How to Configure Office 365 for Inbound and Outbound Mail

https://campus.barracuda.com/doc/24216132/

You can configure Microsoft Office 365 with the Barracuda Email Security Service as your inbound and/or outbound mail gateway.

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

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

Time Requirement

After you update your MX records, you must wait at least 24-48 hours before starting work on Step 4 below. Plan accordingly.

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

You can also specify the Barracuda Email Security Service as the *outbound mail gateway* through which all mail is sent from your domain via your Office 365 account to the recipient. As the outbound gateway, the Barracuda Email Security Service processes the mail by filtering out spam and viruses before final delivery. By configuring Office 365 as described in **Configure Outbound Mail Flow** below, you instruct the Office 365 mail servers to pass all outgoing mail from your domain to the Barracuda Email Security Service (the gateway server).

Ensure Connectivity and Redundancy\

Open your firewall ports to allow the IP address ranges based on your Barracuda Email Security Service instance ; see Barracuda Email Security Service IP Ranges for a list of ranges based on your Barracuda Email Security Service instance

Step 1. Launch the Barracuda Email Security Service Setup Wizard

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

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

1. When you launch the Essentials wizard, the **Getting Started** page displays. Click **Continue**.
2. The **Link Office 365 Account** page displays. Use this page to connect Essentials to your Office 365 account. Click **Authorize**; the Office 365 login screen displays. Enter your Office 365 admin credentials, and click **Sign in**. In the Office 365 permissions page, click **Accept** to connect Essentials to your Office 365 account.
3. The **Route Outbound Email** page displays. Use this page to create outbound email connectors for domains on your Office 365 account. By default, **Route outbound email for all domains through Barracuda Essentials** is selected and a list of all domains that will be configured displays. Click **Continue**; the wizard verifies your domains and replaces your current MX records with the Barracuda Email Security Service Primary and Backup MX records.

   If you only want to route *inbound* mail through the Barracuda Email Security Service and not your outbound mail, clear **Route outbound email for all domains through Barracuda Essentials**.
4. Click **Continue**. The **Configure Office 365** page displays. Use this page to configure and set up your services. Select from the following options:
   - **Option 1. Allow Barracuda to configure connectors and permissions (recommended)** – Select to automatically configure permissions via PowerShell.
     1. When prompted, log in using your Office 365 admin credentials, and click **OK**.

        Note that if your Office 365 account requires multi-factor authentication (MFA), Barracuda cannot automatically run the PowerShell script.
     2. Once configuration is complete and your Office 365 account authorizes the connection, the **Configuration Summary** displays. Click **OK**.
   - **Option 2. Download and run the Windows PowerShell script** – Select to download and run the PowerShell script from your local system.
     1. Download the Microsoft tools using the provided links.
     2. Download and run the PowerShell script.
     3. When prompted, enter your Office 365 admin credentials.
     4. Once authorized, click **Finish**. The **Essentials** page displays in Barracuda Cloud Control.
   - **Option 3. Manually configure connectors and permissions** – Select to manually configure connectors and permissions.
     1. In Barracuda Cloud Control, click the Barracuda Email Security Service icon, click **Domains**, and click **Add Domain**.
     2. In the dialog box, enter the primary Office 365 **Domain Name** you want to filter, for example: `corpdomain.com`
     3. Enter the **Mail Server** hostname (FQDN) or IP address for the domain entered in the previous step, for example: `corpdomain-com.mail.protection.outlook.com`
     4. Click **Add**.
     5. Click **Verify** in the **Mail Servers** column; the **Domains > Domain settings** page

displays. Select the manner in which to verify the domain ownership:

- **MX Records** – Replace your current MX records with the Barracuda Email Security Service MX records displayed on the verify page.
- **CNAME Records** – Validate your domain by adding a CNAME record.
- **Email to the domain's technical contact** – Send a verification email to the technical contact email address listed on your domain's WHOIS entry.

  This verification option is not available if the Barracuda Email Security Service cannot find your domain's WHOIS entry. If there is not a technical contact, then only the **MX Records**, **CNAME**, and **Email to the Postmaster** options displays on this page.
- **Email to the postmaster** – Send a verification email to the postmaster email address for your domain. The confirmation email will include a link that the recipient can click to verify the domain.

  This option is available if the Barracuda Email Security Service can find your postmaster in your domain's WHOIS records. This method sends a verification email to the postmaster email address for your domain. The confirmation email includes a link that the recipient must click to verify the domain.

6. On the **Domains** page, click **Edit** in the **Settings** column; the **Domains > Domain Settings** page displays where you can complete the configuration.

Step 2. Add Additional Email Domains *(Optional)*

Use the steps in this section *only if you want to manually add additional email domains .*

Obtain the hostname:

1. Log into the Office 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, *cudaware-com.mail.protection.outlook.com*

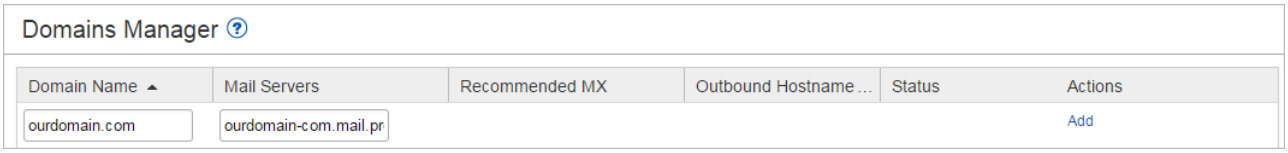
Enter the hostname:

Barracuda 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 Barracuda Email Security Service configuration. This address indicates where the Barracuda Email Security Service should direct inbound mail from the Internet to your Office 365 Exchange server. For example, your domain displays to the Internet as: *bess-domain*.mail.protection.outlook.com

1. Log into the Barracuda Email Security Service as administrator, click **Domains**, and click **Add**

Domain.

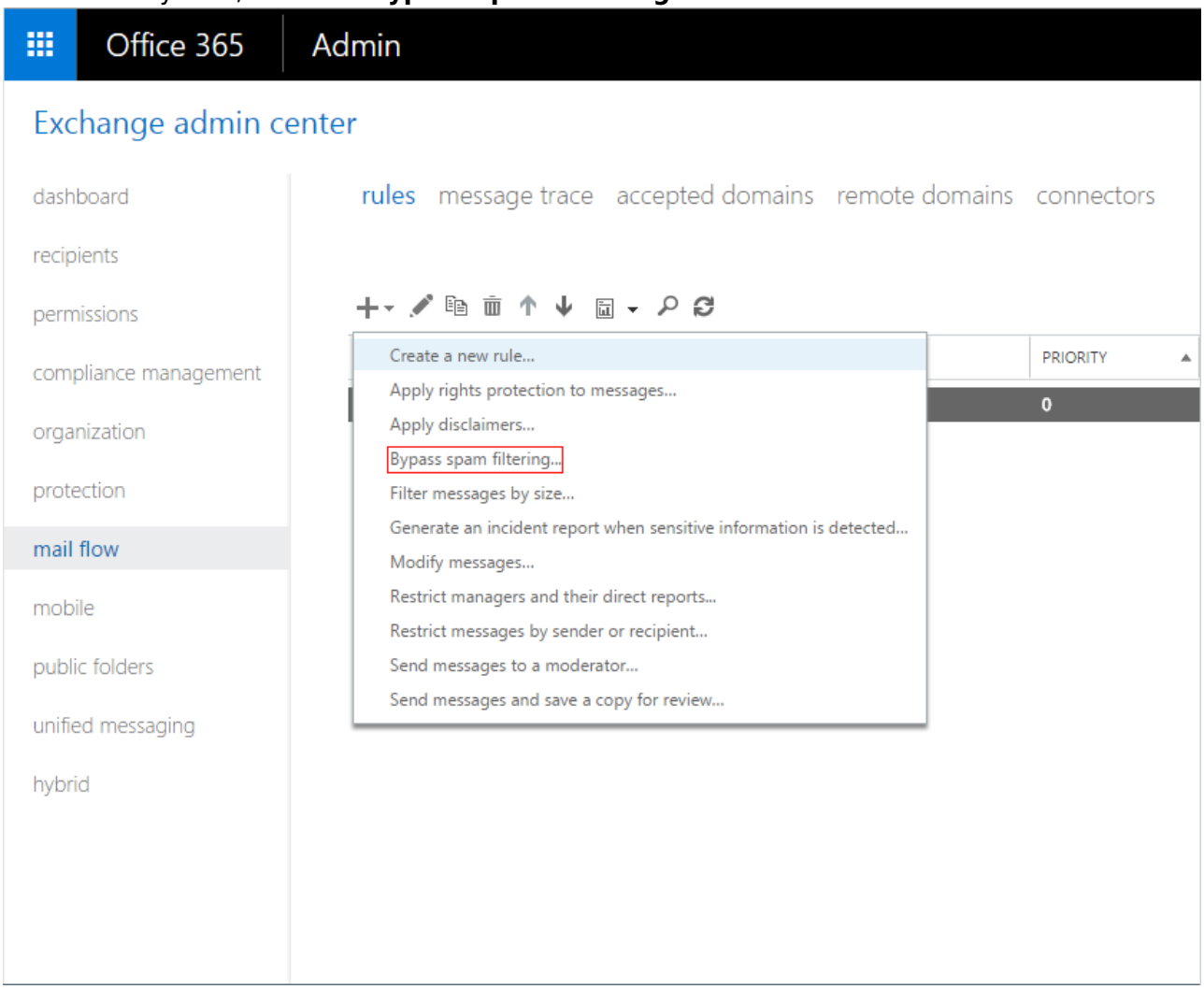
2. Enter the domain name and destination mail server hostname obtained from your Office 365 account:



3. Click **Add**; the **Domain Settings** page displays.

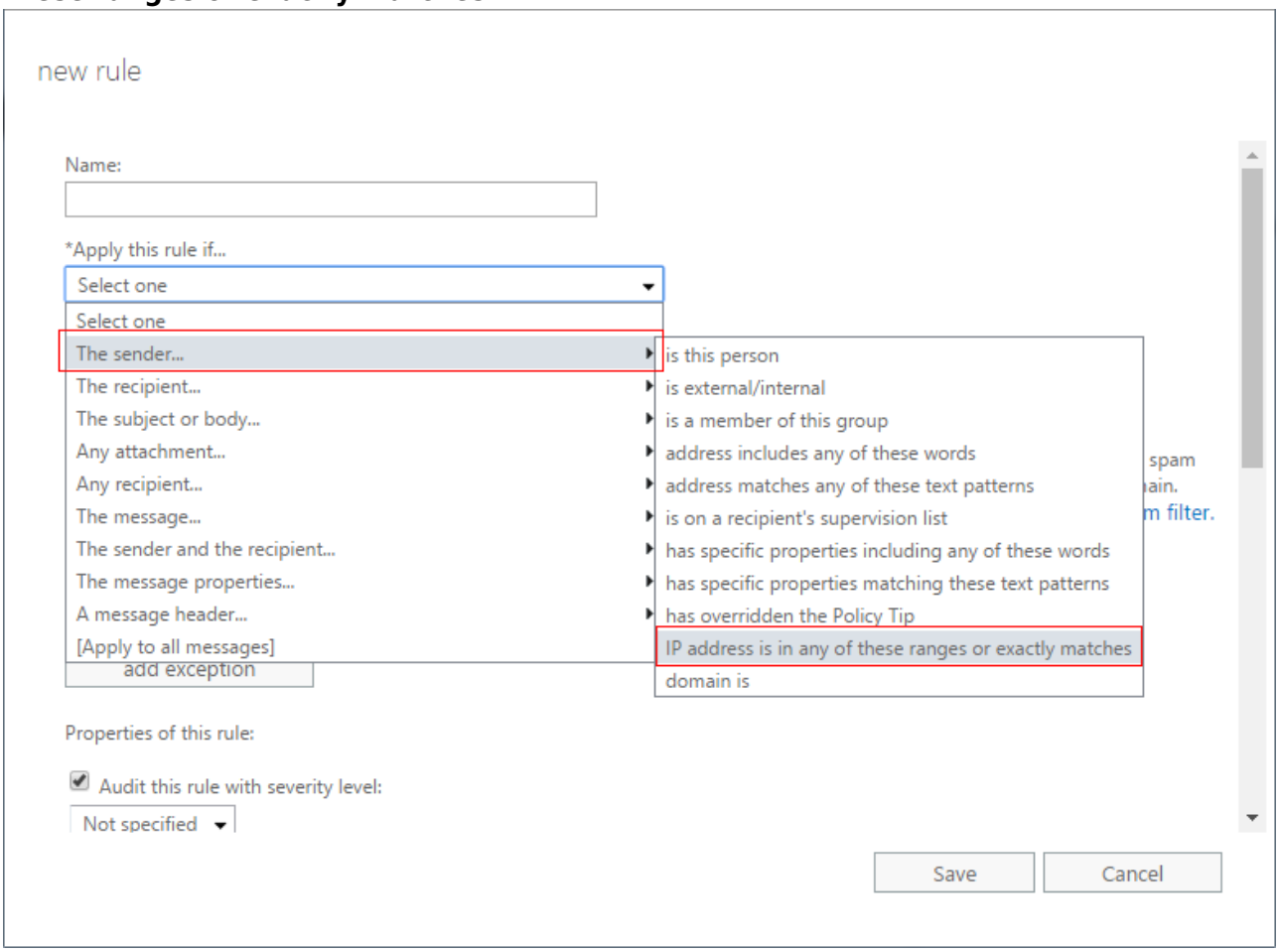
Step 3. Create Transport Rule to Bypass Spam Filtering

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

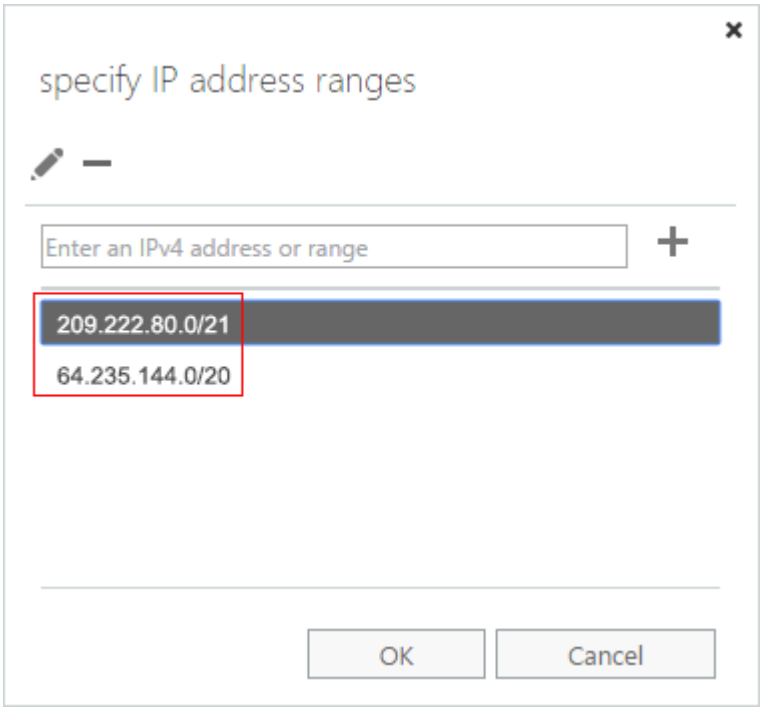


4. In the **new rule** page, enter a **Name** to represent the rule.
5. From the **Apply this rule** drop-down menu, select **The sender > IP address is in any of**

these ranges or exactly matches:



6. In the **specify IP address ranges** page, type `64.235.144.0/20` as the IP address/range for the Sender (Barracuda Email Security Service), and click the **+** symbol.
7. Next type `209.222.80.0/21`, and click the **+** symbol:



8. Click **OK**, and click **Save** to create the transport rule.
9. Click the **Edit** icon for the rule, scroll to the **Properties of this rule** section, and in the **Priority** field, type 0.
10. Click **Save**.
11. Verify the new rule displays at the top of the list of mail flow rules. If the rule is not at the top, click on the rule, and use the **Up** (↑) arrow to move the rule to the top of the list.

Step 4. Restrict Inbound Mail to the Barracuda Email Security Service IP Range

Select the PowerShell script to restrict inbound mail to the Barracuda Email Security Service based on the region selected when setting up the your service. Refer to the Barracuda Email Security Service IP Ranges for the IP ranges corresponding to your region.

Optionally, you can choose to create mail flow rule to restrict inbound access as described in How to Configure Office 365 to Block Inbound Email Not Originating from Barracuda Email Security Service IP Address Range.

IMPORTANT. It is essential that you wait at least 24-48 hours after you update your MX records before you begin working on the steps in this section. That time is needed for the records to propagate and to avoid your mail's being rejected.

PowerShell Script for the US Region

```
# Set-ExecutionPolicy unrestricted
```

```
# $UserCredential = Get-Credential
```

```
# $Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential
$UserCredential -Authentication Basic -AllowRedirection
```

```
# Import-PSSession $Session
```

```
# New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true
-SenderDomains * -SenderIPAddresses
64.235.144.0/24,64.235.145.0/24,64.235.146.0/24,64.235.147.0/24,64.235.148.0/
24,64.235.149.0/24,64.235.150.0/24,64.235.151.0/24,64.235.152.0/24,64.235.153
.0/24,64.235.154.0/24,64.235.155.0/24,64.235.156.0/24,64.235.157.0/24,64.235.
158.0/24,64.235.159.0/24,209.222.80.0/24,209.222.81.0/24,209.222.82.0/24,209.
222.83.0/24,209.222.84.0/24,209.222.85.0/24,209.222.86.0/24,209.222.87.0/24 -
RestrictDomainstoIPAddresses $true
```

PowerShell Script for the German Region

```
# Set-ExecutionPolicy unrestricted
# $UserCredential = Get-Credential
```

```
# $Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential
$UserCredential -Authentication Basic -AllowRedirection
```

```
# Import-PSSession $Session
```

```
New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -
SenderDomains * -SenderIPAddresses
35.157.190.225,35.157.190.226,35.157.190.227,35.157.190.228,35.157.190.229,35
.157.190.230,35.157.190.231,35.157.190.232,35.157.190.233,35.157.190.234,35.1
57.190.235,35.157.190.236,35.157.190.237,35.157.190.238,35.157.190.239,35.157
.190.240,35.157.190.241,35.157.190.242,35.157.190.243,35.157.190.244,35.157.1
90.245,35.157.190.246,35.157.190.247,35.157.190.248,35.157.190.249,35.157.190
.250,35.157.190.251,35.157.190.252,35.157.190.253,35.157.190.254,35.157.190.2
55 -RestrictDomainstoIPAddresses $true
```

PowerShell Script for the UK Region

```
# Set-ExecutionPolicy unrestricted
# $UserCredential = Get-Credential
```

```
# $Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential
```

```
$UserCredential -Authentication Basic -AllowRedirection

# Import-PSSession $Session

New-InboundConnector -Name "Barracuda Inbound Connector" -RequireTls $true -
SenderDomains * -SenderIPAddresses
35.176.92.96,35.176.92.97,35.176.92.98,35.176.92.99,35.176.92.100,35.176.92.1
01,35.176.92.102,35.176.92.103,35.176.92.104,35.176.92.105,35.176.92.106,35.1
76.92.107,35.176.92.108,35.176.92.109,35.176.92.110,35.176.92.111,35.176.92.1
12,35.176.92.113,35.176.92.114,35.176.92.115,35.176.92.116,35.176.92.117,35.1
76.92.118,35.176.92.119,35.176.92.120,35.176.92.121,35.176.92.122,35.176.92.1
23,35.176.92.124,35.176.92.125,35.176.92.126,35.176.92.127 -
RestrictDomainstoIPAddresses $true
```

Alternatively, you can use mail flow rules. Click below for instructions.

Important

After updating your MX records, allow 24 hours before completing the steps in this section to allow the records to propagate.

1. Log into 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 a new rule**.
4. In the **new rule** page, enter a **Name** to represent the rule. For example, type: Barracuda ESS IP restriction
5. Scroll down to and click **More Options**.
6. From the **Apply this rule if** drop-down menu, select **The Sender > Is External/Internal > Outside the organization**.
7. From the **Do the following** drop-down menu, select **Reject this message with the explanation**.
8. Enter the message you want included in the non-delivery report (NDR) that is sent to the sender. For example, enter:
   You have attempted to bypass our Email Security Service. Please ensure your DNS is up-to-date and try sending your message again.
9. Click **Add Exception**.
10. Select **The Sender > Sender's IP address is in any of these ranges or exactly matches**, and enter the Barracuda Email Security Service IP range based on your Barracuda Email Security Service instance.
11. Enter the Barracuda Email Security Service IP range, for example: 64.235.144.0/20

12. Click the **+** symbol.
13. Enter the Barracuda Email Security Service IP range, for example: 209.222.80.0/21
14. Click the **+** symbol.
15. Click **OK**.
16. Scroll to the **Properties of this rule** section, and in the **Priority** field, type: 0
17. Under **Match sender address in message**, select **Envelope**.
18. In the **new rule** page, click **Stop processing more rules**, and click **Save** to create the rule.
19. Office 365 is now configured to block any email that does not originate from the Barracuda Email Security Service IP address ranges.
20. Verify the new rule displays at the top of the list of mail flow rules. If the rule is not at the top, click on the rule, and use the **Up** (↑) arrow to move the rule to the top of the list.

If you complete both Step 3. Create Transport Rule to bypass Spam Filtering and Step 4. Restrict Inbound Mail from Outside Your Organization to the Barracuda Email Security Service IP Range, verify the **Restrict Inbound Mail from Outside Your Organization to the Barracuda Email Security Service IP Range** rule displays *first* in the mail flow rules list, and **Transport Rule to bypass Spam Filtering** displays *second* in the mail flow rule list.

Step 5. Configure Sender Policy Framework for Outbound Mail

To assure Barracuda Networks is the authorized sending mail service of outbound mail from your Barracuda Email Security Service, 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 Email Security Service. See Sender Policy Framework for Outbound Mail for INCLUDE values based on your Barracuda Email Security Service instance.

For example, if you are using Office 365, your record would look similar to:

```
v=spf1 include:spf.protection.outlook.com
include:spf.ess.barracudanetworks.com -all
```

See Sender Authentication for more information.

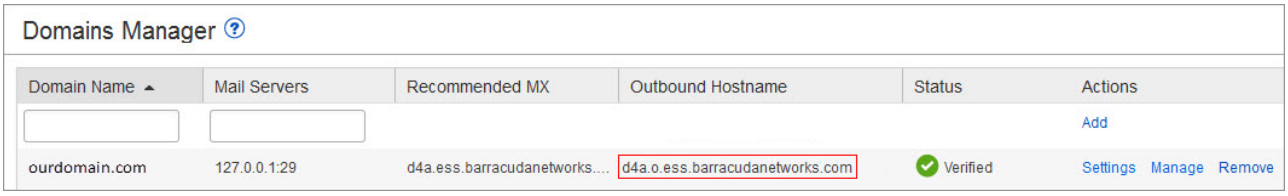
- If you have an SPF record set up for your domain, edit the existing record, and add the following to the INCLUDE line for each domain sending outbound mail based on your Barracuda Email Security Service instance. For example: `include:spf.ess.barracudanetworks.com -all`
- If you do not have an SPF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

Step 6. Configure Outbound Mail

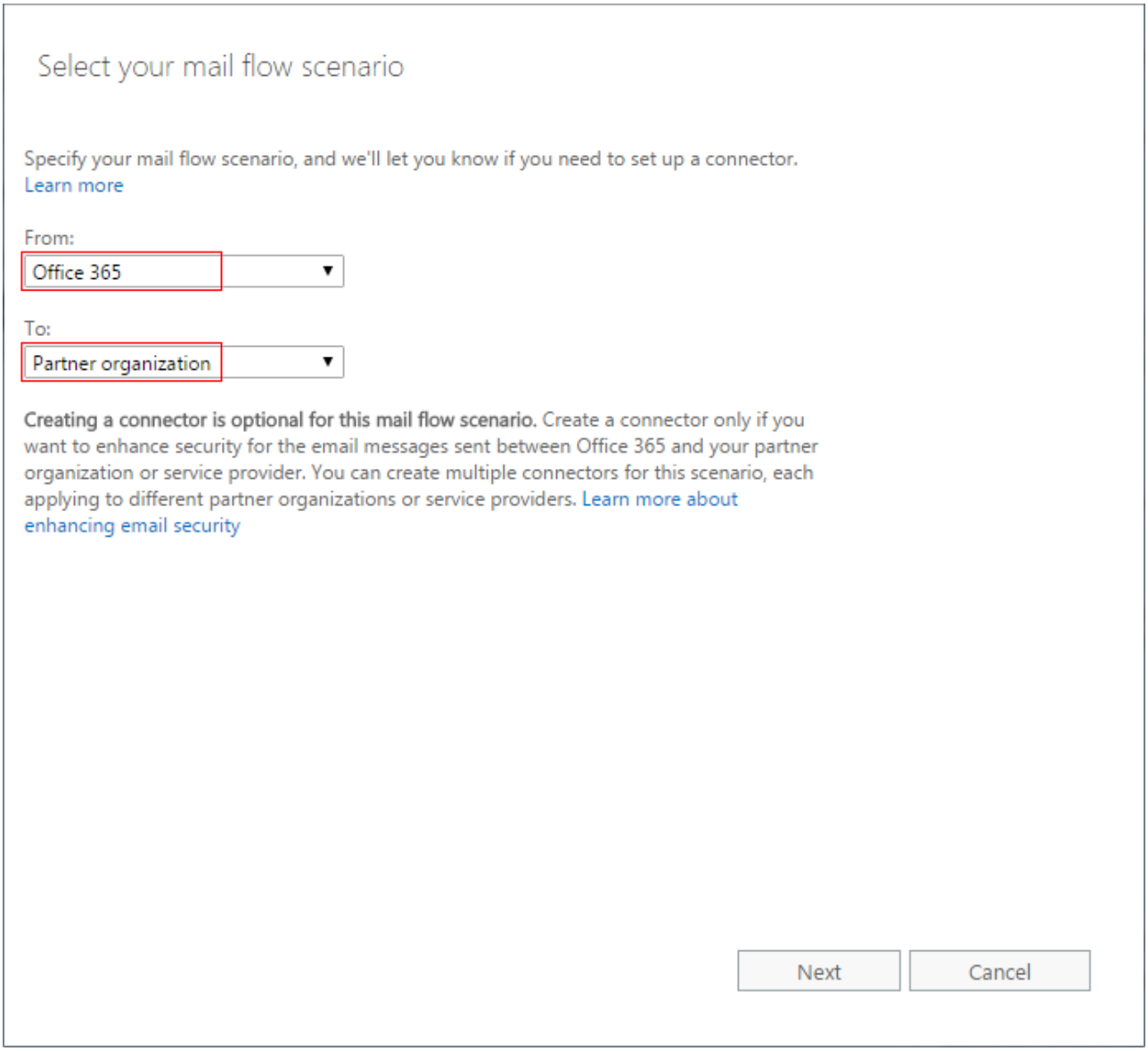
Important

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 Office 365 to Scan Only Selected Domains Outbound. The directions in the section below describe how to filter for all domains for outbound mail.

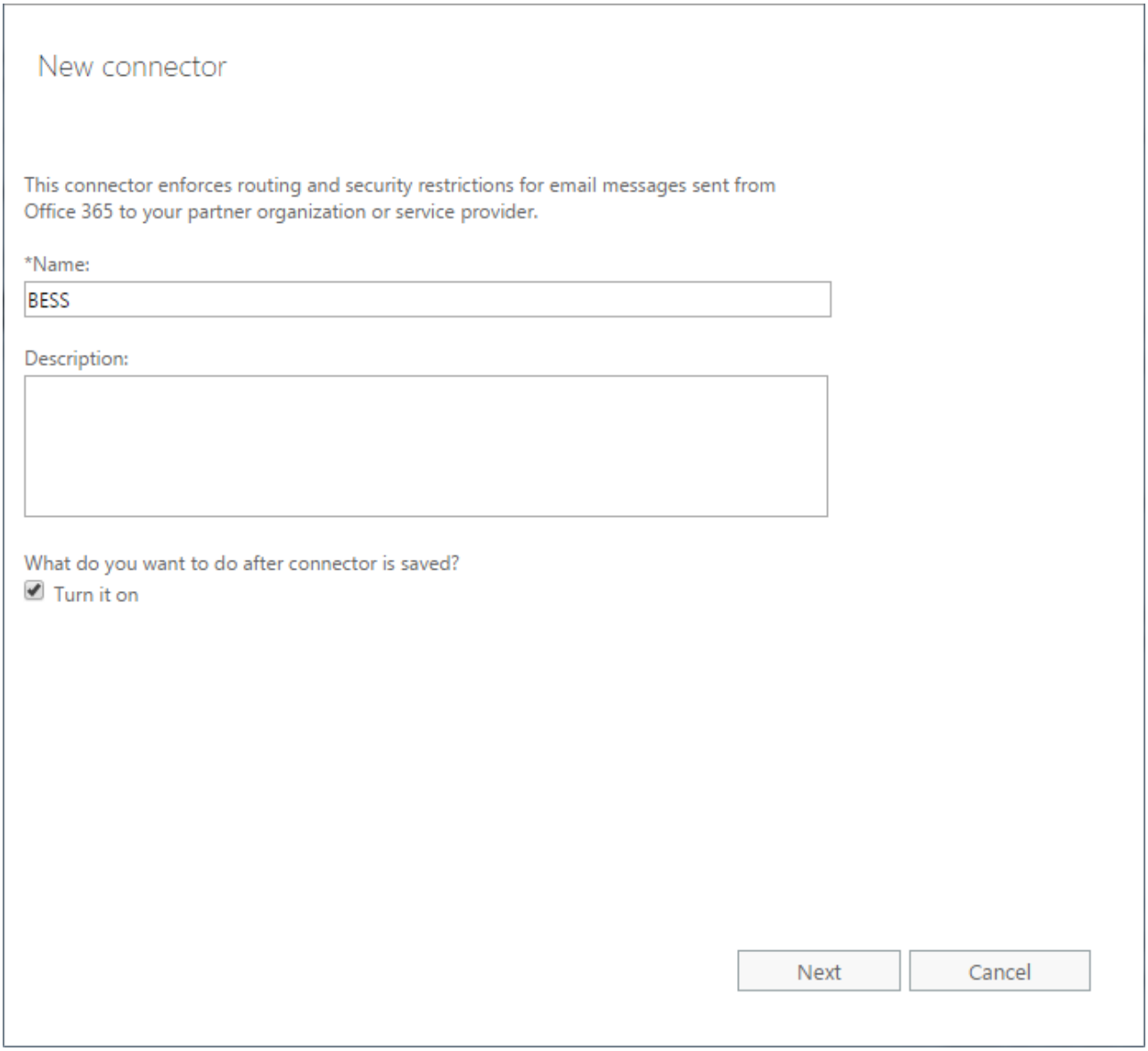
1. If you have not already done so, contact Barracuda Technical Support and request that *Outbound Groups* be enabled on your Barracuda Email Security Service account.
2. Log into the Barracuda Email Security Service, and click **Domains**; make note of the Outbound Hostname:



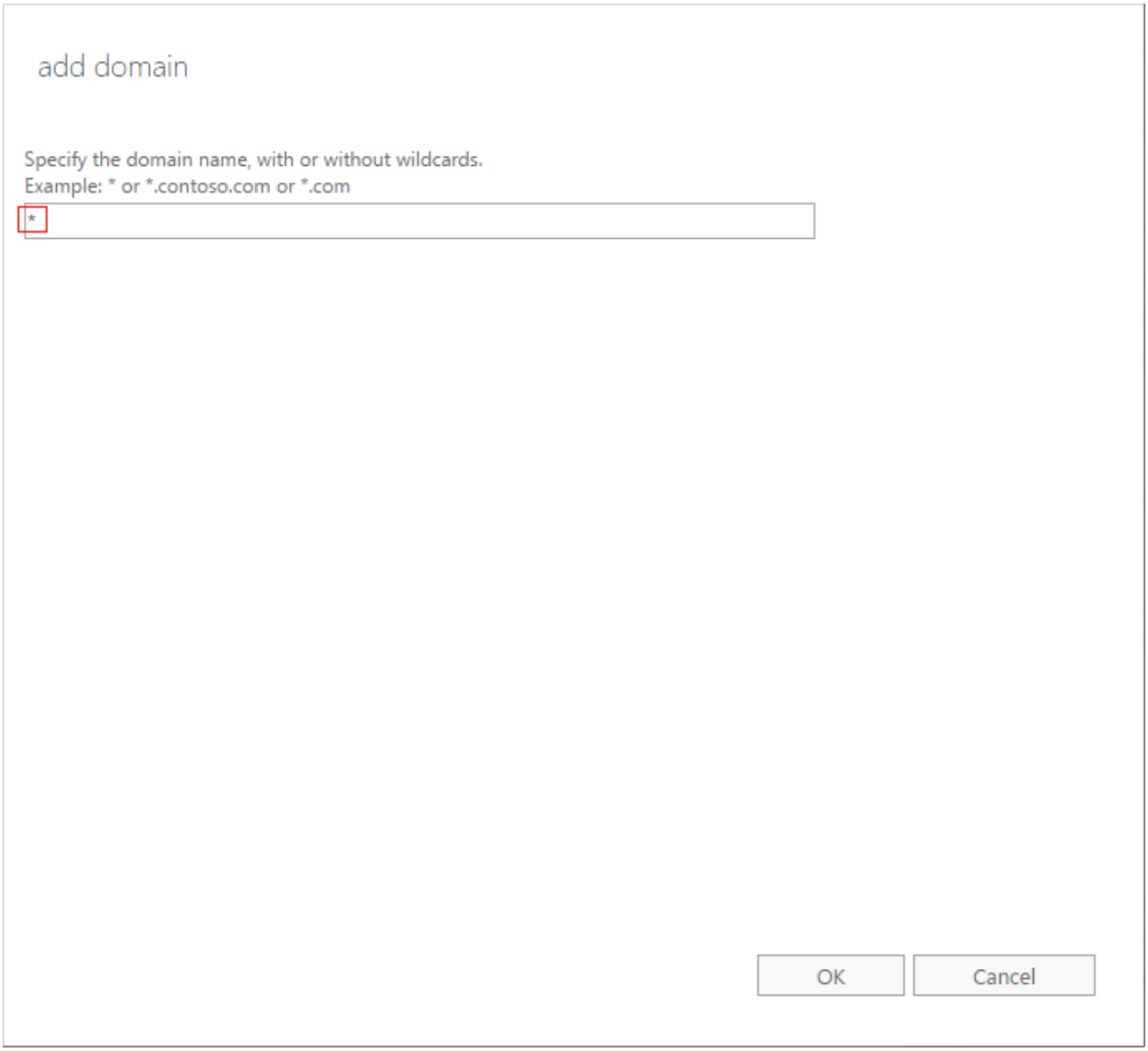
3. Log into the Office 365 admin center, and go to **Admin centers > Exchange**.
4. In the left pane, click **mail flow**, and click **connectors**.
5. Click the **+** symbol, and use the wizard to create a new connector.
6. From the **From** drop-down menu, select **Office 365**, and from the **To** drop-down menu, select **Partner organization**:



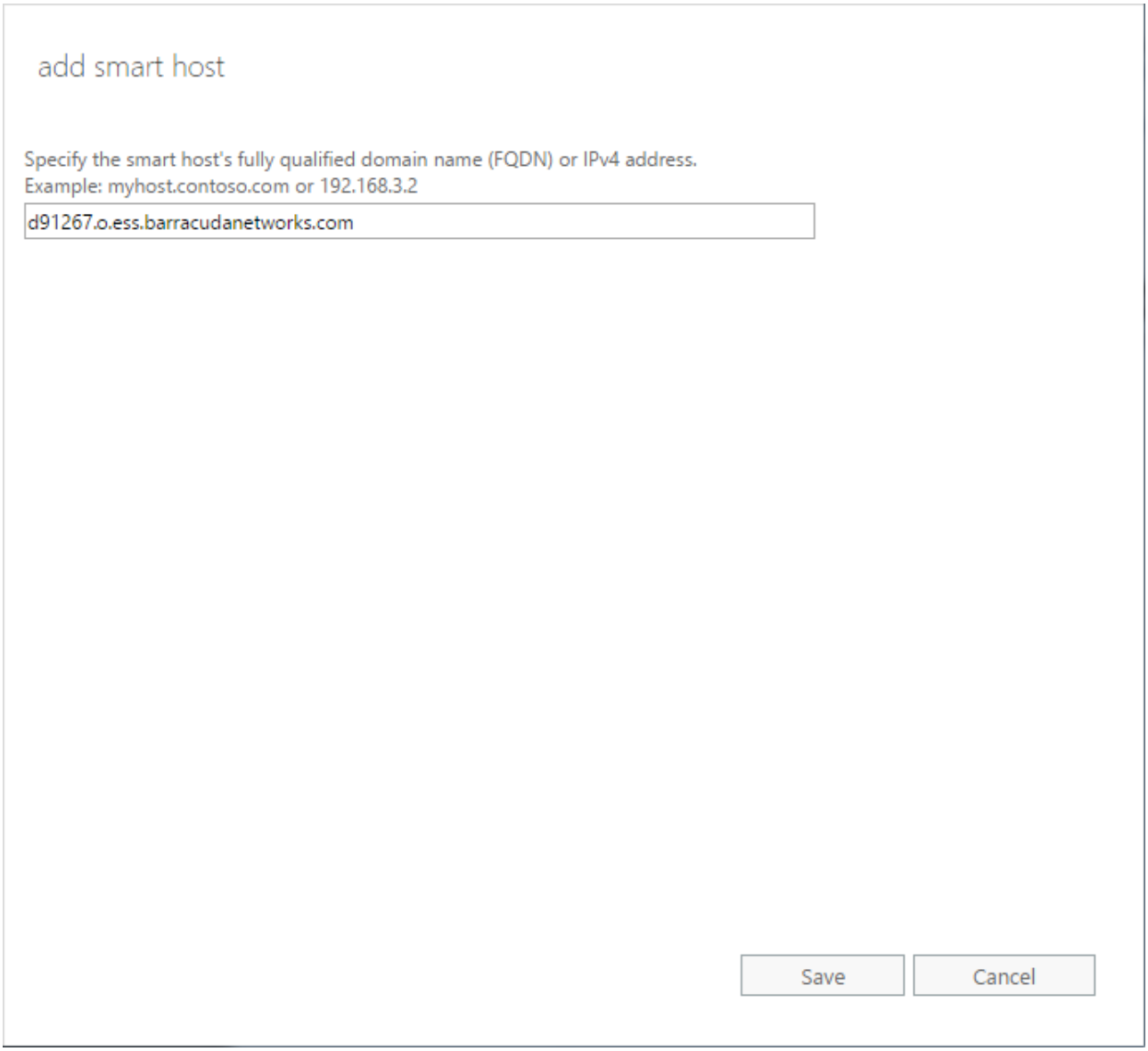
7. Enter a **Name** and (optional) **Description** to identify the connector:



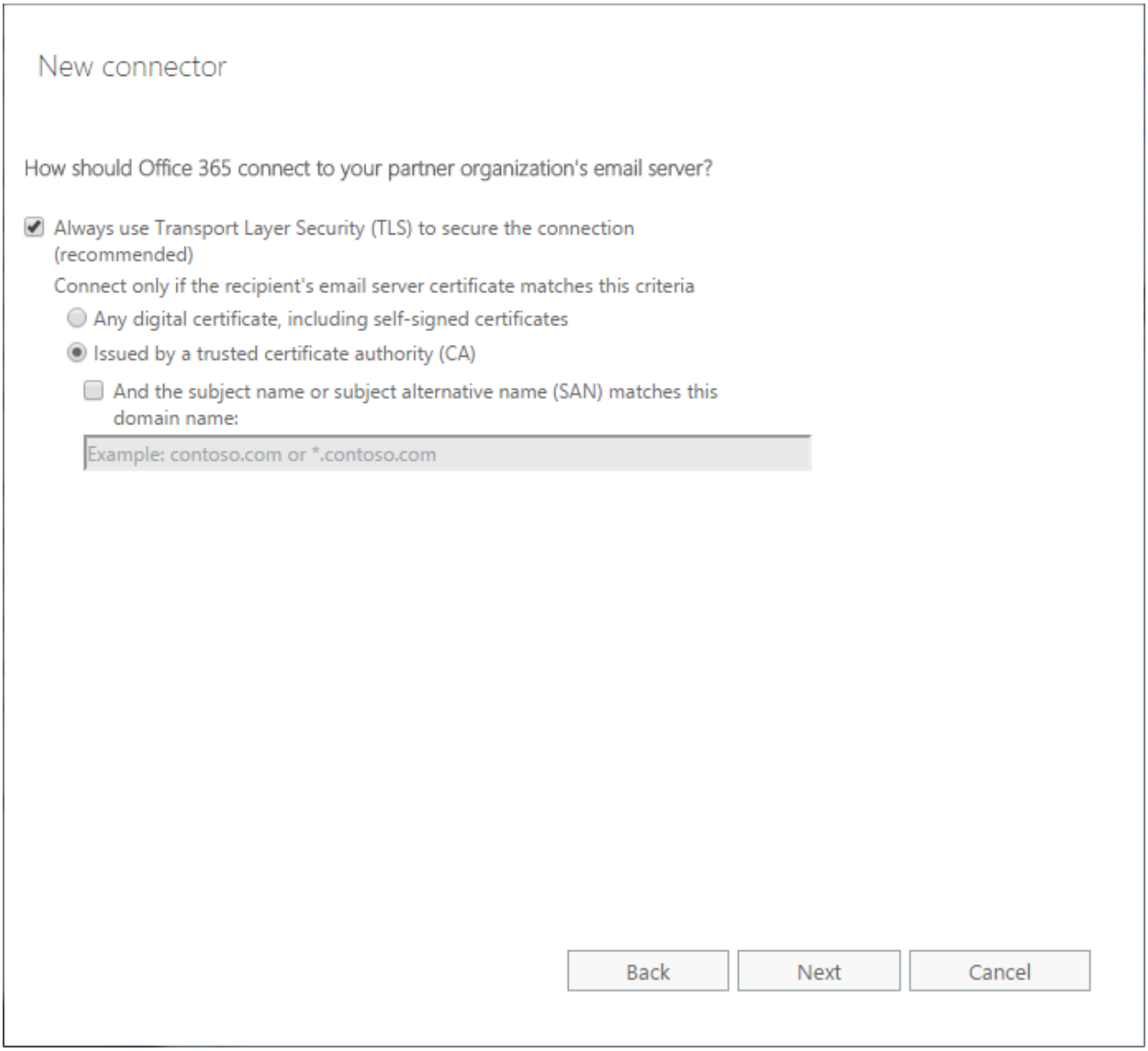
8. Click **Next**. Select **Only when email messages are sent to these domains**, click the **+** symbol, and enter an asterisk (*) in the **add domain** field:



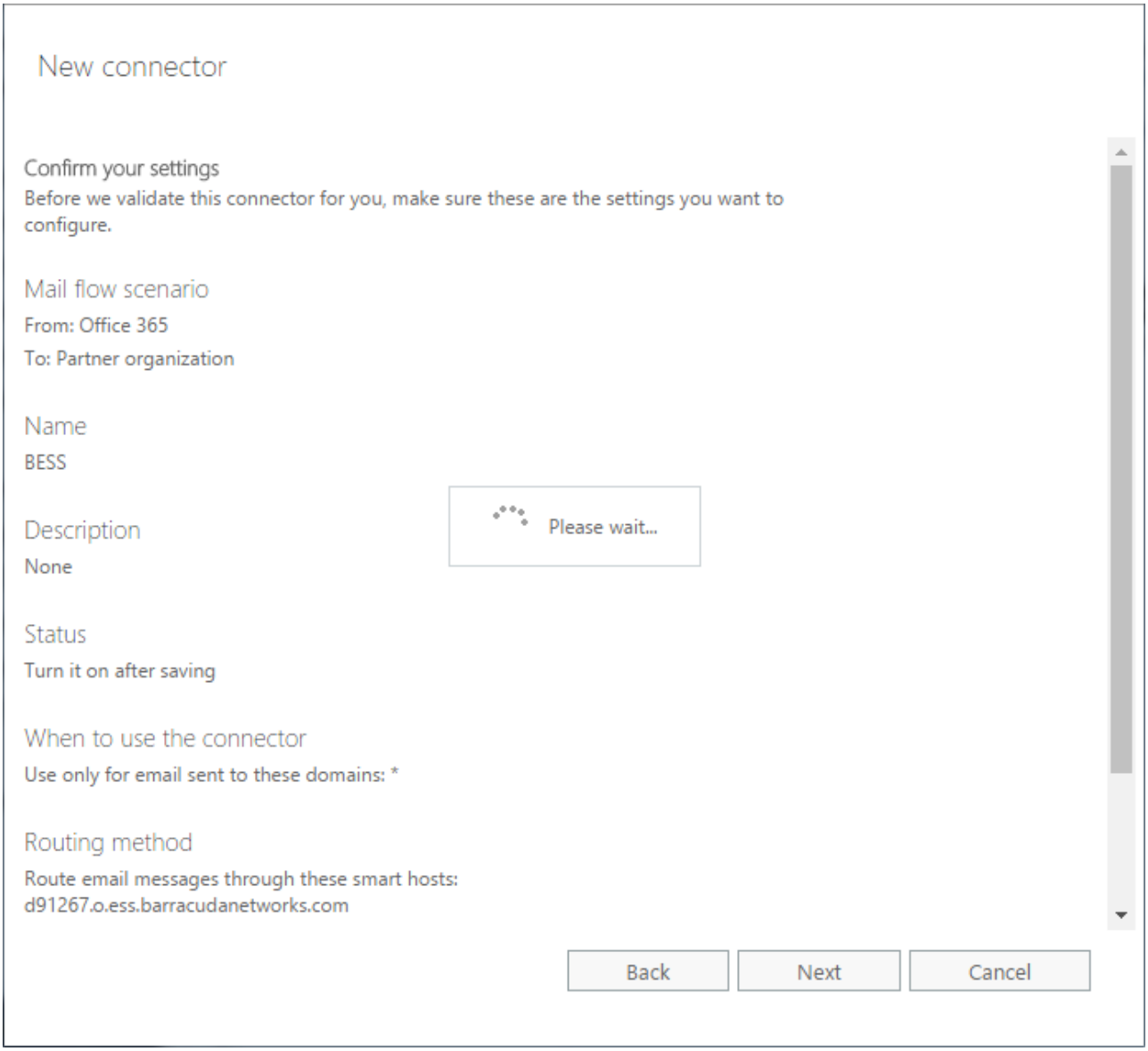
9. Click **OK**, and click **Next**. Select **Route email through these smart hosts**, and click the **+** symbol.
10. Go to the Barracuda Email Security Service, and click the **Domains** tab. Copy your outbound hostname from the MX records, and enter it in the **add smart host** page:



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)**:



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



13. When the verification page displays, enter a test email address, and click **Validate**. Once the verification is complete, your mail flow settings are added.

Barracuda Email Security Service now accepts outbound traffic from Outlook 365.

For additional configuration options and features, log into the web interface, and click **Help**.

Figures

1. hostname.png
2. BypassSpamFiltering.png
3. SenderIPAddress.png
4. SpecifyIPranges.png
5. UpArrow.png
6. UpArrow.png
7. outboundAddress_update.png
8. MailFlowScenario.png
9. NewConnector2.png
10. AddDomain.png
11. AddSmartHost_Updated.png
12. TLS.png
13. confirmationUpdated.png