Office 365 and scan to email

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

Exchange Online

Applies to: Exchange Online

Topic Last Modified: 2016-05-04

You can use SMTP submission, direct send, or SMTP relay to allow a multifunction device, printer, or application to send email using Office 365 and Exchange Online.

This topic explains how to send email from devices and business applications when all of your mailboxes are in 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.

Use this article to choose the option that meets your requirements, then configure your device or application to send email:

Image not found or type unknown

Note:

This document helps you set up email for multifunction printer devices and business applications only. If you want to set up a mobile device, such as a smart phone, or other email clients to send and receive from an Office 365 mailbox, see Settings for POP and IMAP access for Office 365 for business or Microsoft Exchange accounts.

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

If you have mailboxes in Office 365 and an email server that you manage (also called an on-premises email server), always configure your devices and applications to use your local network and route email through your own email server. For details about setting up your Exchange server to receive email from systems that are not running Exchange (such as a multifunction printer), see Create a Receive connector to receive email from a system not running Exchange.

How can devices and applications send email to recipients?

If all of your mailboxes are in Office 365, here are the options for sending email from an application or device:

- Option 1 (recommended): Authenticate your device or application directly with an Office 365 mailbox, and send mail using SMTP client submission
  Configure your device or application to authenticate with an Office 365 mailbox, and use Simple Mail Transfer Protocol (SMTP) client submission. In this scenario, the device or application uses an email account to send email to recipients just like an email client.
- Option 2: Send mail direct from your printer or application to Office 365 (direct send)
  Configure your device or application to send mail directly to recipients in your organization. When you set up your device or application, configure it to point to your mailboxes in Office 365 using your mail exchange (MX) endpoint record.
- Option 3: Configure a connector to send mail using Office 365 SMTP relay
  Configure a connector so your device or application can send email to Office 365. Office 365 can then relay email to your organization mailboxes and to external recipients.

Note:

If you have already configured email for printers or devices and want to troubleshoot an issue, see the article Troubleshoot email sent from devices and business applications.

Descriptions of each method and configuration instructions follow.

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

If your device or application can authenticate and send email using an Office 365 mailbox account, this is the recommended method. The device or application sends mail using SMTP client submission. In the following diagram, the application or device in your organization's network uses SMTP client submission and authenticates with a mailbox in Office 365.

Using SMTP client submission

To send mail using SMTP client submission, each device or application must be able to authenticate with Office 365. Each device or application can have its own sender address, or all devices can use one address, such as printer@contoso.com. If you want to send email from a third-party hosted application or service, you must use SMTP client submission. In this scenario, the device or application connects directly to Office 365 using the SMTP client submission endpoint smtp.office365.com.

Features of SMTP client submission

- SMTP 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 client submission

- Authentication: You must be able to configure a user name and password to send email on the device.
- Mailbox: You must have a licensed Office 365 mailbox to send email from.
- Transport Layer Security (TLS): Your device must be able to use TLS version 1.0 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.

Note:
For information about TLS, see How Exchange Online uses TLS to secure email connections in Office 365 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 client submission

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

Set up SMTP client submission by following How to configure SMTP client submission.

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

If SMTP client submission is not compatible with your business needs or with your device, consider using direct send. Direct send makes it easy to send messages to recipients in your own organization with mailboxes in Office 365.

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

Using direct send

You can configure your device to send email direct to Office 365. However, in this case, Office 365 does not relay messages for external recipients and will only deliver to your hosted mailboxes. If your device sends an email to Office 365 that is for a recipient outside your organization, the email will be rejected.

Note:
If your device or application has the ability to act as a mail server and deliver to Office 365 as well as other mail providers, consult your device or application instructions; there are no Office 365 settings needed for this scenario.

There are several scenarios where direct send can be the best choice:

- If the device or application is only sending email to your own Office 365 users and SMTP client submission is not an option, this is the simplest method as there is no Office 365 configuration needed.
- 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. When you use direct send, avoid using a single mailbox with Send As permissions for all your users. This method is not supported because of complexity and potential issues.
- Your device or application does not meet the requirements of SMTP client submission, such as TLS support.
- Office 365 does not allow you to send bulk email or newsletters via SMTP client submission. Direct send allows you to send a higher volume of messages. However, there is a risk of your email being marked as spam by Office 365. You might want to enlist the help of a bulk email provider to assist you. There are best practices for bulk email, and bulk email providers can help ensure that your domains and IP addresses are not blocked

by others on the Internet.

Features of direct send

Direct send:

- Uses Office 365 to send emails, but does not require a dedicated 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.

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.
- Office 365 uses throttling policies to protect the performance of the service.

Set up direct send by following How to configure direct send.

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

Office 365 SMTP relay uses a connector to authenticate the mail sent from your device or application. This allows Office 365 to relay those messages to your own mailboxes as well as external recipients. 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 Office 365 SMTP relay, unless you must send email to external recipients. To send email using 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 Office 365 from a third-party hosted service, such as Microsoft Azure.

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.

Using Office 365 SMTP relay

The Office 365 connector that you configure authenticates your device or application with 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 Office 365 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.

Features of Office 365 SMTP relay

- Office 365 SMTP relay does not require the use of a licensed Office 365 mailbox to send emails.
- 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 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 Office 365 mailbox to send email. This is why it’s important that only licensed users send email from devices or applications configured for SMTP relay. If you have senders using devices or LOB applications who don’t have an Office 365 mailbox license, 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 Office 365.

Limitations of 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 Higher Risk Delivery Pool for Outbound Messages.
- Requires static unshared IP addresses (unless a certificate is used).

Set up SMTP relay by following How to configure Office 365 SMTP relay

Summary of options for sending email from a device or application

The following table will help you decide which one of these options will meet your needs. Detailed information and setup steps follow each method.

	SMTP client submission	Direct send	SMTP relay
Features			
Send to recipients in your domain(s)	Yes	Yes	Yes
Relay to Internet via Office 365	Yes	No. Direct delivery only.	Yes
Bypasses antispam	Yes, if the mail is destined for an Office 365 mailbox.	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	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	Office 365 user name 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 Office 365.
Limitations			
Throttling limits	10,000 recipients per day. 30 messages per minute.	Standard throttling is in place to protect 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 Higher Risk Delivery Pool for Outbound Messages.

How to configure SMTP client submission

Devices and applications vary in functionality and terminology use. However, these configuration settings will help you set up SMTP client submission.

Enter the settings directly on the device or in the application as the device guide or manual instructs. As long as your scenario meets the requirements for SMTP client submission, these 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
TLS/ StartTLS	Enabled
Username/email address and password	Login credentials of 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 1.0 or above:

- Use direct send or Office 365 SMTP relay for sending mail instead (depending on your requirements).
- If it is essential to use SMTP client submission and your printer only supports SSL 3.0, you can set up an alternative configuration called Indirect SMTP client submission. This uses a local SMTP relay server to connect to Office 365. This is a much more complex setup.

  Instructions can be found here: How to configure Internet Information Server (IIS) for relay with Office 365.

Note:
If your device recommends or defaults to port 465, it does not support SMTP client submission.

How to configure direct send

Devices and applications vary in functionality and terminology use. To configure 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 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

Full configuration 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. Log on to the Office 365 Portal.
3. Make sure your domain, such as contoso.com, is selected. Click Manage DNS, and find the MX record. The MX record will have a POINTS TO ADDRESS value that looks similar to cohowineinc-com.mail.protection.outlook.com, as depicted in the following screenshot. Make a note of the MX record POINTS TO ADDRESS 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. 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.
6. 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.

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

How to configure Office 365 SMTP relay

This method allows Office 365 to relay emails on your behalf by authenticating using your public IP address (or a certificate). This requires a connector to be set up for your Office 365 account. If your device or application supports or requires user name and password authentication, consider the SMTP client submission method instead. Quick configuration details follow. If you prefer full instructions, check the next section.

Device or application setting	Value
Server/smart host	Your MX endpoint, e.g. yourcontosodomain-com.mail.protection.outlook.com
Port	Port 25
TLS/StartTLS	Enabled
Email address	Any email address for one of your Office 365 verified domains. This email address does not need a mailbox.

If you have set up Exchange Hybrid or have a connector configured for mail flow from your email server to Office 365, it is likely that no additional setup will be required for this scenario. Otherwise, create a mail flow connector to support this scenario:

Connector setting	Value
From	Your organization's email server
To	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 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

Full configuration instructions

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. Log on to the Office 365 Portal.
3. Select Domains. Make sure your domain, such as contoso.com, is selected. Click Manage DNS and find the MX record. The MX record will have a POINTS TO ADDRESS value that looks similar to cohowineinc-com.mail.protection.outlook.com as depicted in the following screenshot. Make a note of the MX record POINTS TO ADDRESS value. You'll need this later.

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 Office 365, click Admin, and then click Exchange to go to the Exchange admin center.

Note:
If you have Microsoft Office 365 Small Business Premium, see the instructions here.

6. In the Exchange admin center, click mail flow, and click 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 Office 365, create one.
   1. 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.
   2. 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.
   3. Leave all the other fields with their default values, and select Save.
8. Now that you are done with configuring your 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.

From <https://technet.microsoft.com/en-us/library/dn554323(v=exchg.150).aspx>

Revision #1
Created 23 December 2023 04:36:41 by ColtM
Updated 13 June 2024 01:28:01 by ColtM