



Setting Up Sage 100

To Work With OAuth on Azure & Office 365

Email is one of the leading ways bad actors can gain access to your environment, collect your data, and gain access to your online accounts. Basic Authentication (Username and password) is being replaced by a more robust modern authentication method to help keep your environment secure. We strongly recommend that all Sage 100 users leverage these new methods, in conjunction with Multi-Factor Authentication for all users to reduce the likelihood of intrusion.

Our Sage consultants have prepared this step-by-step educational guide to walk you through the configuration of Modern Authentication (OAuth) for Azure/O365. This guide was developed specifically for IT professionals to interpret and aid the installation within your own environment. Given the self-service nature of this guide, it's important to note that the Blytheco team is not responsible for any misinterpretations of this documentation or failed installs as a result. Our consultants are available to assist with upgrades, installations, and system configuration at any time.

What you will need:

Supported Sage 100 Versions

- 2020 Release 6 +
- 2021 Release 4 +
- 2022 Release 1 +

Sage 100 Deployment Methods

- Sage 100 installed on-premise or in most private cloud environments
- Azure, AWS, and other public cloud services may have different methods.

Additional Requirements

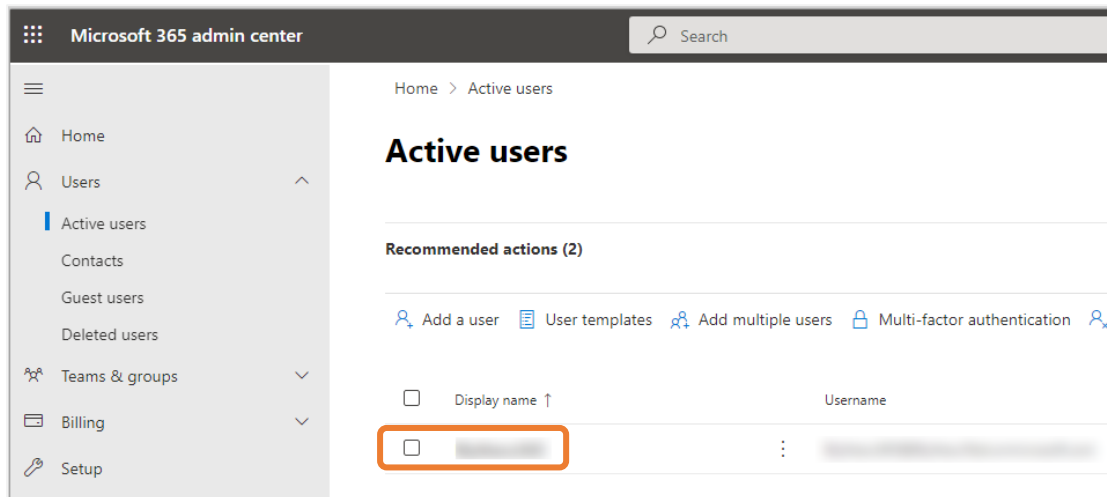
- Admin credentials for the Azure account. (If multi factor authentication is enabled you will need someone with access to that device)
- An email with an Office 365 professional license. This is the user that will send email from Sage 100. Using an email that is not used by a regular email user is suggested but not required.
 - Email Address (Username):
 - Password:

Information you will collect during setup:

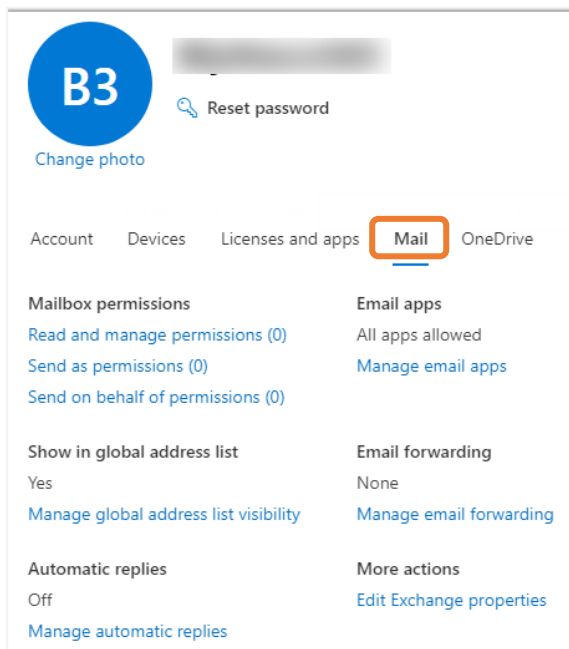
- Application (Client) ID:
- Authorization endpoint (v2):
- Token endpoint (v2):

Configure email account for authenticated SMTP:

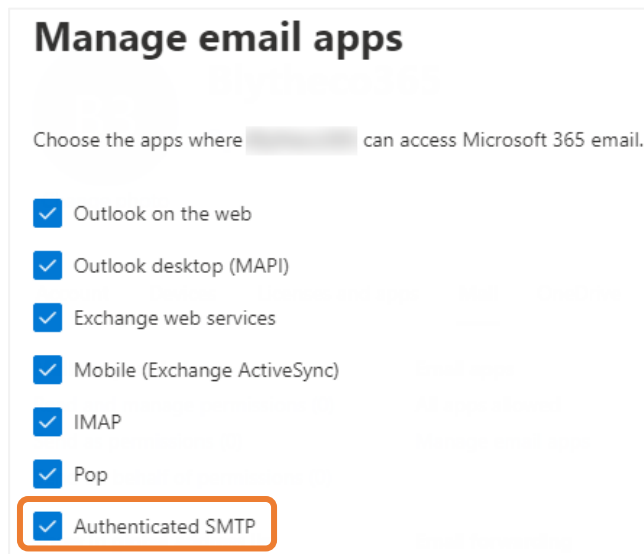
1. In a web browser go to <https://admin.microsoft.com/#/users> (if you don't get to active users click **Users / Active Users** on the left pane menu).
2. Login as an administrator



3. Click the user that will be used to send the email.
4. Click **Mail** in the menu at the top



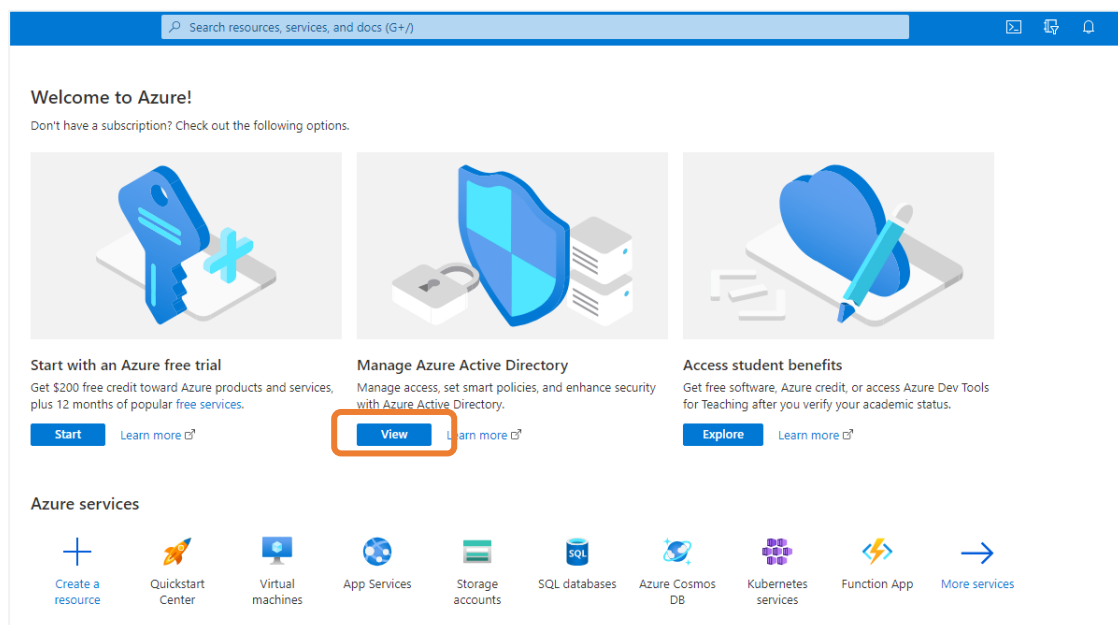
- Click **Manage Email Apps**



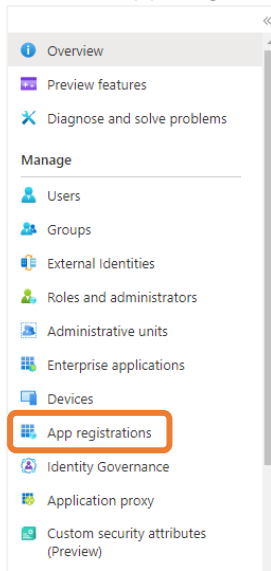
- Make Sure **Authenticated SMTP** is checked.
- Close the sub window.

Configure Azure:

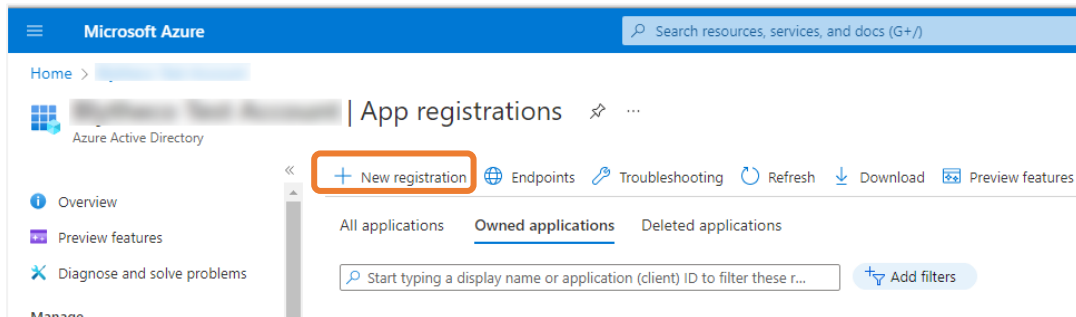
- In a web browser go to portal.azure.com
- Login as an admin user for the Azure account.
- Click on **Manage Azure Active Directory**



4. Click on **App Registrations** in the left menu pane:



5. Click on **New Registration** on the menu in the main pane.



6. Fill in the Register an application form with the following values.
- Name:** Sage 100 Email (any name works)
 - Supported Account Type:** Accounts in this organizational directory only
 - Redirect URI:**
 - Drop down box: **Public Client / Native**
 - Address box: https://localhost

- d. Click the button: *Register*

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations >

Register an application

Name

The user-facing display name for this application (this can be changed later).

Sage 100 Email

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Blytheco Test Account only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... | https://localhost

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

7. Copy the **Application (client) ID** and record it

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations >

Sage 100 Email

Search (Ctrl+)

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Essentials

Display name : Sage 100 Email

Application (client) ID : [highlighted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [0 web, 0 spa, 1 public client](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : Sage 100 Email

8. Click **Endpoints** in the main pane menu.

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations >

Sage 100 Email

Search (Ctrl+)

Delete **Endpoints** Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Essentials

Display name : Sage 100 Email

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [0 web, 0 spa, 1 public client](#)

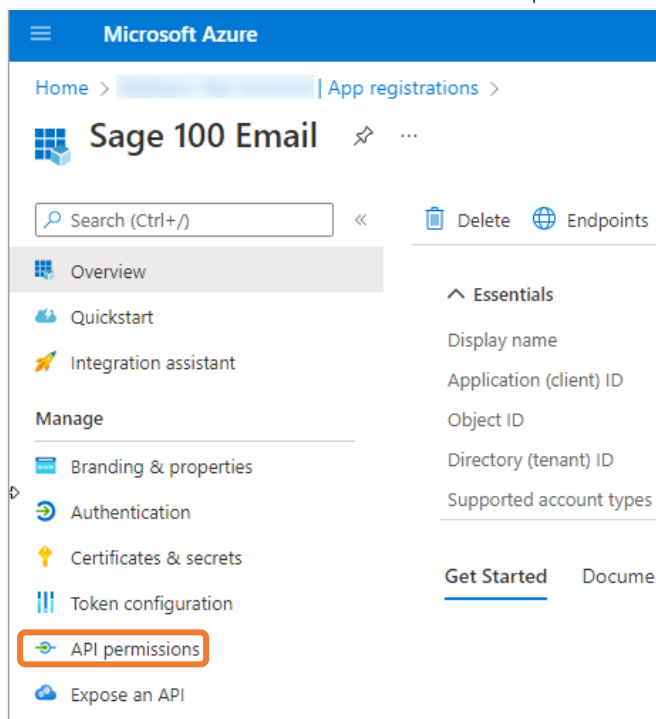
Application ID URI : [Add an Application ID URI](#)

Managed application in L... : Sage 100 Email

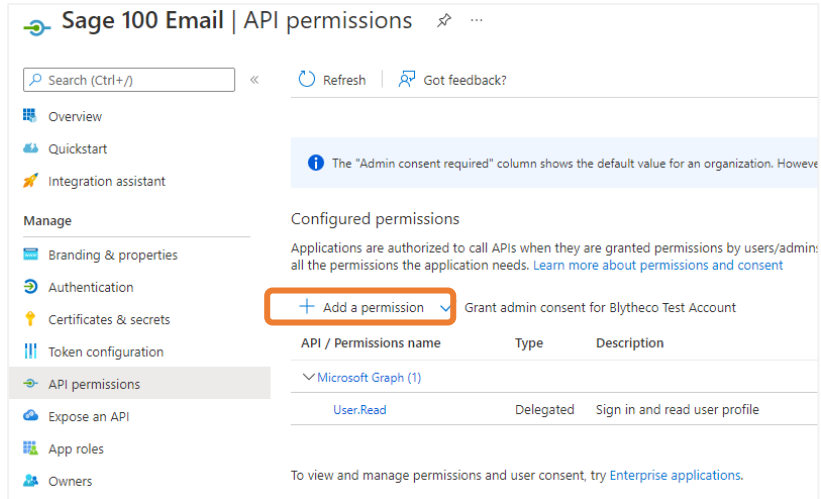
9. From the pop-up window copy and record these values:
- Authorization endpoint (v2)
 - Token endpoint (v2)



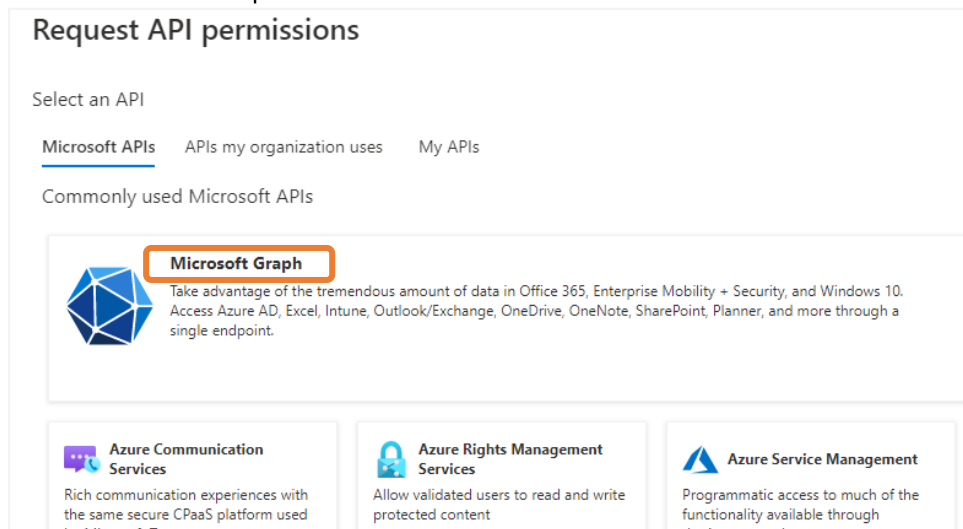
10. Click the X to close the window.
11. Click on **API Permissions** in the left menu pane.



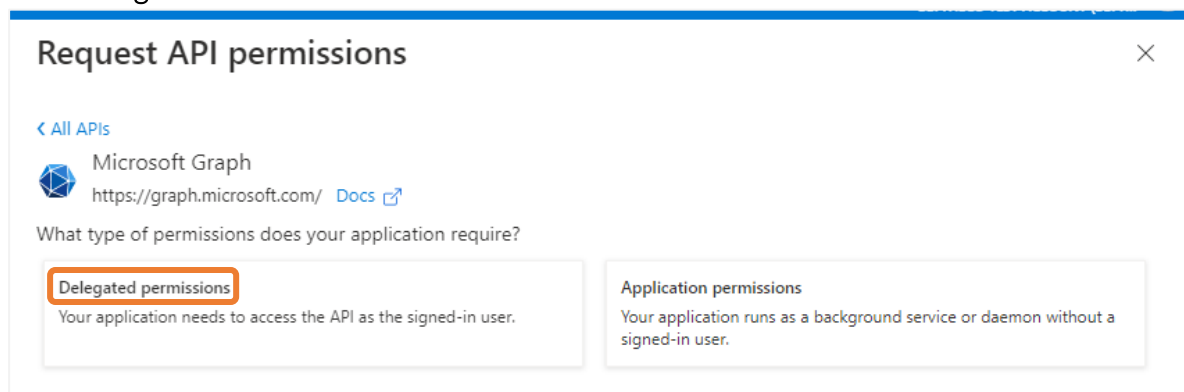
12. Click **Add a Permission** on the main pane menu.
- Note: You may see an “Admin consent required” message at the top. You can ignore that for now
 - Note: You may already see a Microsoft Graph permission **User.Read**. It is fine to leave.



13. Click **Microsoft Graph**



14. Click **Delegated Permissions**



15. In the Select Permissions section search for and select the following permissions:
- offline_access
 - SMTP.Send
 - User.Read

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Start typing a permission to filter these results

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
OpenId permissions	
☐ email View users' email address	No
☐ offline_access Maintain access to data you have given it access to	No
☐ openid Sign users in	No
☐ profile View user's basic profile information	No

Add permissions Discard

16. Click the **Add Permissions** button.
17. Click **Grant admin consent for...** In the menu in the main pane.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (3)				
offline_access	Delegated	Maintain access to data you have given it access to	No	...
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	...
User.Read	Delegated	Sign in and read user profile	No	...

18. Click **Yes**

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in [redacted]

Yes No

19. You will see the permissions granted.

Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for Blytheco Test Account](#)

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3) ...				
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for [redacted] ...
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	✓ Granted for [redacted] ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for [redacted] ...

20. Setup on Azure is complete.

Sage 100 Email Setup

- Open Sage 100 and Company maintenance.
- Select the company for which you want to set up email.
- Enter the settings:
 - *Authentication Method:* OAuth
 - *Address:* smtp.office365.com (this may be different with more advanced O365 Setups.)
 - *Port:* 587
 - *SMTP encryption:* TLS
 - *User ID:* the email account that will be sending the email used in the Azure setup.
 - *Client Secret:* {leave blank}
 - *Client ID:* Application (Client) ID from Azure
 - *Auth End Point:* Authorization endpoint (v2) from Azure
 - *Token End Point:* Token endpoint (v2) from Azure
 - *Scope:* https://outlook.office.com/SMTP.Send offline_access
 - *Redirect URL:* https://localhost
 - *Code Challenge Method:* S256
 - *Use 128-bit encryption....:* Checked

Company Maintenance (ABC) 8/11/2022

Company Code: ABC
Company Name: ABC Distribution and Service Corp.
Company Type: Demo

1. Main 2. Additional 3. Preferences 4. Dates 5. Payment 6. E-mail 7. Fax 8. Theme

SMTP (Mail) Server

Select the Authentication Method used to connect to the SMTP mail server.

Authentication Method: OAuth

Enter the DNS address (for example, mail.example.com) or IP address (for example, 128.0.0.102) of the SMTP server you are using to send e-mail. The address is needed to generate e-mail. Enter the port number the SMTP server is using if it is not configured to use the default port.

Address: smtp.office365.com Port: 587

Select the type of encryption to use between the SMTP client and SMTP server to send e-mail.

SMTP Encryption: TLS

Enter the user ID and client credentials that will be used to obtain an access token from the authorization server. While not always required, it is a good idea to only send 'authenticated' mail. This user does not have to be the one the mail is from, it is only used to log on to the e-mail server when sending mail.

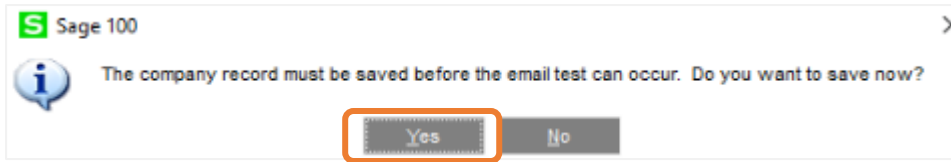
User ID: .onmicrosoft.com
Client ID:
Client Secret:
Auth End Point: https://login.microsoftonline.com/
Token End Point: https://login.microsoftonline.com/
Scope: https://outlook.office.com/SMTP.Send offline_access
Redirect URI: https://localhost
Code Challenge Method: S256

E-mail Options

Use 128-bit Encryption for Password Protected Documents ☒ Test E-mail...

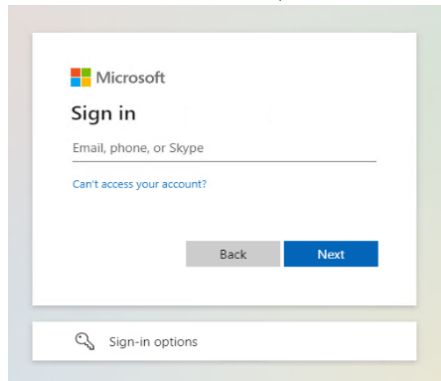
Use as Default Company for Server Settings ☒ Accept Cancel Delete

- Click **Test E-mail** (you can click Accept first and reopen the record if you wish)
- Click ok to Save if prompted.



- Fill in the email form to send a test email. The From email address is the address that was set up in O365 and in the email form in Sage.

- Click **Send**.
- You will be prompted to enter the username and password of the O365 email account.
 - If MFA is set up, you will need to authenticate with that here as well.
 - If you are prompted to allow access and or allow access on behalf of your organization, check the check box (if there is one) and accept.



- The test email should be sent.

The email address is now authenticated with Azure/O365 and will use a token to continuously authenticate.

- The token is valid for 90 days.
- It will refresh the token, if necessary, when an email is sent unless it has been more than 90 days when it was last refreshed. (If you send emails less than 90 days apart this should be perpetual).
- If the authentication chain is broken, you can return to company maintenance and test an email again to re authenticate.
- If the password on the O365 account is changed you will need to reauthenticate.

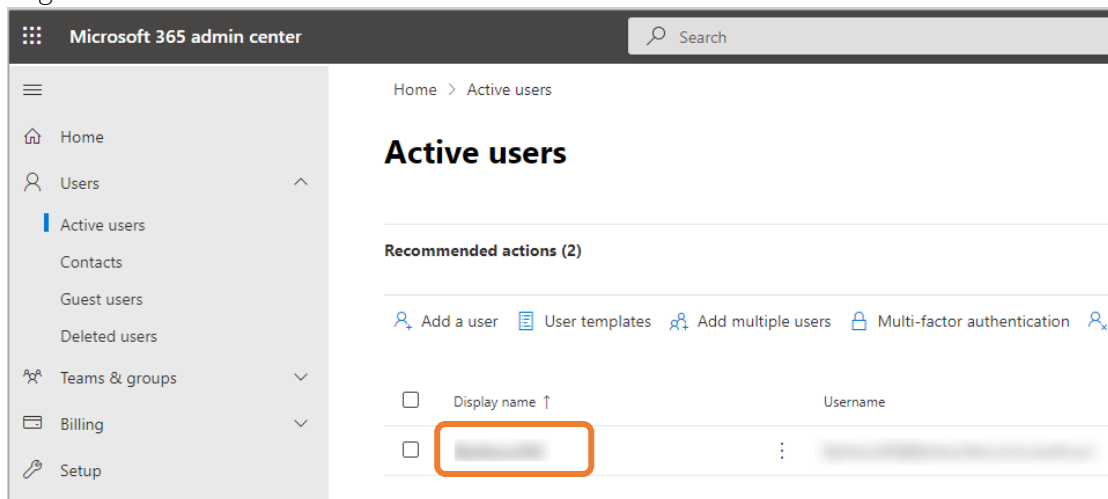
Additional Options

Additional Security

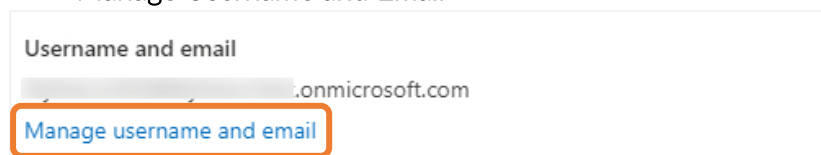
If you have an external static IP address, you can limit the IP address that an email can send from in O365 to your static IP address. (this will require advanced knowledge on O365)

Set alias emails up as the send from.

1. In a web browser go to <https://admin.microsoft.com/#/users> (if you don't get to active users click **Users / Active** users on the left pane menu).
2. Login as an administrator.



3. Click user that will be used to send the email.
4. Click **Account** in the menu at the top
5. Click **Manage Username and Email**



6. Enter an Alias Email name in the **Username** field
7. Click **Add**.
8. Click **Save Changes** at the bottom of the screen.

Manage username and email

If the primary email is also their username, then changing the primary email will also change their current username. An alias is another email address that people can use to email Blytheco365.

Primary email address and username

onmicrosoft.com



Aliases

Username		Domains	
	@	onmicrosoft.com	Add

9. You can now use that email address as the send from in Paperless Office.