How to create an Email Send Account

Email Send Accounts are used when Print Director sends emails. An email will be sent for any of the following reasons:

- Manual User Send: Right-click the user(s) in Resource Manager and choose Send Email. This is normally used for sending PIN numbers to users.
- Report Export & Flat File Export: Scheduled tasks that send Report Exports or Flat File Exports.
- Rule Violation: Rule Violation notifications.
- Email Verification:
    - User registration via PDAgent client application.
    - User resetting their PIN via PDAgent client.
    - User forgot password process via PDAgent client.
- New user welcome: If a new user is created during an LDAP or Azure sync, they can be automatically sent an email. This is normally used to send their auto-allocated PIN.
- Email to Print: Responding to all Email to Print events (e.g. Guest PIN number, successful receipt or invalid attachments).

Create the Email Send Account

- Open Resource Manager.
- Navigate to **Email Management, Email Send Accounts**.
- In the right hand pane, click **Add**.
- Enter a descriptive name in the **Send account name** textbox.
- Choose the Sending service type. See below for configuration of each Sending service type.
    - MS Graph application authentication: This method uses MS Graph API to send emails. Application authentication requires a Registered Application to be created in your Azure AD with Client Secret that can be saved here. It does not execute as a 'user' in MS Graph, it executes as an 'application'.
    - MS Graph user delegated authentication: This method uses MS Graph API to send emails. It executes as the 'user' that authenticates when creating the token. The token is stored by PD and is refreshed each time it is used.

Send Service Type: Basic SMTP AUTH

This is the original way to send emails using an SMTP server. It supports non-authentication sending as well as authenticated.

Obtain the SMTP server settings required

If you have an open relay SMTP server on your network, then all you need is the SMTP server address. This can be the host name or an IP address.

If the SMTP server requires authentication and/or SSL/TLS, then these credentials along with the port number will be required.

Example: Office 365 SMTP AUTH settings

Note: Ensure that the mailbox used has SMTP Auth enabled. See Enable or disable SMTP AUTH | Microsoft Docs for further information.

- SMTP server address: smtp.office365.com

- 'From' address: must match the User ID.
- SMTP port number: 587
- Server requires SSL: Ticked.
- SMTP server requires authentication: Ticked.
- Enter the username and password for the Office 365 account that will be used for sending emails.

Example: Gmail SMTP settings

- SMTP server address: smtp.gmail.com
- 'From' address: must match the User ID.
- SMTP port number: 587
- Server requires SSL: Ticked.
- SMTP server requires authentication: Ticked.
- Enter the username and password for the Google account that will be used for sending emails.

Enter SMTP AUTH details

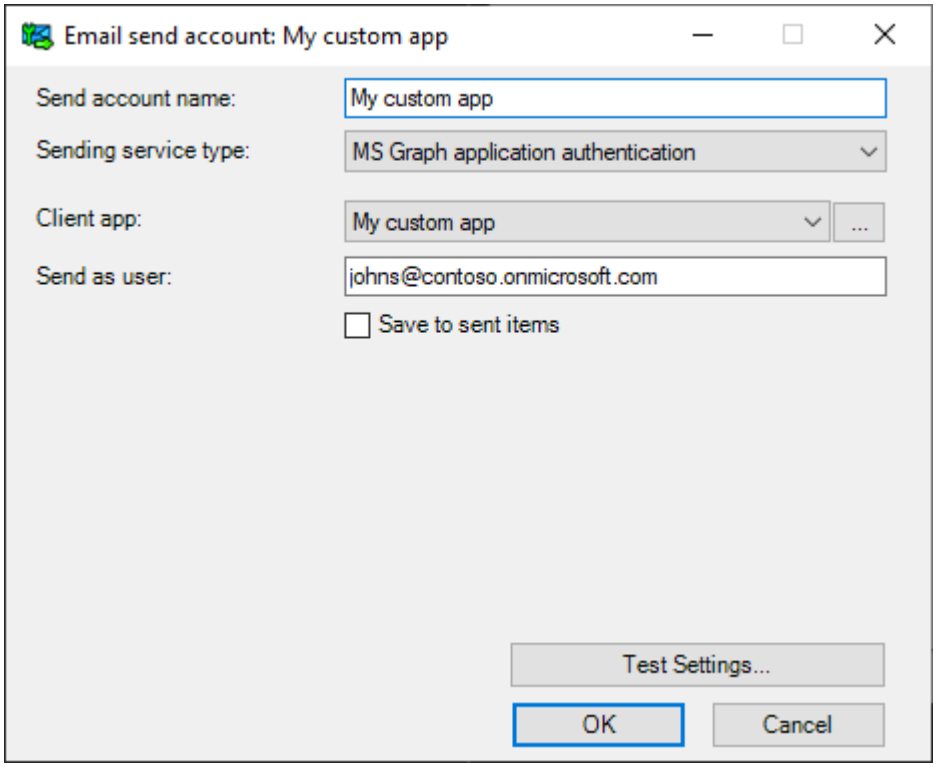
Once you have the SMTP Auth details fill out the rest of the fields:

- Enter the **SMTP server address** in the textbox.
- In the **'From' address** textbox, type the email address from which the emails will be sent. Note that depending on the SMTP server's configuration, there may be rules in place that check the 'From' and either allow or deny the relay.
- Enter the SMTP port number. Normally, if there is no authentication or SSL required, the port is 25. If SSL is required, it is normally 587. This will need to be supplied by the SMTP administrator.
- If SSL or TLS is required, tick the **Server requires an encrypted connection (SSL)** checkbox.
- If authentication is required, tick the **SMTP server requires authentication** checkbox and enter the **User name** and **Password**.
- Click **Test Settings** to test sending an email.
- Click **OK**.

Send Service Type: MS Graph application authentication

This method uses MS Graph API to send emails. Application authentication requires a Registered Application to be created in your Azure AD with a Client Secret that can be saved here. It does not execute as a 'user' in MS Graph, it executes as an 'application'. This means it will be able to send as any mailbox in the tenant.
To use this method, you will need to create a registered application in your Azure tenant. See this document for instructions on how to do this: Blue Swift Technologies | How to create a custom private client app in Azure.

Once the record has been created, ensure it is selected in the Client app drop down. Enter the user principal name for the mailbox that will be used to send mail.

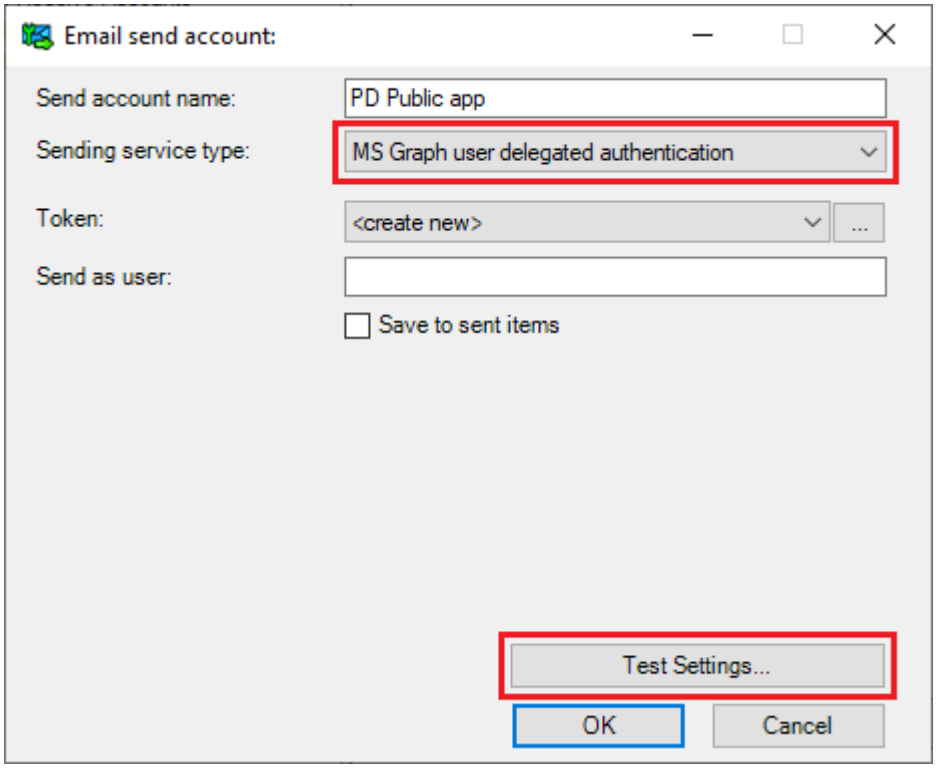


Click the Test Settings button to send a test email.

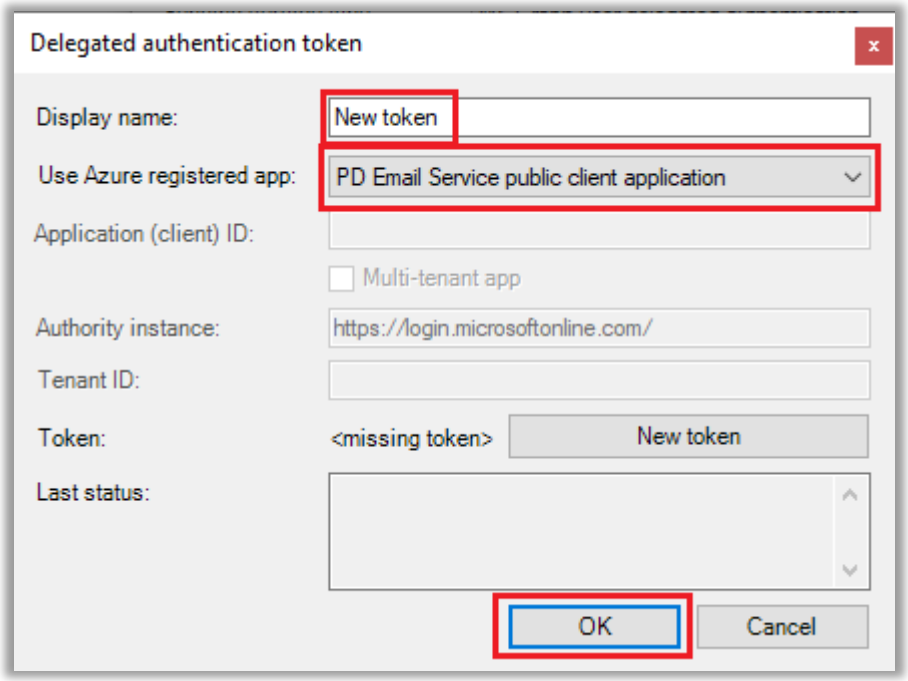
Send Service Type: MS Graph delegated authentication

A delegated authentication application executes as a specific user. This user will need to 'grant' access to the application. This is the simplest way to make use of MS Graph for sending emails and doesn't require the creation of your own registered application in your Azure tenant.

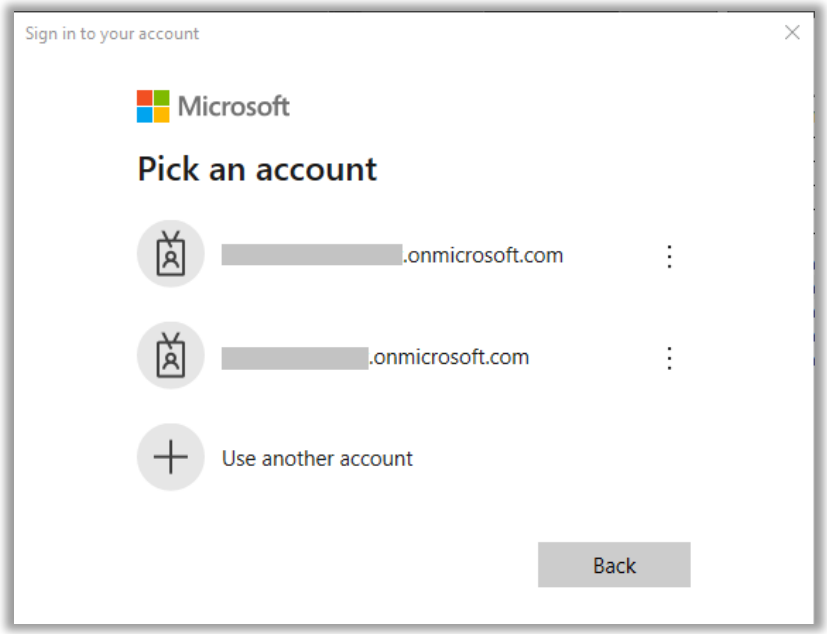
Once the Send service type dropdown is set to MS Graph user delegated authentication, leave the Token dropdown on <create new> and click Test Settings.



The **Delegated authentication token** window will be displayed. Enter anything in the **Display name** textbox. Leave the **Use Azure registered app** dropdown on **PD Email Service public client application** and click **OK**.

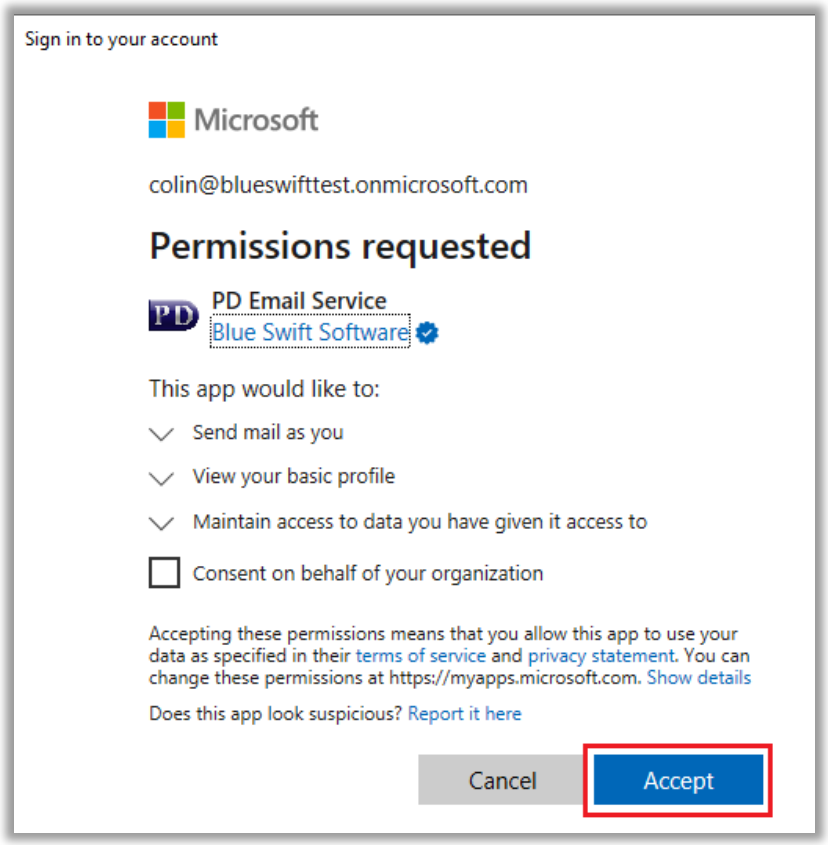


The Microsoft client credentials flow window will open. Log in as a user that has sufficient access rights to grant admin consent to enterprise application permissions.



Once logged in, it will show a window asking you to accept the permissions requested by the application.

Click the Accept button.



The **Send test email** window will be displayed. Note the email address to which the message will be sent in the **Send to** textbox and click the **Send email** button.

Check the mailbox to confirm receipt of the message.

Document revision date: 2021/10/08
Software version: 2.3.6.6