How to configure Office 365 SMTP Relay for Multi Functional Devices (Printers, Scanners etc.)

[@techpress](https://techpress.net/author/techpress/)

October 10, 2020

[0](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "respond)

[Office 365](https://techpress.net/category/office-365/)

August 19, 2021

Table of Contents

* [Configuration Options](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "configuration-options)
  + [SMTP Authenticated Submission](https://techpress.net/office-365-smtp-relay-setup-and-configuration/#smtp-authenticated-submission)
  + [Direct Send Method](https://techpress.net/office-365-smtp-relay-setup-and-configuration/#direct-send-method)
  + [Create a connector on Office365](https://techpress.net/office-365-smtp-relay-setup-and-configuration/#create-a-connector-on-office365)
* [References:](https://techpress.net/office-365-smtp-relay-setup-and-configuration/#references)
  + [Check SMTP Auth at organization level](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "check-smtp-auth-at-organization-level)
  + [Check SMTP Auth at Mailbox level](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "check-smtp-auth-at-mailbox-level)
* [Troubleshooting](https://techpress.net/office-365-smtp-relay-setup-and-configuration/#troubleshooting)
  + [Delisting / Unblock of ISP Public IP on https://sender.office.com](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "delisting-unblock-of-isp-public-ip-on-httpssenderofficecom)
  + [Delisting / Unblock of ISP Public IP on Spamhaus.org](https://techpress.net/office-365-smtp-relay-setup-and-configuration/#delisting-unblock-of-isp-public-ip-on-spamhausorg)

When you move all mailboxes to the office365 (“cloud”), the next thing in your task is to migrate the SMTP Relay Service. If you plan to keep your existing on premise exchange server then it can be used / utilized as a SMTP Relay server. Else, if you plan to decommission the exchange server for good, in that case you can utilize Office365 as a SMTP Relay server to relay the emails.

There are three methods which you can use to configure / utilize Office 365 SMTP Relay Service. Any of the given methods can be used to configure the SMTP Relay. However, each one is having a different set of configuration and requirements. I will show you how to configure it using all the three methods. Depending upon your requirement, select the best option and configure it for your Devices like Printers/scanners/Application Servers/Powershell or any other Scripts or Tools which you are using in your environment.

Configuration Options

SMTP Authenticated Submission

* **Easiest to setup**, No extra configuration or steps required in Office365.
* A **Licensed Office365 User Mailbox** is required (This will be the from address which will be used to send the emails).
* Use this option if you want to send the emails **within your organization as well as outside your organization**.
* Send the Email from any location or IP.
* [SMTP Auth must be Enabled on Organisation or Mailbox Level.](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "Smtp)
* **Device must support TLS 1.2** or above (Please check the vendor documentation to confirm this).
* SMTP Authenticated Submission cannot be used to send bulk email or newsletters.
* Firewall must allow **Port 587 or Port 25**.

Once you confirm that you are meeting the above mentioned requirements, Go ahead and configure the device to send the emails using below information.

Direct Send Method

* Requires **Static Public IP Address** of your Device or Server or the Application.
* Firewall must allow Port 25 from Client to Office365.
* **MX Endpoint** of your domain.
* No Office365 Mailbox is required.
* Make sure the DNS IP Addresses set on the printer are reachable.
* [Create a](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "bypass)**[Rule](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "bypass)**[on office365 to bypass spam filtering for the email address configured on the Printer to send the emails (Scroll down to the page to check the screenshot of how to create this rule.](https://techpress.net/office-365-smtp-relay-setup-and-configuration/" \l "bypass)
* [Troubleshooting](https://techpress.net/office-365-smtp-relay-setup-and-configuration/#trouleshooting)

Once you meet all the above requirements and noted down the points. You can start configuration of Direct Send SMTP Relay.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SMTP Server** | **Port** | **TLS/StartTLS** | **UserName** | **Password** |
| yourdomain-com.mail.protection.outlook.com | 25 | Not Required (Recommendation is to enable if this option is available) | **SMTP From Address**. Please specify any email ID from your verified domain. For Example: if your domain is techpress.net then you can use any name before @ sign e.g. **myscanner@techpress.net** | Not required (you can turn off SMTP Authentication) |

1. You can find the **MX Endpoint** of your domain from office365 portal by clicking on **Setup -> Domains and Click on the your company domain**. This will open below page, you can copy the **Point to address or value** for MX record Type

2. Add Static Public IP Address of your Device or Server or the Application to SPF Record [**Optional**]

**Let’s take an example**: Your Office Public IP Address is 1.2.3.4 and your server or application or printer /scanner is in the office so it will use the Public IP address 1.2.3.4 to go out and communicate with office365. Therefore, include the IP Address 1.2.3.4 in your SPF Record so that your emails are not marked as SPAM.

Note: Well, this is optional but recommended step to perform, and if your emails are landing in the SPAM folder you can configure this.

v=spf1 ip4:1.2.3.4 include:spf.protection.outlook,com -all

3. If your emails are still going into the **SPAM** folder. Please create a **SPAM Bypass rule** on office365 for the email ID which you have used to send the email from. **Login to Exchange online management portal ->**  **click mail flow -> Rule -> Create a Rule**.

**Example of Direct Send (Screenshot from Printer Configuration)**

**Create Bypass Spam Filtering Rule**

Create a connector on Office365

* **Static Public IP Address** of your Device or Server or the Application.
* **Firewall must allow Port 25** from Client to Office365.
* **MX Endpoint** of your domain.
* No Office365 Mailbox is required.
* A **Connector will need to be created on office365** for accepting the email from the Static Public IP noted before.

Once A connector is configured then use below settings on the device to configure for SMTP Service.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SMTP Server** | **Port** | **TLS/StartTLS** | **UserName** | **Password** |
| yourdomain-com.mail.protection.outlook.com | 25 | Not Required (Recommendation is to enable if this option is available) | **SMTP From Address**. Please specify any email ID from your verified domain. For Example: if your domain is techpress.net then you can use any name before @ sign e.g. **myscanner@techpress.net** | Not required (you can turn off SMTP Authentication) |

Well, Mostly its a **direct Send Method + A Connector on Office365** which will be required so that you can send the email to external users. Please follow below instructions to create a connector:

* Logon to [**Microsoft Office365 Exchange Online Portal**](https://outlook.office365.com/ecp/) with admin rights.
* Click on **mail flow** and then **connectors** tab.
* Click on **+**Sign to create a **New Connector**
* Select From: **Your Organization’s email Server** and To: **Office365**
* Provide appropriate name to this connector e.g <companyname> SMTP Relay
* Select the Option “**By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization**“
* Add the Static Public IP noted earlier.
* Click **Save** to Save this connector.
* Its [Optional] but recommended to add this Static Public IP Address to your SPF Record.
* If your emails are still going into the **SPAM** folder. Please create a **SPAM Bypass rule** on office365 for the email ID which you have used to send the email from. Go to **mail flow -> Rule -> Create a Rule**.

References:

Check SMTP Auth at organization level

Get-TransportConfig | Format-List SmtpClientAuthenticationDisabled

Check SMTP Auth at Mailbox level

Get-CASMailbox "Jatin Makhija" | fl SmtpClientAuthenticationDisabled

In my case you can see its blank, That means this setting is controlled by the corresponding **SmtpClientAuthenticationDisabled** parameter on the**Set-TransportConfig** cmdlet for the whole organization.

**External Links:**

[SMTP Auth Client Submission](https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission" \t "_blank)

Troubleshooting

* Launch Command Prompt on the PC (IP of the PC should be in the same subnet as printer)
* Type Command **telnet <MX EndPoint> 25** and press Enter. (*If telnet command is not recognized on the Windows 10 PC. The Please first Install Telnet Client by going to****Start menu -> Type “Turn Windows featured on or off”****and****find Telnet Client, Select it and click OK***)

**For Example:**

Once you enter on the above command, you should get a response from the server. On the console type **ehlo**

Then type **mail from** and **rcpt to** and try to send the email (*as shown in below screenshot*). If it works fine then there are no issues with the port / email delivery and it could be issue directly related to printer.

Use below commands to send a test email using telnet.

ehlo

MAIL FROM:<myscanner@techpress.net>

250 2.1.0 Sender OK

RCPT TO:<internal email ID>

250 2.1.5 Recipient OK

DATA

354 Start mail input; **end** with <CRLF>.<CRLF>

SUBJECT:Hello World

**This** is a test message

Thanks,

Jatin

. <Dot to **end** the email>

Delisting / Unblock of ISP Public IP on https://sender.office.com

As you will see in the screenshot, I tried to send a test email and our ISP Public IP seems to be banned, due to this email from printer was not getting delivered. To get the IP out of the banned list. Login to **https://sender.office.com/** and type email ID and IP address, follow the Instructions to get it DE-listed. It took me around 30 minutes to get the IP DE-listed but it may take longer.

After requesting DE-listed of my ISP Public IP on **Office 365 Anti-Spam IP Delist Portal** (<https://sender.office.com/>) and waiting for approx. 30 minutes, I tried to send the email again using telnet protocol and this time it was a success:

Delisting / Unblock of ISP Public IP on Spamhaus.org

You can also encounter blocking of ISP Public IP on **https://www.spamhaus.org/query/ip/<ISP Public IP Address>**. Replace ISP Public IP Address with your Public IP Address and check if this is blocked and follow below process to Delist / Unblock it.

Once you land on **https://www.spamhaus.org/query/ip/<ISP Public IP Address>** site. You can see below page. Click on **Show details** and then click on “**I am running my own mail server**“