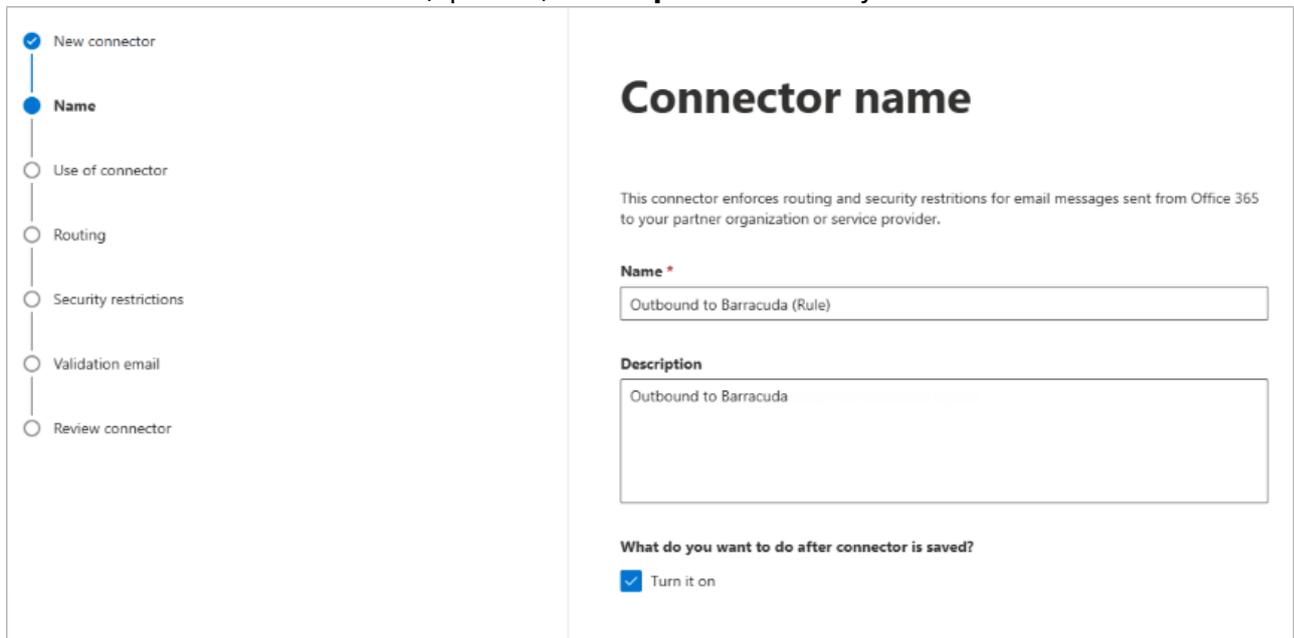
Connection from

- Office 365
- Your organization's email server
- Partner organization

Connection to

- Your organization's email server
- Partner organization

5. Click **Next**. 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 Barracuda (Rule)

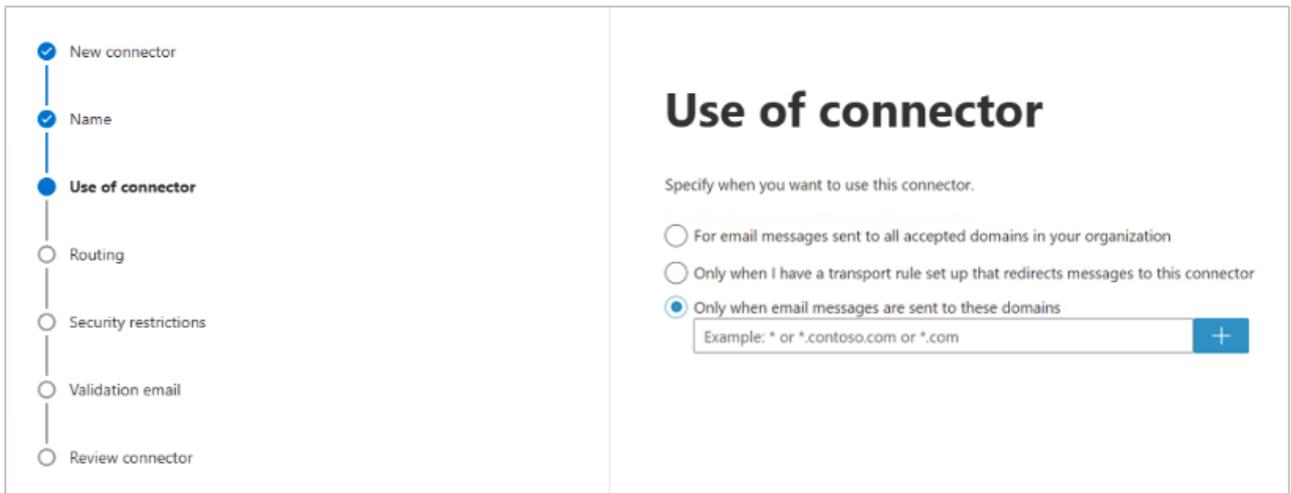
Description

Outbound to Barracuda

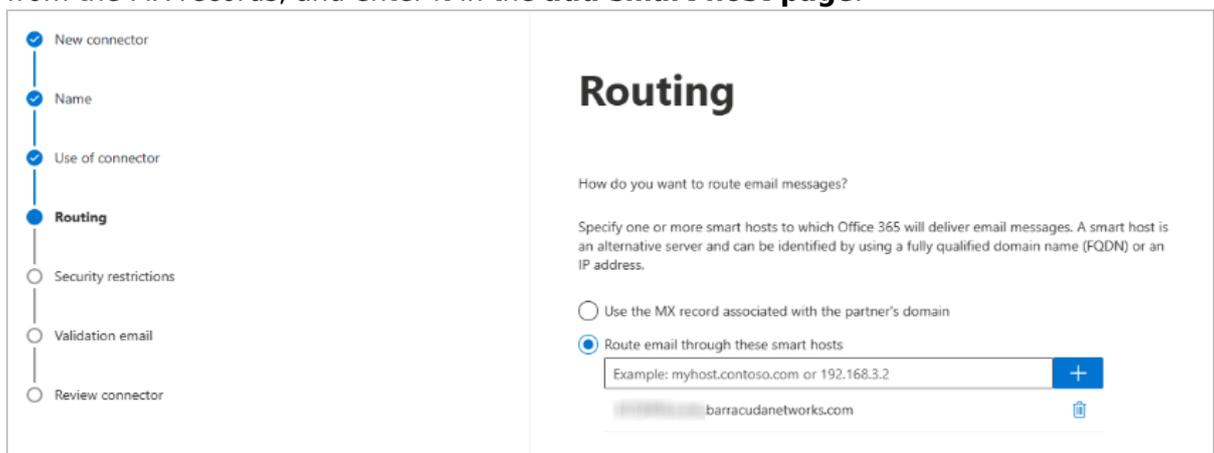
What do you want to do after connector is saved?

- Turn it on

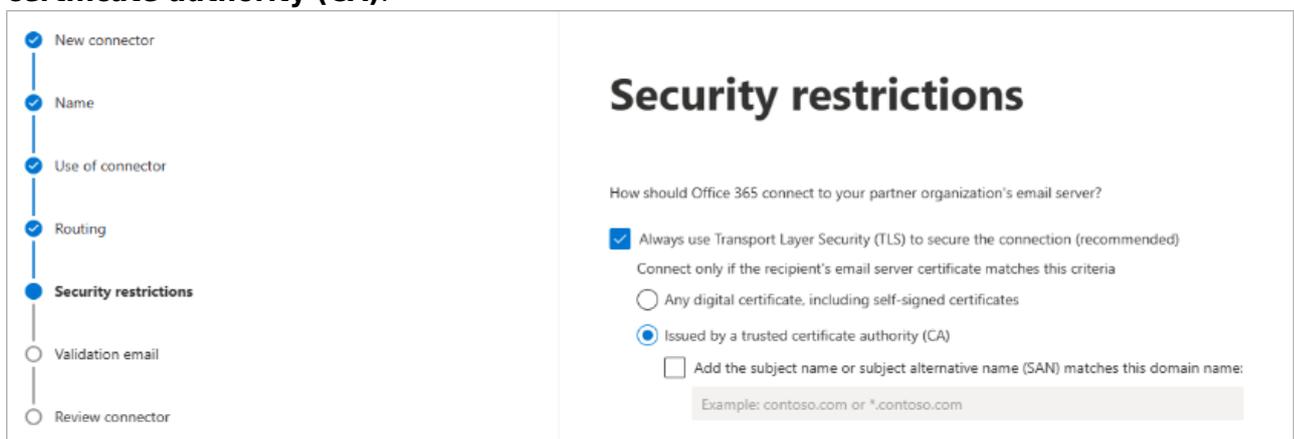
6. Click **Next**. Select **Only when email messages are sent to these domains**. Enter an asterisk (*) in text box field and click the blue + .



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**:



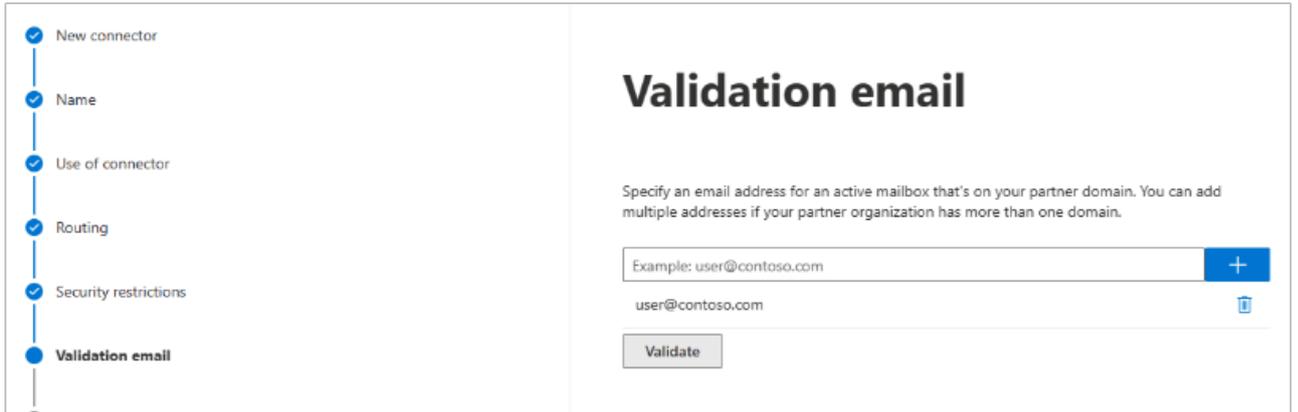
8. Click **Next**. Use the default settings for the **Security restrictions: Always use Transport Layer Security (TLS) to secure the connection (recommended) > Issues by Trusted certificate authority (CA)**:



9. 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:

1. **Test Connectivity** – If this test fails, Outbound Groups is not enabled. Contact [Barracuda Networks Technical Support](#) and request that Outbound Groups be enabled on your Email Gateway Defense account.
2. **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.



10. Once the validation process is complete, click **Next**. Review your settings and then click **Create connector**.

Email Gateway Defense now accepts outbound traffic from Outlook 365.

Step 8. Disable RTF (Rich Text Format) (Optional)

Customers sending outbound mail through Email Gateway Defense can consider disabling Rich Text Format (RTF) on their outbound external mail. When a message is formatted as Rich Text, the attachments will be formatted with TNEF, a Microsoft proprietary encoding that can be configured at the client or organization level. RTF refers to the message format and TNEF refers to the attachment format. RTF encoding can cause issues with attachments converting to `winmail.dat` files which can only be read by other Outlook clients. This can cause problems for outbound content/DLP policies that examine attachments. For example, if an end user sends an email with a PDF attachment that contains a SSN and the email is sent with RTF encoding, Email Gateway Defense would not be able to scan the PDF and identify the SSN to apply a DLP policy. By disabling RTF at the account level, it will force all outbound external mail to be HTML encoded instead.

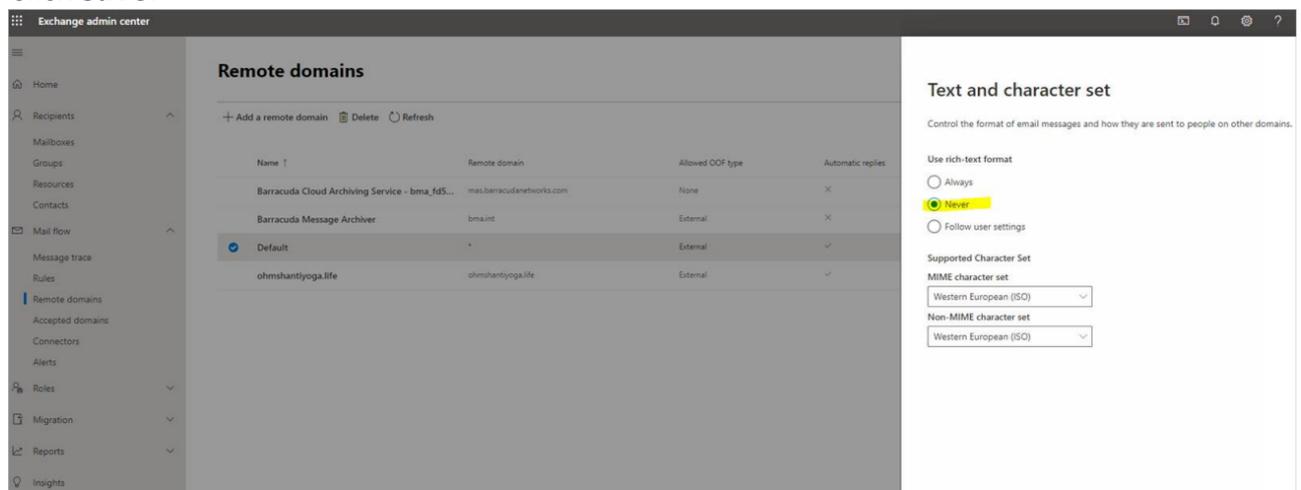
To disable RTF on Exchange Online and Exchange 2013 and newer, use one of the following methods.

- **Powershell Command**

```
Set-RemoteDomain -Identity Default -TNEFEnabled $false
```

- **Exchange Admin Center**

1. Log into the Microsoft 365 [Exchange Admin Center](#).
2. In the left pane, click **Mail flow > Remote domains**.
3. Edit the **Default** remote domain.
4. Under **Text and character set**, select **Never** for **Use rich-text format**.
5. Click **save**.



For additional configuration options and features, log into Email Gateway Defense web interface, and click **Help**.

Your deployment is now complete! [Learn more about Email Gateway Defense](#).

Figures

1. egdTrialHub.png
2. egdWizardSetUpNow.png
3. egdDataCenterRegion.png
4. egdWizardSpecifyMailSvr.png
5. greeCheckMark.png
6. greeCheckMarkVerified.png
7. egd_setup_addMXrecords1.png
8. egd_wizard_addMXrecords1.png
9. greeCheckMark.png
10. greeCheckMarkVerified.png
11. egd_setup_removeMXrecords1.png
12. greeCheckMark.png
13. greeCheckMarkVerified.png
14. AddDomain.png
15. createRule.png
16. egd_ruleConditions.png
17. specifyIP.png
18. ruleConditions.png
19. ruleSettings.png
20. enableRule.png
21. egd_editRuleSettings.png
22. egd_rulePriority.png
23. outboundHost.png
24. MailFlowScenario.png
25. NewConnector2a.png
26. AddSmartHost_Updated.png
27. TLS.png
28. confirmationUpdated1.png
29. ms_newConnector.png
30. ms_ConnectorName1.png
31. ms_UseofConnector2.png
32. ms_ConnectorRouting.png
33. ms_SecurityRestrictions1.png
34. ms_validateEmail1.png
35. disable_rtf.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.