

## Microsoft 365 Journaling

<https://campus.barracuda.com/doc/46204171/>

This article applies to Barracuda Message Archiver firmware version 5.0 and higher, and Microsoft 365 Enterprise cloud-based mail service, live@edu.

See also:

- [Microsoft 365 Message Encryption](#) to enable journal report decryption

### Hybrid Deployment

Warning! Hybrid deployment can cause duplicate mails in some environments. This is an issue with Hybrid deployment and not with your Barracuda Message Archiver. Contact your Sales or Support representative for more information. If you are using a hybrid Microsoft Exchange Server / Microsoft 365 deployment, where some mailboxes are located on a physical server and some mailboxes are hosted by Microsoft 365, to properly deploy your configuration, you must journal directly to the physical Barracuda Message Archiver from your Exchange Server.

Use the following articles to set up journaling based on the version of Exchange Server running in your environment:

- [How to Configure Envelope \(SMTP\) Journaling for Microsoft Exchange Server 2013 - Standard Journaling](#)
- [How to Configure Envelope \(SMTP\) Journaling for Microsoft Exchange Server 2013 - Premium Journaling](#)
- [Configuring Envelope Journaling for Microsoft Exchange Server 2007 and 2010](#)

## Step 1. Ensure Public Access to Port 25 on the Barracuda Message Archiver

To journal mail directly from Microsoft 365 to your Barracuda Message Archiver, you must have a public IP address and port 25 open and NATed to the Barracuda Message Archiver. Additionally, you can optionally have a public DNS record. You can test this by attempting to telnet to the Barracuda Message Archiver on port 25. You can expect one of three outcomes:

1. If the Barracuda Message Archiver is *not accessible*, either due to port 25 being blocked or incorrectly configured on the firewall, the attempt to telnet simply hangs at **Trying [IP address]**. In this case, troubleshoot your network settings:

```
$telnet 104.209.184.162 25
Trying 104.209.184.162...
```

2. If the Barracuda Message Archiver is *accessible* and you have set **Allow Only Trusted Hosts** on the **Mail Sources > SMTP** page to **No**, telnet establishes a connection to the Barracuda Message Archiver:

```
$telnet 104.209.184.162 25
Trying 104.209.184.162...
Connected to 104.209.184.162.
Escape character is '^]'.
220 barracudaV650.getcuda.com ESMTP Barracuda; Mon, 14 Sep 2015 12:08:12 -0700 (PDT)
```

3. If the Barracuda Message Archiver is *accessible*, you have set **Allow Only Trusted Hosts** on the **Mail Sources > SMTP** page to **Yes**, and you are attempting to telnet from an IP address not listed in the **Trusted SMTP Servers** section, telnet establishes a connection and the connection is immediately closed.

```
$telnet 104.209.184.162 25
Trying 104.209.184.162...
Connected to 104.209.184.162.
Escape character is '^]'.
550 Sender Not Recognized
Connection closed by foreign host.
```

## Step 2. Add Microsoft 365 Endpoints to the Trusted SMTP Servers List

Microsoft publishes a list of IP addresses used for Microsoft 365 endpoints. The endpoints are grouped into four service areas:

- Exchange Online
- SharePoint Online and OneDrive for Business
- Skype for Business Online and Microsoft Teams
- Microsoft 365 Common and Office Online.

See the TechNet article [Microsoft 365 URLs and IP address ranges](#) for further details. Note: For Microsoft 365 Germany endpoints, see the TechNet article [Microsoft 365 Germany endpoints](#).

1. Log into the Barracuda Message Archiver as the administrator, and go to the **Mail Sources > SMTP** page.
2. Click **Bulk Edit**.
3. Go to the TechNet article [Microsoft 365 URLs and IP address ranges](#). Copy and paste the IP addresses based on your Microsoft 365 endpoints.
4. Click **Save**.

## Step 3. Configure SMTP Forwarding Settings

Because this configuration requires the Barracuda Message Archiver to be public-facing, Barracuda Networks strongly recommends that you configure the Barracuda Message Archiver to only accept mail from the list of Trusted SMTP Servers. If you are also receiving mail from

sources other than Microsoft 365, such as an on-premise Exchange server, make sure you add those IP addresses to the list of Trusted SMTP Servers before setting the Barracuda Message Archiver to **Allow Only Trusted Hosts**.

To configure SMTP forwarding settings:

1. Log into the Barracuda Message Archiver as the administrator, and go to the **Mail Sources > SMTP** page.
2. In the **SMTP Forwarding Settings** section, set **Allow Only Trusted Hosts** to **Yes**.
3. Click **Save**.

## Step 4. Configure Local Domains

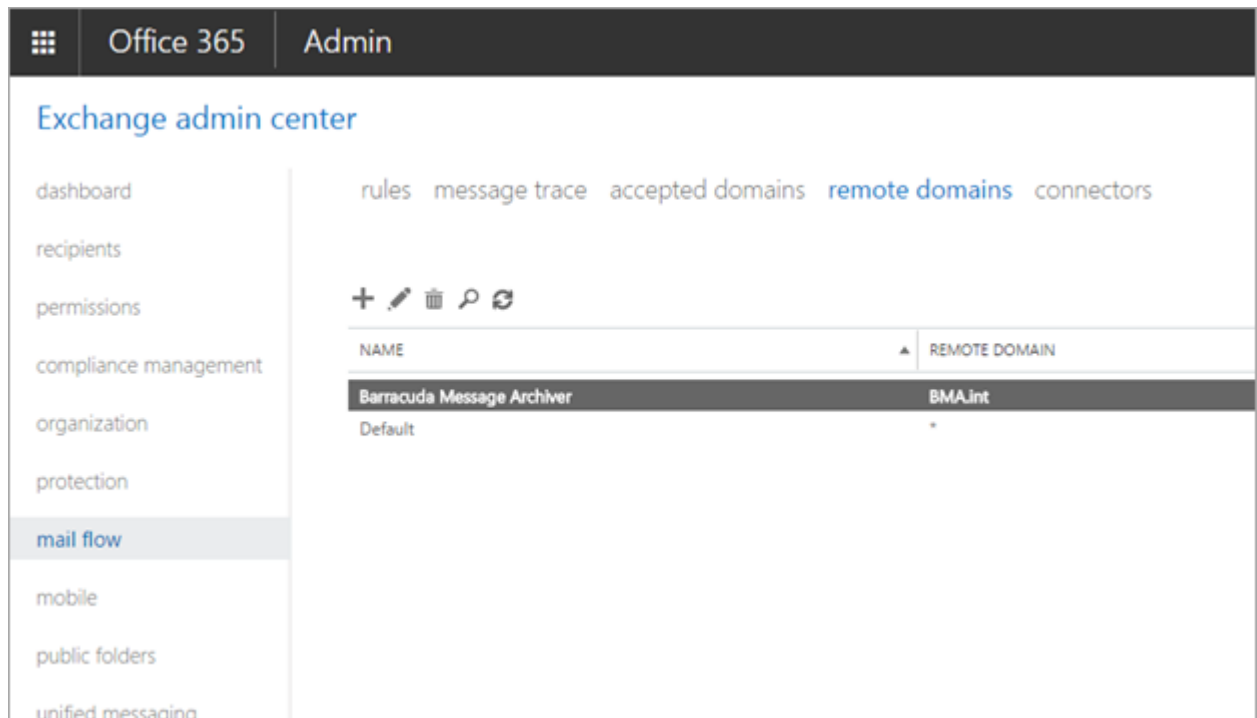
1. Log into the Barracuda Message Archiver as the administrator, and go to the **Basic > IP Configuration** page.
2. In the **Local Domains** section, add all of your mail-enabled domains including your *onmicrosoft.com* domain, as well as your non-routable domain, for example, *bma.int*.
3. Click **Add** after each domain entry, and then click **Save**.

## Step 5. Configure SMTP Over TLS/SSL (Optional)

1. Log into the Barracuda Message Archiver as the administrator, and go to the **Advanced > SMTP Configuration** page.
2. In the **SMTP Over TLS/SSL** section, set **Enable SMTP over TLS/SSL** to **Yes**.
3. Click **Save**.

## Step 6. Create a Remote Domain

1. Log into the Exchange admin center (EAC), and click **mail flow > remote domains**:



2. Click the + symbol, and in the **new remote domain** dialog box, configure the following options:
  1. **Name** - Type Barracuda Message Archiver
  2. **Remote Domain** - Type BMA.int or any non-routable domain
  3. **Out of Office automatic reply types** - Select **None**
  4. **Automatic replies** - Select **Allow automatic forwarding**
  5. **Message reporting** - Clear all options
  6. **Use rich-text format** - Select **Never**
  7. **MIME Character Set** - Select **None**
  8. **Non-MIME Character Set** - Select **None**

new remote domain

Specify a domain that will be considered remote when mail is received.

\*Name:

\*Remote Domain:

Out of Office automatic reply types:

☒ None  
☐ Allow only external Out of Office replies  
☐ Allow internal Out of Office replies

Automatic replies:

☐ Allow automatic replies  
☒ Allow automatic forwarding

Message reporting:

☐ Allow delivery reports  
☐ Allow non-delivery reports  
☐ Allow meeting forward notifications

Use rich-text format:

☐ Always  
☒ Never  
☐ Follow user settings

Supported Character Set  
MIME character set:

Non-MIME character set:

3. Click **Save**.

## Step 7. Create a Send Connector for the Remote Domain

1. Log into EAC, and click **mail flow > connectors**.
2. Click the + symbol. In the **Select your mail flow scenario** page, configure the following options:
  1. **From** – Select **Office 365**

## 2. To – Select **Your organization's email server**

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:

You need to create a connector for this mail flow scenario. Because your domain's MX record points to Office 365, you must set up an alternative server (called a smart host) so that Office 365 can send email to your organization's email server (also called on-premises server). To complete the scenario, you might need to configure your email server to accept messages delivered by Office 365. [Learn more about configuring your email server](#)

### 3. Click **Next**. In the **New connector** page, Configure the following options:

1. **Name** – Type Barracuda Message Archiver
2. **What do you want to do after connector is saved** – Select both **Turn it on** and **Retain internal Exchange email headers (recommended)**:  
Ensure the **Turn it on** check box is selected, otherwise the connector will fail to validate and will not send a test message.

### New connector

This connector lets Office 365 deliver messages to your organization's email server.

\*Name:

Description:

What do you want to do after connector is saved?

☒ Turn it on

☒ Retain internal Exchange email headers (recommended)

4. Click **Next**. In the **New Connector** page, select **Only when email message are sent to these domains**.
5. Click the **+** symbol. Enter the non-routable domain configured in [Step 6](#) (for example, `bma.int`), and click **OK**:


## New connector

When do you want to use this connector?

☐ Only when I have a transport rule set up that redirects messages to this connector

☐ For email messages sent to all accepted domains in your organization

☒ Only when email messages are sent to these domains

+

-

bma.int

BackNextCancel

- Click **Next**. In the **New connector** page, click the **+** symbol. Type your public FQDN or IP Address assigned to your Message Archiver. For example, `archiver.getcuda.com`. Click **Save**:



### New 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](#)

+ ✎ -

archiver.getcuda.com

Back

Next

Cancel

- Click **Next**. In the **New connector** page, select **Always use Transport Layer Security (TLS)** and **Any digital certificate, including self-signed certificates**:

Note that this step is optional and only applies if you enabled SMTP Over TLS/SSL in [Step 5](#).

If you previously configured a certificate from a trusted certificate authority, select the **Issued by a trusted certificate authority (CA)** option.

### New connector

How should Office 365 connect to your 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

8. Click **Next**. Verify your settings in the summary page, and click **Next**.
9. Click the **+** symbol in the **Validate this connector** page, type test@[non-routable domain] , and click **OK**:


### New connector

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

Specify an email address for an active mailbox that's on your email server. You can add multiple addresses if your organization has more than one domain.

+



–

test@bma.int

Back

Validate

Cancel

10. Click **Validate**.

11. In the **New connector** validation results page, verify the connector **Status** displays as **Succeeded**, and click **Finish**.

## Step 8. Create a Non-Delivery Report Recipient

Before creating journal rules, specify a journal recipient for non-delivery reports (NDRs) to reduce the risk of losing journal reports:

## Warning

Any mail sent to the address used for undeliverable journal reports won't be journaled and won't honor transport and mailbox rules settings. It's recommended that you create a dedicated mailbox for undeliverable journal reports.

OK

### To create an NDR recipient:

1. Log into the Microsoft Purview compliance portal, navigate to **Solutions > Data lifecycle management > Exchange (legacy)**.
2. Click the **Settings** icon.
3. In **Send undeliverable journal reports to**, enter the email address of a valid user account. **Note** that the mailbox must be a mail user, mail contact, or external user, *not* an Exchange Online Mailbox.
4. Click **Save**.

## Step 9. Configure Journaling

1. Log into the Microsoft Purview compliance portal, navigate to **Solutions > Data lifecycle management > Exchange (legacy) > Journal rules**, and then select **+ New rule**.
2. On the **Define journal rule settings** page, provide a name for the journal rule and then configure the following options:
  1. **Send journal reports to** - Type `journal@[non-routable domain]`. For example, type: `journal@bma.int`
  2. **Journal rule name** - Type Barracuda Message Archiver
  3. **Journal messages sent or received from** - Select **Apply to all Messages**.
  4. **Type of message to journal** - Select **All Messages**.
3. Select **Next**, review the settings, and then click **Submit** to create the journal rule.

## Figures

1. telnet\_port\_25\_blocked.png
2. telnet\_port\_25\_open\_all.png
3. telnet\_port\_25\_open0365.png
4. 365\_02.png
5. CreateRemoteDomain.png
6. SelectMailFlow.png
7. NewConnector.png
8. AddDomain.png
9. GetCuda.png
10. Certificate.png
11. Validate.png
12. ndr\_warning.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.