How to create an Email Send Account

An Email Send Account is the mailbox Print Director sends its emails from. Every email Print Director sends goes through an Email Send Account, including:

- **Manual sends:** right-click one or more users in Resource Manager and choose **Send Email**, usually to send users their PIN.
- **Report exports and flat file exports** sent by scheduled tasks.
- **Rule violation** notifications.
- **User self-service in the PDAgent client:** email verification when a user registers, PIN resets and forgotten passwords.
- **New user welcome** emails to users created by an LDAP or Entra ID sync, usually with their automatically allocated PIN.
- **Email to print** replies (for example a guest PIN, confirmation that a job was received, that an attachment could not be printed, or that a job was delayed or could not be routed to a printer).
- **Scan workflows** that send the scanned document by email.

Create the Email Send Account

1. Open Resource Manager.
2. In the tree, click **Email Management** > **Email Send Accounts**.
3. Click **Add**. The **Email send account** window opens.
4. In **Send account name**, enter a descriptive name.
5. Choose the **Sending service type**, then fill in the settings for that type as described below:
   - **Basic SMTP AUTH:** sends through an SMTP server, with or without a user name and password.
   - **MS Graph application authentication:** sends through Microsoft 365 using your own Entra ID app registration. It runs as an application, not as a user, so it can send as any mailbox in your tenant.
   - **MS Graph user delegated authentication:** sends through Microsoft 365 as the user who signs in when the token is created. This is the simplest way to use Microsoft 365, because you do not need your own app registration.
6. Click **Test Settings...** to send a test email (see Test the account below).
7. Click **OK**.

Basic SMTP AUTH

You need the SMTP server's address. If the server needs a login or an encrypted connection, you also need the port number, user name and password; your email administrator can give you these.

- In **SMTP server address**, enter the server's host name or IP address.
- In **'From' address**, enter the email address the emails are sent from. Depending on how the SMTP server is set up, it may only accept certain 'From' addresses.
- In **SMTP port number**, enter the port (25 is filled in). Without a login or encryption this is usually 25; with encryption it is usually 587.
- If the server needs an encrypted connection (SSL or TLS), tick **Server requires an encrypted connection (SSL)**.
- If the server needs a login, tick **SMTP server requires authentication** and enter the **User name** and **Password**.

Example settings for Microsoft 365 and Gmail:

Setting	Microsoft 365	Gmail
SMTP server address	smtp.office365.com	smtp.gmail.com
'From' address	the same address as the User name	the same address as the User name
SMTP port number	587	587
Server requires an encrypted connection (SSL)	Ticked	Ticked
SMTP server requires authentication	Ticked	Ticked

For Microsoft 365, SMTP AUTH must be enabled for the mailbox. See Enable or disable SMTP AUTH in Exchange Online. For Microsoft 365 we recommend one of the MS Graph types instead.

MS Graph application authentication

This type needs an app registration in your Entra ID tenant, with a client secret that is saved in Print Director. See *How to create a custom private client app in Azure*.

- In **Client app**, select the app registration you created.
- In **Send as user**, enter the user principal name (or Entra ID user ID) of the mailbox the emails are sent from.
- Tick **Save to sent items** if you want a copy of each email kept in that mailbox's Sent Items.

MS Graph user delegated authentication

A delegated token sends as one user, who grants Print Director permission to send email when the token is created. One token can be used by several Email Send Accounts.

- In **Token**, leave **<create new>** selected to create a new token, or select a token that already exists. (The **...** button next to it lists the tokens, with the user each one sends as and its estimated expiry, and lets you add, edit or delete them.)
- Tick **Save to sent items** if you want a copy of each email kept in the Sent Items.
- Click **Test Settings...**. With **<create new>** selected, the **Delegated authentication token** window opens first:
  - In **Display name**, enter a name for the token.
  - Leave **Use Entra ID registered app** on **PD Entra ID**, unless you use your own app registration (see Using your own app registration below).
  - Click **New token** and sign in with Microsoft (see Signing in below). **Token issued date** and **Estimated expiry (default 90 days)** are filled in.
  - Click **OK**.
- **Send as user** is filled in with the user who signed in. If you change it to another mailbox, the token's user must have permission to send as that mailbox; Resource Manager warns you that this may cause an access denied error.

Signing in

The sign-in is done by the PDServer, using the Microsoft device code sign-in. Resource Manager shows a **Sign in to Microsoft** window with a QR code and a code:

- Scan the QR code with your phone, or open the address shown in any web browser. **Open sign-in page here** opens it on this computer.
- On the Microsoft page **Enter code to allow access**, enter the code (**Copy code** copies it) and click **Next**.
- Sign in as the user that emails are to be sent as. The user needs the rights to grant the permissions that are requested; Microsoft then asks you to accept them.

Resource Manager carries on by itself when the sign-in is complete.

If Resource Manager cannot reach a PDServer, or your organisation blocks device code sign-in (for example with a Conditional Access policy), Resource Manager asks whether to sign in with Microsoft directly on this computer instead. Click **Yes**, and a Microsoft sign-in window opens on this computer.

Using your own app registration

If you choose **Specify custom application** in **Use Entra ID registered app**, enter its **Application (client) ID** and **Tenant ID**. Device code sign-in only works if public client flows are allowed on that app registration: in the Entra admin center, go to **App registrations**, select the app, click **Authentication** and set **Allow public client flows** to **Yes**. Otherwise Resource Manager falls back to signing in on this computer.

Test the account

1. Click **Test Settings...**. The **Send test email** window opens, with a test message in **Subject** and **Body** from the **Test email send account** template.
2. Check the address in **Send to**, then click **Send email**.
3. Resource Manager shows **Send successful.** or the reason the send failed. Check the mailbox to make sure the email arrived.

Related articles

- *How to create a custom private client app in Azure*

Print Director version at time of publish: 2.5.15.3. Publish date: 03/11/2026.