How to set up a multifunction device or application to send email using Microsoft 365 or Office 365

8/10/2020 • 18 minutes to read • Edit Online

Prerequisites: Office 365 or Microsoft 365 subscription, Exchange Online Plan

This article explains how you can send email from devices and business applications when all of your mailboxes are in Microsoft 365 or Office 365. For example:

- You have a scanner, and you want to email scanned documents to yourself or someone else.
- You have a line-of-business (LOB) application that manages appointments, and you want to email reminders to clients of their appointment time.

Option 1 (recommended): Authenticate your device or application directly with a Microsoft 365 or Office 365 mailbox, and send mail using SMTP AUTH client submission

> **NOTE**
>
> This option is not compatible with Microsoft Security Defaults or multi-factor authentication (MFA). If your environment uses Microsoft Security Defaults or MFA, we recommend using Option 2 or 3 below.
>
> You must also verify that SMTP AUTH is enabled for the mailbox being used. See Enable or disable authenticated client SMTP submission (SMTP AUTH) in Exchange Online for more information.

This option supports most usage scenarios and it's the easiest to set up. Choose this option when:

- You want to send email from a third-party hosted application, service, or device.
- You want to send email to people inside and outside your organization.

To configure your device or application, connect directly to Microsoft 365 or Office 365 using the SMTP AUTH client submission endpoint **smtp.office365.com**.

Each device or application must be able to authenticate with Microsoft 365 or Office 365. The email address of the account that's used to authenticate with Microsoft 365 or Office 365 will appear as the sender of messages from the device or application.

How to set up SMTP AUTH client submission

Enter the following settings directly on your device or in the application **as their guide instructs** (it might use different terminology than this article). As long as your scenario meets the requirements for SMTP AUTH client submission, the following settings will enable you to send email from your device or application.

DEVICE OR APPLICATION SETTING	VALUE
Server/smart host	smtp.office365.com
Port	Port 587 (recommended) or port 25

DEVICE OR APPLICATION SETTING	VALUE
TLS/StartTLS	Enabled
Username/email address and password	Enter the sign in credentials of the hosted mailbox being used

TLS and other encryption options

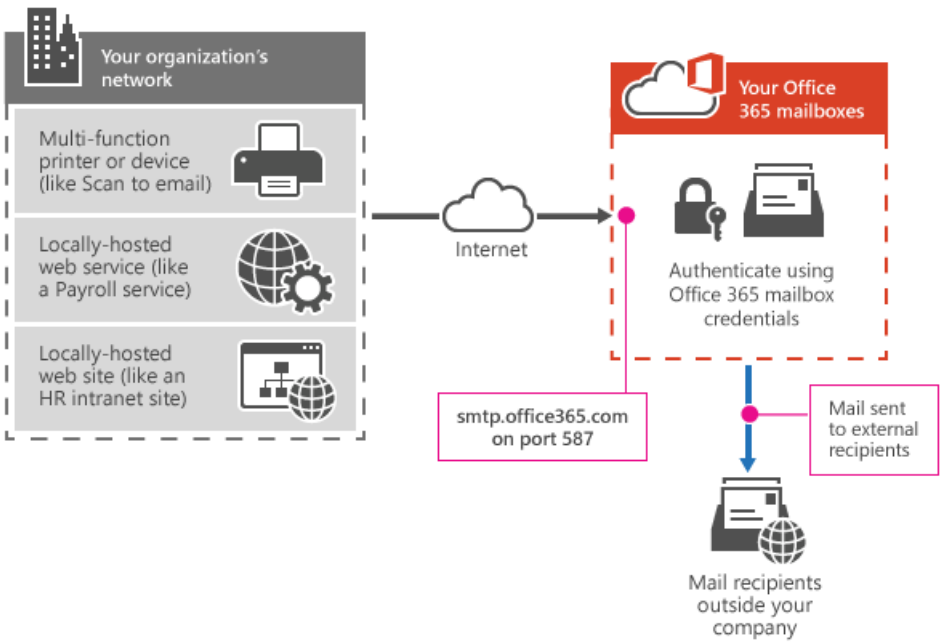
Determine what version of TLS your device supports by checking the device guide or with the vendor. If your device or application does not support TLS 1.2 or above:

- Use direct send (Option 2) or Microsoft 365 or Office 365 SMTP relay (Option 3) for sending mail instead (depending on your requirements).
- Use an on-premises Exchange server (or another SMTP email server) if your device is unable to meet the previous requirements for connecting to Microsoft 365 or Office 365. In fact, you might find it easier to manage multiple devices and applications that send email messages in an on-premises Exchange server instead of connecting them all to Microsoft 365 or Office 365 directly. The Exchange server would relay messages in the same way that a device would use Microsoft 365 or Office 365 to relay messages using Option 3 below. You can find out more about configuring your own email server to send emails to Microsoft 365 or Office 365 here: Set up connectors to route mail between Microsoft 365 or Office 365 and your own email servers.

> **NOTE**
>
> If your device recommends or defaults to port 465, it does not support SMTP AUTH client submission.

How SMTP AUTH client submission works

The following diagram gives you a conceptual overview of what you're environment will look like.



Features of SMTP AUTH client submission

- SMTP AUTH client submission allows you to send email to people in your organization as well as outside your company.
- This method bypasses most spam checks for email sent to people in your organization. This can help protect your company IP addresses from being blocked by a spam list.

- With this method, you can send email from any location or IP address, including your (on-premises) organization's network, or a third-party cloud hosting service, like Microsoft Azure.

Requirements for SMTP AUTH client submission

- **Authentication**: You must be able to configure a user name and password to send email on the device. Note that you cannot use Microsoft Security Defaults or multi-factor authentication (MFA), which disable basic authentication and are designed to protect your users from compromise. If your environment uses Microsoft Security Defaults or MFA, we recommend using Option 2 or 3 below.
- **Mailbox**: You must have a licensed Microsoft 365 or Office 365 mailbox to send email from.
- **Transport Layer Security (TLS)**: Your device must be able to use TLS version 1.2 and above.
- **Port**: Port 587 (recommended) or port 25 is required and must be unblocked on your network. Some network firewalls or ISPs block ports, especially port 25.
- **DNS**: You must use the DNS name smtp.office365.com. Do not use an IP address for the Microsoft 365 or Office 365 server, as IP Addresses are not supported.

> **NOTE**
>
> For information about TLS, see How Exchange Online uses TLS to secure email connections and for detailed technical information about how Exchange Online uses TLS with cipher suite ordering, see Enhancing mail flow security for Exchange Online.

Limitations of SMTP AUTH client submission

You can only send from one email address unless your device can store login credentials for multiple Microsoft 365 or Office 365 mailboxes. Microsoft 365 or Office 365 imposes a limit of 30 messages sent per minute, and a limit of 10,000 recipients per day.

Option 2: Send mail directly from your printer or application to Microsoft 365 or Office 365 (direct send)

Choose this option when:

- Your environment uses Microsoft Security Defaults or multi-factor authentication (MFA).
- SMTP client submission (Option 1) is not compatible with your business needs or with your device.
- You only need to send messages to recipients in your own organization who have mailboxes in Microsoft 365 or Office 365; you don't need to send email to people outside of your organization.

Other scenarios when direct send may be your best choice:

- You want your device or application to send from each user's email address and do not want each user's mailbox credentials configured to use SMTP client submission. Direct send allows each user in your organization to send email using their own address.

  Avoid using a single mailbox with Send As permissions for all your users. This method is not supported because of complexity and potential issues.

- You want to send bulk email or newsletters. Microsoft 365 or Office 365 does not allow you to do this via SMTP client submission. Direct send allows you to send a high volume of messages.

  Note that there is a risk of your email being marked as spam by Microsoft 365 or Office 365. You might want to enlist the help of a bulk email provider to assist you. For example, they'll help you adhere to best practices, and can help ensure that your domains and IP addresses are not blocked by others on the internet.

Settings for direct send

Enter the following settings on the device or in the application directly.

DEVICE OR APPLICATION SETTING	VALUE
Server/smart host	Your MX endpoint, for example, contoso-com.mail.protection.outlook.com
Port	Port 25
TLS/StartTLS	Enabled
Email address	Any email address for one of your Microsoft 365 or Office 365 accepted domains. This email address does not need to have a mailbox.

We recommend adding an SPF record to avoid having messages flagged as spam. If you are sending from a static IP address, add it to your SPF record in your domain registrar's DNS settings as follows:

DNS ENTRY	VALUE
SPF	`v=spf1 ip4:<Static IP Address> include:spf.protection.outlook.com ~all`

Step-by-step instructions for direct send

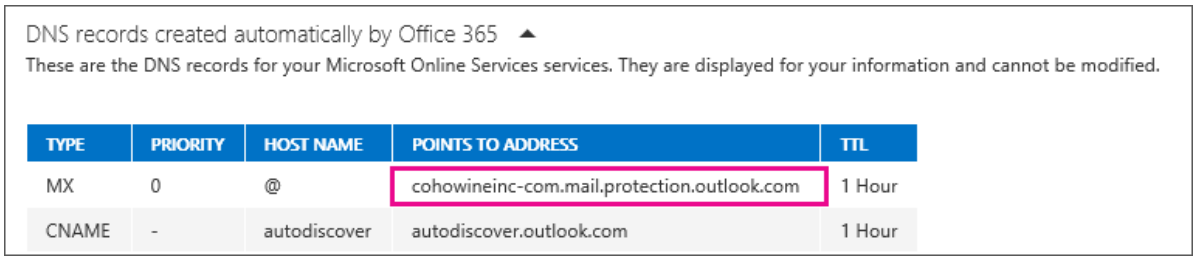
1. If your device or application can send from a static public IP address, obtain this IP address and make a note of it. You can share your static IP address with other devices and users, but don't share the IP address with anyone outside of your company. Your device or application can send from a dynamic or shared IP address but messages are more prone to antispam filtering.

2. Sign in to the Microsoft 365 admin center.

3. Go to **Settings** > **Domains**, select your domain (for example, contoso.com), and find the MX record.

   The MX record will have a **Points to address or value** value that looks similar to `contoso-com.mail.protection.outlook.com`.

   Make a note of the MX record **Points to address or value** value, which we refer to as your MX endpoint.



4. Go back to the device, and in the settings, under what would normally be called **Server** or **Smart Host**, enter the MX record **POINTS TO ADDRESS** value you recorded in step 3.

   > **NOTE**
   > Do NOT use an IP address for the Microsoft 365 or Office 365 server connection, as IP addresses are not supported.

5. Now that you are done configuring your device settings, go to your domain registrar's website to update

your DNS records. Edit your sender policy framework (SPF) record. In the entry, include the IP address that you noted in step 1. The finished string looks similar to this:

```
v=spf1 ip4:10.5.3.2 include:spf.protection.outlook.com ~all
```

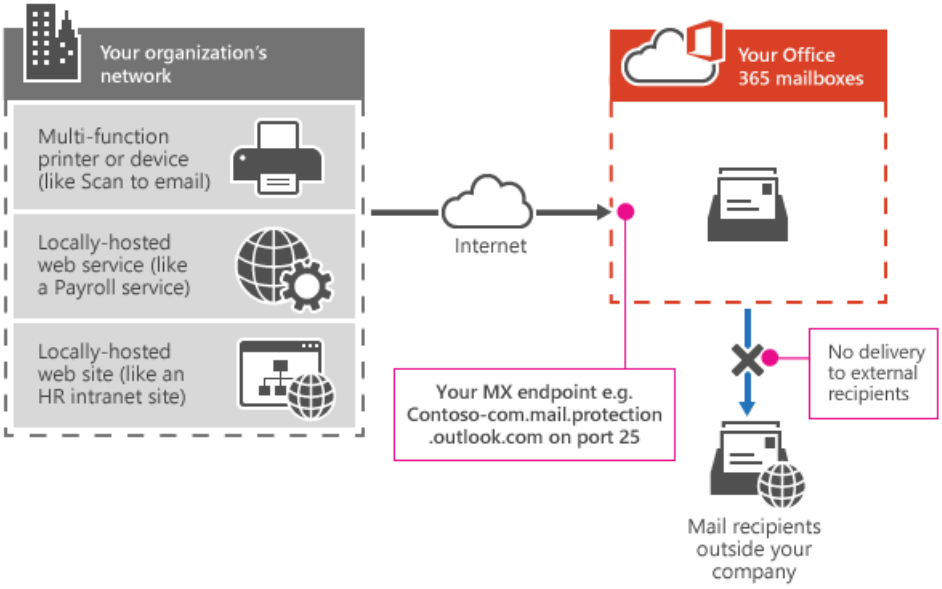
where 10.5.3.2 is your public IP address.

> **NOTE**
> Skipping this step might cause email to be sent to recipients' junk mail folders.

6. To test the configuration, send a test email from your device or application, and confirm that the recipient received it.

How direct send works

In the following diagram, the application or device in your organization's network uses direct send and your Microsoft 365 or Office 365 mail exchange (MX) endpoint to email recipients in your organization. It's easy to find your MX endpoint in Microsoft 365 or Office 365 if you need to look it up.



You can configure your device to send email direct to Microsoft 365 or Office 365. Use direct send to relay email to recipients with Microsoft 365 or Office 365 mailboxes in your organization. Direct send also works for external recipients with mailboxes in Microsoft 365 or Office 365. If your device uses direct send to try to relay an email for a recipient who doesn't have a Microsoft 365 or Office 365 mailbox, the email will be rejected.

> **NOTE**
> If your device or application has the ability to act as a email server to deliver messages to Microsoft 365 or Microsoft 365 or Office 365 as well as other email providers, there are no Microsoft 365 or Office 365 settings needed for this scenario. Consult your device or application instructions for more information.

Features of direct send

- Uses Microsoft 365 or Office 365 to send emails, but does not require a dedicated Microsoft 365 or Office 365 mailbox.
- Doesn't require your device or application to have a static IP address. However, this is recommended if possible.
- Doesn't work with a connector; never configure a device to use a connector with direct send, this can cause

problems.

- Doesn't require your device to support TLS.

Direct send has higher sending limits than SMTP client submission. Senders are not bound by the 30 messages per minute or 10,000 recipients per day limit.

Requirements for direct send

- **Port**: Port 25 is required and must be unblocked on your network.
- **Static IP address is recommended**: A static IP address is recommended so that an SPF record can be created for your domain. This helps avoid your messages being flagged as spam.
- Does not require a Microsoft 365 or Office 365 mailbox with a license.

Limitations of direct send

- Direct send cannot be used to deliver email to external recipients, for example, recipients with Yahoo or Gmail addresses.
- Your messages will be subject to antispam checks.
- Sent mail might be disrupted if your IP addresses are blocked by a spam list.
- Microsoft 365 and Office 365 use throttling policies to protect the performance of the service.

Option 3: Configure a connector to send mail using Microsoft 365 or Office 365 SMTP relay

This option is more difficult to implement than the others. Only choose this option when:

- Your environment uses Microsoft Security Defaults or multi-factor authentication (MFA).
- SMTP client submission (Option 1) is not compatible with your business needs or with your device
- You can't use direct send (Option 2) because you must send email to external recipients.

SMTP relay lets Microsoft 365 or Office 365 relay emails on your behalf by using a connector that's configured with your public IP address or a TLS certificate. Setting up a connector makes this a more complicated option.

Settings for Microsoft 365 or Office 365 SMTP relay

DEVICE OR APPLICATION SETTING	VALUE
Server/smart host	Your MX endpoint, e.g. *yourdomain*-com.mail.protection.outlook.com
Port	Port 25
TLS/StartTLS	Enabled
Email address	Any email address in one of your Microsoft 365 or Office 365 verified domains. This email address does not need a mailbox.

If you already have a connector that's configured to deliver messages from your on-premises organization to Microsoft 365 or Office 365 (for example, a hybrid environment), you probably don't need to create a dedicated connector for Microsoft 365 or Office 365 SMTP relay. If you need to create a connector, use the following settings to support this scenario:

CONNECTOR SETTING	VALUE
From	Your organization's email server
To	Microsoft 365 or Office 365
Domain restrictions: IP address/range	Your on-premises IP address or address range that the device or application will use to connect to Microsoft 365 or Office 365

We recommend adding an SPF record to avoid having messages flagged as spam. If you are sending from a static IP address, add it to your SPF record in your domain registrar's DNS settings as follows:

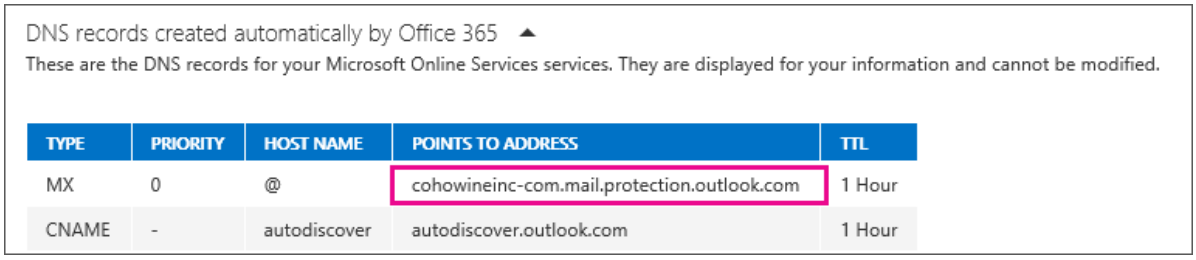
DNS ENTRY	VALUE
SPF	`v=spf1 ip4:<Static IP Address> include:spf.protection.outlook.com ~all`

Step-by-step configuration instructions for SMTP relay

1. Obtain the public (static) IP address that the device or application with send from. A dynamic IP address isn't supported or allowed. You can share your static IP address with other devices and users, but don't share the IP address with anyone outside of your company. Make a note of this IP address for later.
2. Sign in to the Microsoft 365 admin center.
3. Go to **Settings** > **Domains**, select your domain (for example, contoso.com), and find the MX record.

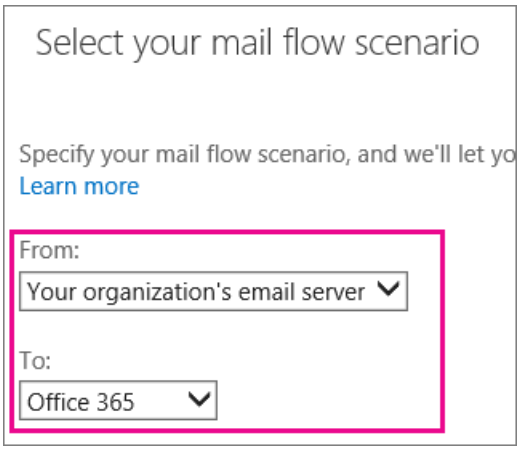
   The MX record will have a **Points to address or value** value that looks similar to `contoso-com.mail.protection.outlook.com`.

   Make a note of the MX record **Points to address or value** value, which we refer to as your MX endpoint.

4. Check that the domains that the application or device will send to have been verified. If the domain is not verified, emails could be lost, and you won't be able to track them with the Exchange Online message trace tool.
5. In Microsoft 365 or Office 365, select **Admin** and then **Exchange** to go to the Exchange admin center.
6. In the Exchange admin center, go to **Mail flow** > **Connectors**.
7. Check the list of connectors set up for your organization. If there is no connector listed from your organization's email server to Microsoft 365 or Office 365, create one:

   a. To start the wizard, click the plus symbol **+**. On the first screen, choose the options that are depicted in the following screenshot:



Click **Next**, and give the connector a name.

b. On the next screen, choose the option **By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization**, and add the IP address from step 1.

c. Leave all the other fields with their default values, and select **Save**.

8. Now that you are done with configuring your Microsoft 365 or Office 365 settings, go to your domain registrar's website to update your DNS records. Edit your SPF record. Include the IP address that you noted in step 1. The finished string should look similar to this `v=spf1 ip4:10.5.3.2 include:spf.protection.outlook.com ~all`, where 10.5.3.2 is your public IP address. Skipping this step can cause email to be sent to recipients' junk mail folders.

9. Now, go back to the device, and in the settings, find the entry for Server or Smart Host, and enter the MX record **POINTS TO ADDRESS** value that you recorded in step 3.

10. To test the configuration, send a test email from your device or application, and confirm that it was received by the recipient.

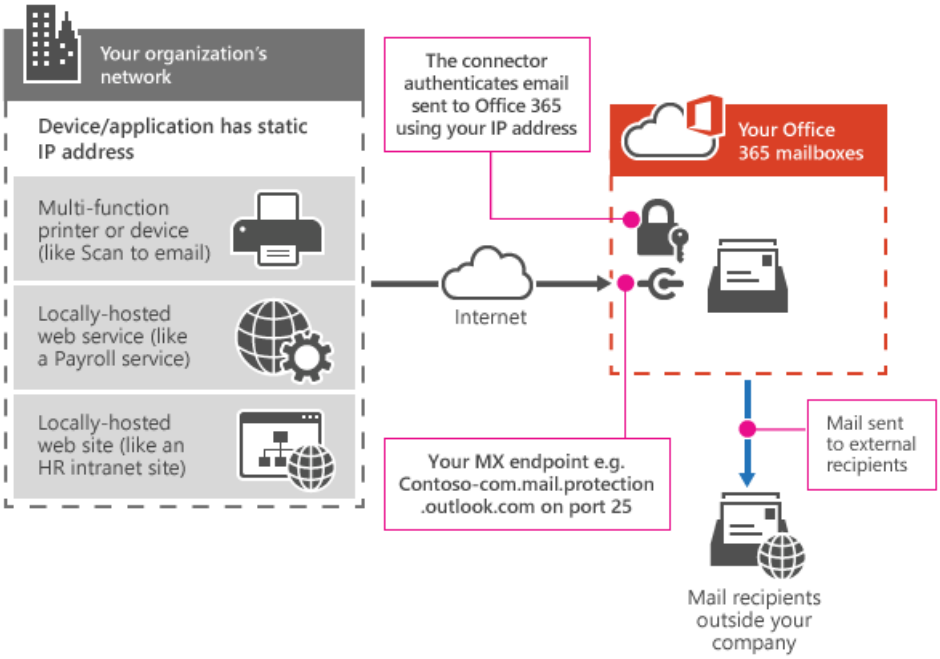
Configure a certificate-based connector to relay email through Microsoft 365 or Office 365

If your devices or applications are capable of using a certificate for mail flow, you can configure a certificate-based connector to relay email through Microsoft 365 or Office 365.

To do this, verify the subject name on the certificate used by the sending device or application. The common name (CN) or subject alternative name (SAN) in the certificate should contain a domain name that you have registered in Microsoft 365 or Office 365. Also, you must create a certificate-based connector in Microsoft 365 or Office 365 with this same domain name to accept and relay emails coming from these devices, applications, or any other on-premises server. For more information about this method, see important notice for email customers who have configured connectors.

How Microsoft 365 or Office 365 SMTP relay works

In the following diagram, the application or device in your organization's network uses a connector for SMTP relay to email recipients in your organization.



- The Microsoft 365 or Office 365 connector that you configure authenticates your device or application with Microsoft 365 or Office 365 using an IP address. Your device or application can send email using any address (including ones that can't receive mail), as long as the address uses one of your domains. The email address doesn't need to be associated with an actual mailbox. For example, if your domain is contoso.com, you could send from an address like do_not_reply@contoso.com.
- Microsoft 365 or Office 365 SMTP relay uses a connector to authenticate the mail sent from your device or application. This allows Microsoft 365 or Office 365 to relay those messages to your own mailboxes as well as external recipients. Microsoft 365 or Office 365 SMTP relay is very similar to direct send except that it can send mail to external recipients.
- Due to the added complexity of configuring a connector, direct send is recommended over Microsoft 365 or Office 365 SMTP relay, unless you must send email to external recipients. To send email using Microsoft 365 or Office 365 SMTP relay, your device or application server must have a static IP address or address range. You can't use SMTP relay to send email directly to Microsoft 365 or Office 365 from a third-party hosted service, such as Microsoft Azure. For more information, see Troubleshoot outbound SMTP connectivity issues in Azure.

Features of Microsoft 365 or Office 365 SMTP relay

- Microsoft 365 or Office 365 SMTP relay does not require the use of a licensed Microsoft 365 or Office 365 mailbox to send emails.
- Microsoft 365 or Office 365 SMTP relay has higher sending limits than SMTP client submission; senders are not bound by the 30 messages per minute or 10,000 recipients per day limits.

Requirements for Microsoft 365 or Office 365 SMTP relay

- **Static IP address or address range**: Most devices or applications are unable to use a certificate for authentication. To authenticate your device or application, use one or more static IP addresses that are not shared with another organization.
- **Connector**: You must set up a connector in Exchange Online for email sent from your device or application.
- **Port**: Port 25 is required and must not be blocked on your network or by your ISP.
- **Licensing**: SMTP relay doesn't use a specific Microsoft 365 or Office 365 mailbox to send email. This means that users must have their own licenses if they send email from devices or applications that are configured for SMTP relay. If you have senders who use a device or LOB application and those senders do

not have Microsoft 365 or Office 365 mailbox licenses, obtain and assign an Exchange Online Protection license to each unlicensed sender. This is the least expensive license that allows you to send email via Microsoft 365 or Office 365.

Limitations of Microsoft 365 or Office 365 SMTP relay

- Sent mail can be disrupted if your IP addresses are blocked by a spam list.
- Reasonable limits are imposed for sending. For more information, see High-risk delivery pool for outbound messages.
- Requires static unshared IP addresses (unless a certificate is used).

Compare the options

Here's a comparison of each configuration option and the features they support.

	SMTP CLIENT SUBMISSION	DIRECT SEND	SMTP RELAY
Features			
Send to recipients in your domain(s)	Yes	Yes	Yes
Relay to internet via Microsoft 365 or Office 365	Yes	No. Direct delivery only.	Yes
Bypasses antispam	Yes, if the mail is destined for one of your Microsoft 365 or Office 365 mailboxes.	No. Suspicious emails might be filtered. We recommend a custom Sender Policy Framework (SPF) record.	No. Suspicious emails might be filtered. We recommend a custom SPF record.
Supports mail sent from applications hosted by a third party	Yes	Yes. We recommend updating your SPF record to allow the third party to send as your domain.	No
Saves to Sent Items folder	Yes	No	No
Requirements			
Open network port	Port 587 or port 25	Port 25	Port 25
Device or application server must support TLS	Required	Optional	Optional
Requires authentication	Microsoft 365 or Office 365 username and password required	None	One or more static IP addresses. Your printer or the server running your LOB app must have a static IP address to use for authentication with Microsoft 365 or Office 365.
Limitations			

	SMTP CLIENT SUBMISSION	DIRECT SEND	SMTP RELAY
Throttling limits	10,000 recipients per day. 30 messages per minute.	Standard throttling is in place to protect Microsoft 365 or Office 365.	Reasonable limits are imposed. The service can't be used to send spam or bulk mail. For more information about reasonable limits, see High-risk delivery pool for outbound messages.

Use your own email server to send email from multifunction devices and applications

If you happen to have an on-premises email server, you should seriously consider using that server for SMTP relay instead of Microsoft 365 or Office 365. A local email server that you have physical access to is much easier to configure for SMTP relay by devices and applications on your local network. The details about how to do this depend on your on-premises email server. For Exchange Server, see the following topics:

- Allow anonymous relay on Exchange servers
- Receive messages from a server, service, or device that doesn't use Exchange

Related Topics

Fix issues with printers, scanners, and LOB applications that send email using Microsoft 365 or Office 365

Set up connectors to route mail between Microsoft 365 or Office 365 and your own email servers

Fix issues with printers, scanners, and LOB applications that send email using Microsoft 365 or Office 365

8/10/2020 • 9 minutes to read • Edit Online

Email clients provide actionable error messages when something goes wrong. Sending email from devices and applications is less easy to fix, and you might not get clear information to help you. This article can help you troubleshoot, and it uses printer configurations as examples.

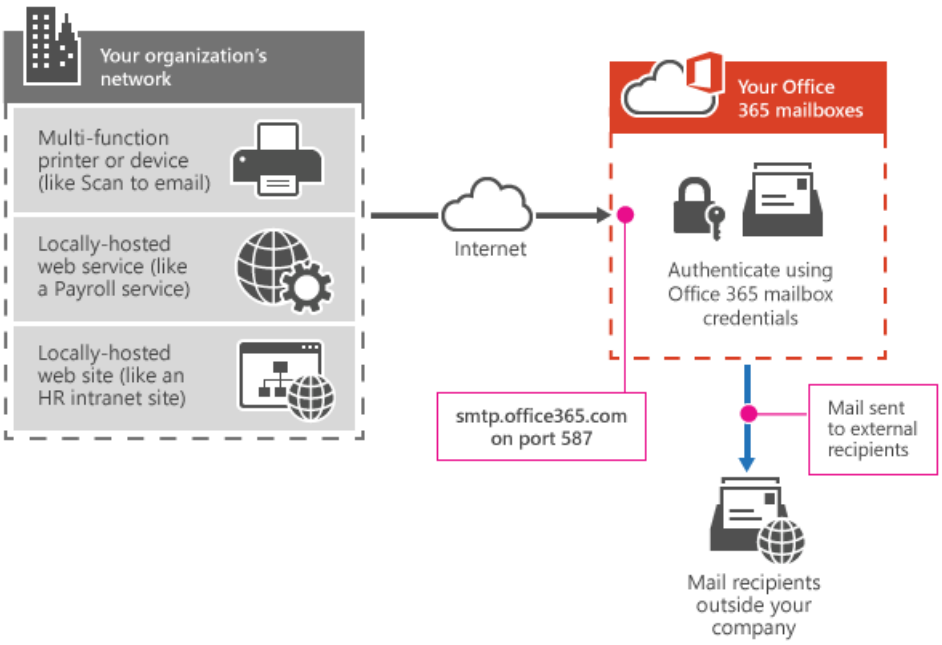
As a first step to fixing any problems, check your configuration. See How to set up a multifunction device or application to send email using Microsoft 365 or Office 365 for detailed information about the configuration options.

My printer is already configured for email, but I don't know which configuration option it uses

Below are the three configuration options to help you identify which one is in use:

1. SMTP client submission (recommended)

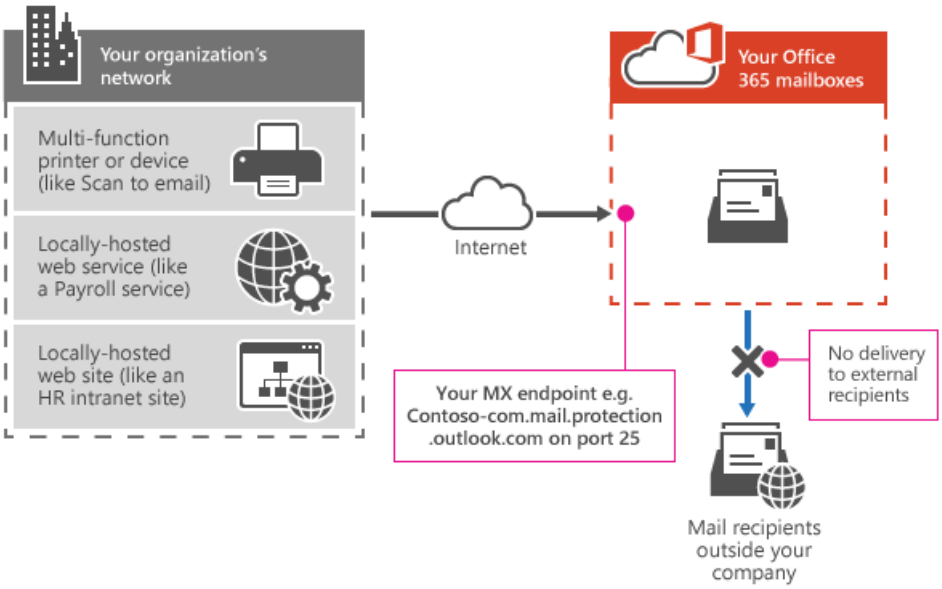
- Your printer is connected to the server "smtp.office365.com."
- You entered an email address and password for the printer mailbox.
- The printer can send email to people inside and outside your organization.



2. Direct send

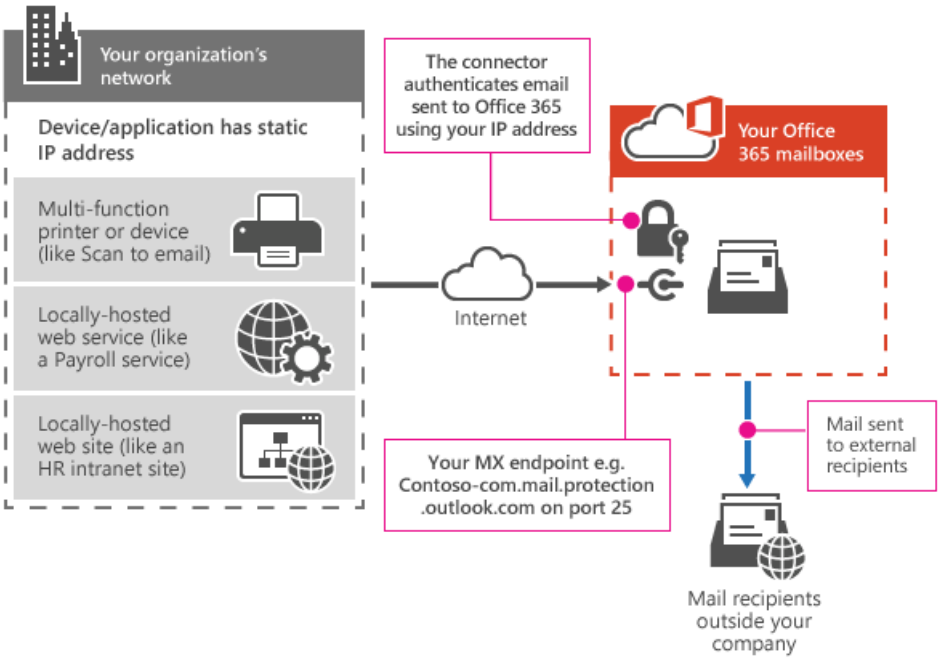
- Your printer is connected to a Microsoft 365 or Office 365 server whose name ends with "mail.protection.outlook.com."
- There is no connector set up in Microsoft 365 or Office 365 for emails sent from your organization's network.

- The printer can send email only to people in your organization; email can't be sent to recipients outside your organization.



3. Microsoft 365 or Office 365 SMTP relay

- Your printer is connected to a Microsoft 365 or Office 365 server whose name ends with "mail.protection.outlook.com."
- There is a connector set up in Microsoft 365 or Office 365 for emails sent from your organization's network to Microsoft 365 or Office 365.
- The printer can send email to people inside and outside your organization.



Fix issues with SMTP client submission

I set up my printer for SMTP client submission, but it still can't send emails

1. Check the settings entered directly into the printer:

PRINTER SETTING	VALUE
Server/smart host	smtp.office365.com
Port	Port 587 (recommended) or port 25
TLS/ StartTLS	Enabled
Username/email address and password	Login credentials of Microsoft 365 or Office 365 mailbox the printer uses

2. If your printer didn't require a password for the email address you entered, your printer is trying to send emails without logging on to Microsoft 365 or Office 365. SMTP client submission requires your printer to log on to Microsoft 365 or Office 365. Direct send and Microsoft 365 or Office 365 SMTP relay do not require a logon; consider one of these options instead.

3. Your printer or application must send email from the same address that you entered logon credentials for during email setup. If the printer or application tries to send email from a different account, this results in an error similar to:

   > 5.7.60 SMTP; Client does not have permissions to send as this sender.

   For example, if you entered login credentials for sales@contoso.com in your application settings, but the application tries to send emails from salesperson1@contoso.com, this is not supported. For this scenario, use Microsoft 365 or Office 365 SMTP relay instead.

4. Test the user name and password by logging on to Outlook on the web, and try to send a test email to make sure the account is not blocked. If the user is blocked, you can find help in the article, Remove blocked users from the Restricted Users portal.

5. Next, test that you can connect to Microsoft 365 or Office 365 from your network by doing the following:

   a. Follow the instructions to install the Telnet Client tool on a computer on the same network as the device or application.

   b. Run the tool from the command line by typing **telnet**.

   c. Type **open smtp.office365.com 587** (or substitute **25** for **587** if you are using that port setting instead).

   d. If you connected successfully to an Office 365 server, expect to receive a response line similar to this:

      > 220 BY1PR10CA0041.outlook.office365.com Microsoft ESMTP MAIL Service ready at Mon, 1 Jun 2015 12:00:00 +0000

   e. If you can't connect to Microsoft 365 or Office 365, your network firewall or Internet Service Provider (ISP) might have blocked port 587 or 25. Correct this so you can send email from your printer.

6. If none of these issues applies to your device, it might not meet requirements for Transport Layer Security (TLS) encryption. Your device must support TLS version 1.2 or above. Update the firmware on the device to solve this, or try one of the other configuration options where TLS is optional.

   For more information about TLS, see How Exchange Online uses TLS to secure email connections and for detailed technical information about how Exchange Online uses TLS with cipher suite ordering, see Enhancing mail flow security for Exchange Online.

I receive an authentication error when my device tries to send email

This can be caused by a number of issues:

1. Make sure that you entered the correct username and password.
2. Try logging into OWA with the printer's username and password. Send an email to make sure that the mailbox is active and has not been blocked for sending spam.
3. Check that your device or application supports TLS version 1.2 or above. The best way to check is by upgrading the firmware on the device or updating the application you're sending email from to the latest version. Contact your device manufacturer to confirm that it supports TLS version 1.2 or above.

Error: 5.7.60 SMTP; Client does not have permissions to send as this sender

This error indicates that the device is trying to send an email from an address that doesn't match the logon credentials. An example would be if your entered login credentials for sales@contoso.com in your application settings but the application tries to send emails from salesperson1@contoso.com. If your application or printer behaves this way, use Microsoft 365 or Office 365 SMTP relay because SMTP client submission does not support this scenario.

Error: Client was not authenticated to send anonymous mail during MAIL FROM

This error indicates that your printer connects to the SMTP client submission endpoint (smtp.office365.com). However, your printer must also logon to a mailbox to send a message. This error occurs when you have not entered mailbox logon credentials in the printer's settings. If there is no option to enter credentials, this printer does not support SMTP client submission; use either direct send or Microsoft 365 or Office 365 SMTP relay instead. See How to set up a multifunction device or application to send email using Microsoft 365 or Office 365.

Error: 550 5.1.8 Bad outbound sender

This error indicates that the device is trying to send an email from a Microsoft 365 or Office 365 mailbox that is on a spam block list. For help, see Remove blocked users from the Restricted Users portal.

Fix issues with direct send

I set up my printer for direct send and it's not sending email - or - My device was sending email using direct send, but it stopped working

This can be caused by a number of issues.

1. A common reason for issues with direct send is a blocked IP address. If antispam tools detect outbound spam from your organization, your IP address can be blocked by a spam block list. Check whether your IP address is on a block list by using a third-party service, such as MXToolbox or WhatIsMyIPAddress. Follow up with the organization that added your IP address to their block list. Microsoft 365 and Office 365 use block lists to protect our service. For help, see Remove blocked users from the Restricted Users portal.
2. To rule out a problem with your device, send a test email to check your connection to Microsoft 365 or Office 365. To send a test email, follow these steps in the article, Use Telnet to Test SMTP Communication. If you can't connect to Microsoft 365 or Office 365, your network or ISP might have blocked communication using port 25. If you can't reverse this, use SMTP client submission instead.

Error: Client was not authenticated to send anonymous mail during MAIL FROM

This indicates that you are connecting to the SMTP client submission endpoint (smtp.office365.com), which can't be used for direct send. For direct send, use the MX endpoint for your Microsoft 365 or Office 365 organization, which ends with "mail.protection.outlook.com." You can find your MX endpoint by following the steps in Option 2: Send mail directly from your printer or application to Microsoft 365 or Office 365 (direct send).

My emails are not sent to recipients who are not in my organization

This is by design. Direct send allows email to be sent only to recipients in your organization that are hosted in

Microsoft 365 or Office 365. If you need to send to external recipients, use SMTP client submission or Microsoft 365 or Office 365 SMTP relay.

The MX endpoint is too long for the printer setting box. Can I use an IP address instead?

It's not possible to use an IP address in place of an MX endpoint. This could result in your not being able to send messages in the future. If the MX endpoint is too long, consider using SMTP client submission, which has a shorter endpoint (smtp.office365.com).

Emails from my device are marked as junk by Microsoft 365 or Office 365

For direct send, we recommend using a device that sends from a static IP address. This allows you to set up a Sender Policy Framework (SPF) record to help prevent emails being marked as spam. Check that your SPF record is set up with your static IP address. A network or ISP change could change your static IP address. Update your SPF record to reflect this change. If you aren't sending from your own static IP address, consider SMTP client submission instead.

Fix issues with Microsoft 365 or Office 365 SMTP relay

I set up my printer for Microsoft 365 or Office 365 SMTP relay but it's not sending email -or- My device was sending email using SMTP relay, but it stopped working

This can be caused by a number of issues.

1. A common reason for issues with Microsoft 365 or Office 365 SMTP relay is a blocked IP address. If antispam tools detect outbound spam from your organization, your IP address can be blocked by a spam block list. Check whether your IP address is on a block list by using a third-party service, such as MXToolbox or WhatIsMyIPAddress. Follow up with the organization that added your IP address to their block list. Microsoft 365 and Office 365 use block lists to protect our service. For help, see Remove blocked users from the Restricted Users portal.

2. To rule out a problem with your device, send a test email to check your connection to Microsoft 365 or Office 365. To send a test email, follow these steps in the article, Use Telnet to Test SMTP Communication. If you can't connect to Microsoft 365 or Office 365, your network or ISP might have blocked communication using port 25. If you can't reverse this, use SMTP client submission instead.

Emails are no longer being sent to external recipients

Network or ISP changes might change your static IP address. This results in your connector not identifying and relaying your messages to external recipients. Update your connector and your SPF record with the new IP address. Follow the steps in Option 3: Configure a connector to send mail using Microsoft 365 or Office 365 SMTP relay to edit your existing connector settings.

Emails from my device are marked as junk by Microsoft 365 or Office 365

Microsoft 365 or Office 365 SMTP relay requires your device to send email from a static IP address. Check that your SPF record is set up with your static IP address. A network or ISP change could change your static IP address. Update your SPF record to reflect this change. If you aren't sending from your own static IP address, consider SMTP client submission instead.