Connect to Office 365 SMTP server

Overview

Microsoft is in the process of deprecating basic authentication for the Office 365 SMTP server. This means a more modern authentication is required where a token is provided which the sender must use in order access the Office 365 SMTP server.

Microsoft 365 Admin Center

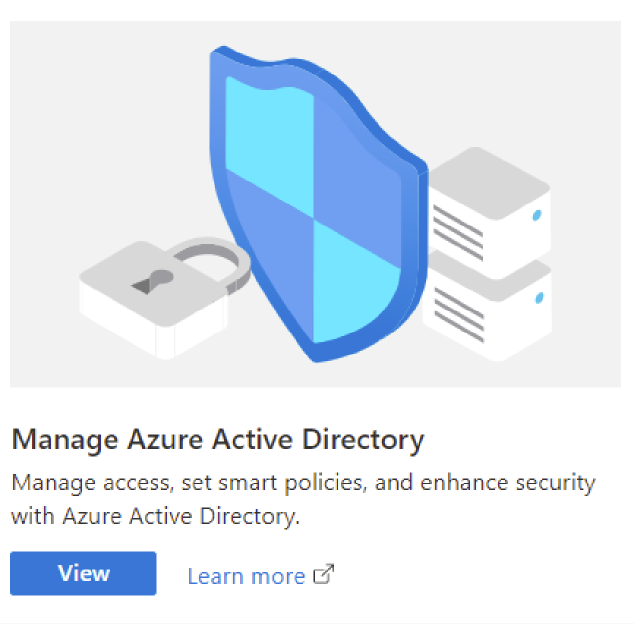
The first step is to make sure Authenticated SMTP is enabled for the user that you wish to send email from.

This is done by going to the **Microsoft 365 admin center**, locating the user under the **Active Users**, clicking the **Manage email apps** link and checking **Authenticated SMTP**.

Azure Active Directory

The next step is to create an XLReporter Mailer app in the Azure Active Directory. To do so, use your web browser open the Azure Active Directory (portal.azure.com).

Log in with the user you wish to send email through, if it is not already logged in.

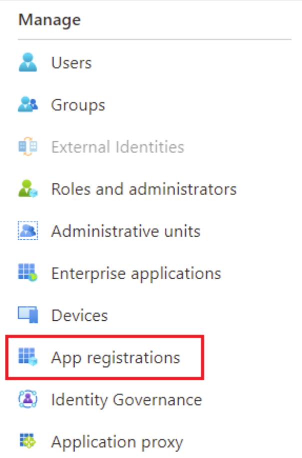


Manage Azure Active Directory

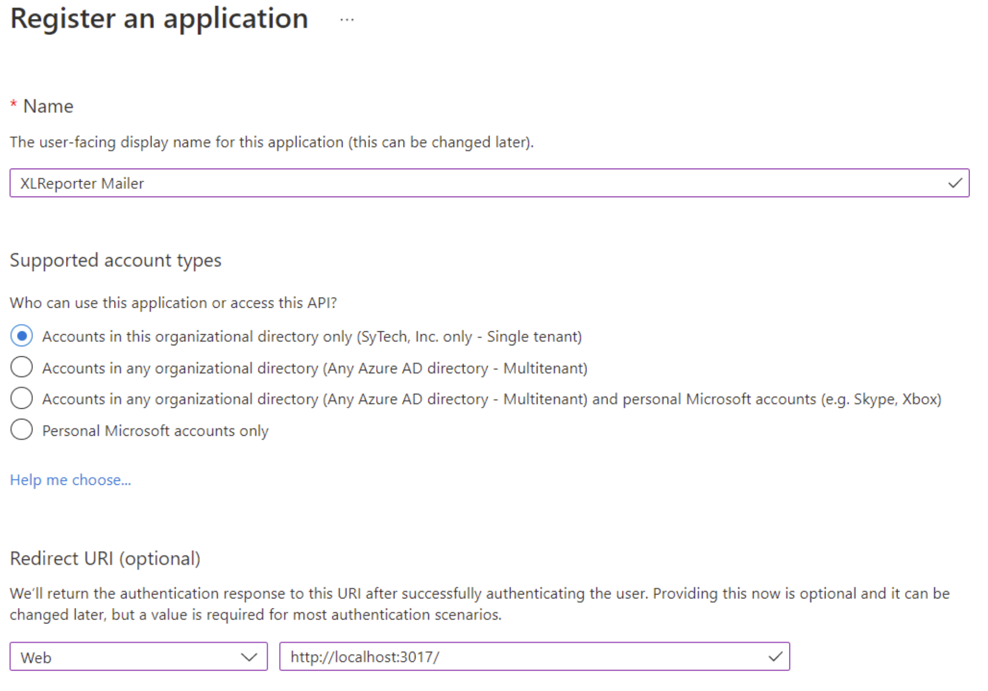
Manage access, set smart policies, and enhance security with Azure Active Directory.

In the **Manage Azure Active Directory** section click **View**.

Create and Register Application



On the left side, under **Manage**, select **App registrations**. In **App registrations** on the right, select **New registration**.



Register an application ···

* Name

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

XLReporter Mailer ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (SyTech, Inc. 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)

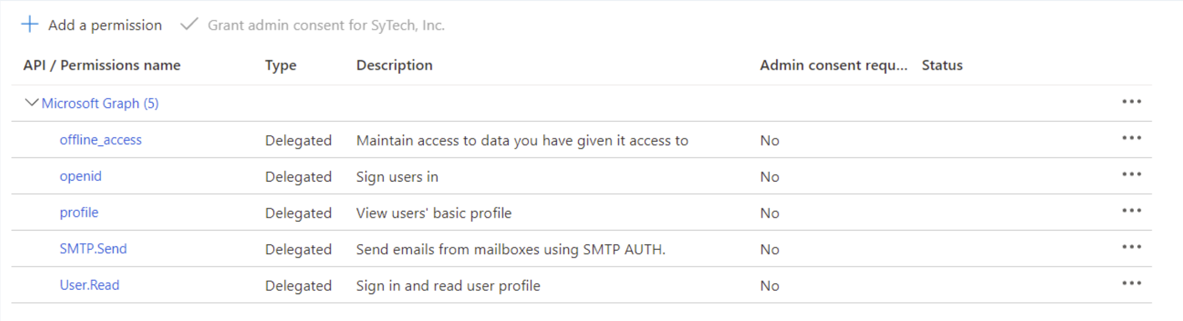
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ⌄ | http://localhost:3017/ ✓

Set **Name** to *XLReporter Mailer*. Under the **Redirect URI** section, select **Web** and then specify *http://localhost:Port/* where *Port* is an open port number on your system (typically port *3017* is not used by anything). Click **Register** at the bottom to register the application.

Add Permissions

Now permissions need to be added. Select API permissions on the left side. The following permissions need to be added:



API / Permissions name	Type	Description	Admin consent requ...	Status	
⌄ Microsoft Graph (5)					···
offline_access	Delegated	Maintain access to data you have given it access to	No		···
openid	Delegated	Sign users in	No		···
profile	Delegated	View users' basic profile	No		···
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No		···
User.Read	Delegated	Sign in and read user profile	No		···

Permissions are added by clicking Add a permission, selecting Microsoft Graph, Delegated permissions and then checking the ones listed. The offline_access, openid and profile permissions are found under OpenId permissions and SMTP.Send is found under SMTP.

Create a Client Secret

Select **Certificates & Secrets** on the left side. On the right side, click **New client secret**.

In **Add a client secret**, set a **Description** and when it **Expires**. Click **Add** when complete.

Be sure to record the **Value** for the secret you just created. This is the only time it will be visible, and you will need to provide it to XLReporter.

Identify Information

The application configuration is now complete. The following information must be identified and provided to XLReporter:

- Port
  The port number specified in the Redirect URI. If you do not recall, you can view this in the **Overview** by clicking **Redirect URIs**.
- Client ID
  The client ID can be found in the Azure Active Directory by selecting **Overview** on the left side. **Application (client) ID** is listed directly under **Display Name**.
- Client Secret
  The client secret value should have been recorded in the previous step.
- OAuth 2.0 authorization endpoint (v2)
  In the **Overview**, click **Endpoints** at the top. The **OAuth 2.0 authorization endpoint (v2)** is the first one listed.
- OAuth 2.0 token endpoint (v2)
  In the same **Endpoints** display, **OAuth 2.0 token endpoint (v2)** is the second one listed.

Windows Firewall

If the Windows Firewall is enabled on the machine where XLReporter is installed, the XLReporter Mailer application should be allowed to communicate through Windows Defender Firewall. You will need administrator privileges to do this.

Open the **Windows Defender Firewall**. Click **Allow an app or feature through the Windows Defender Firewall**.

To add, click **Change settings** at the top. Scroll to the bottom and click **Allow another app…**

Browse to **C:\XLReporter\bin** (assuming XLReporter is installed on the C drive) and select **XLRiMailDesign.exe**. Click **Add**.

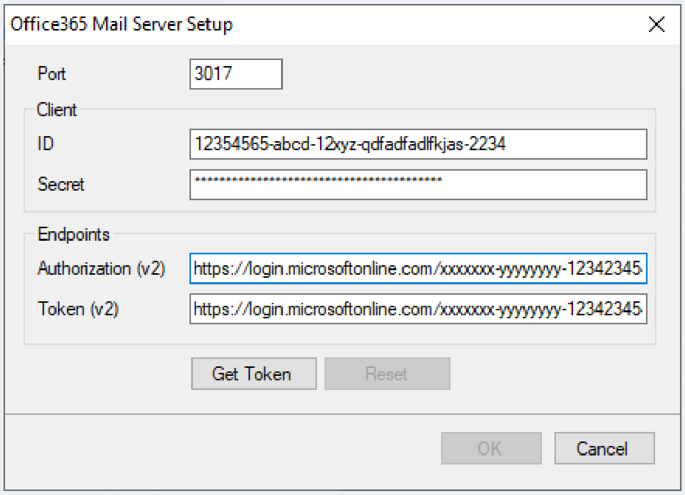
XLReporter Mail Designer should now appear in the list. Check to enable the appropriate networks.

Please note that if this step is skipped, when attempting to authenticate you may receive a message from Windows Defender Firewall prompting to allow the application to communicate. This will require administrator privileges right at that time which may not be readily available which is why this step is strongly recommended.

Mail Designer

Office 365 Setup

In the Mail Designer, under the **Edit** menu select *Office 365*.



Office365 Mail Server Setup

Port: 3017

Client

ID: 12354565-abcd-12xyz-qdfadfadlfkjas-2234

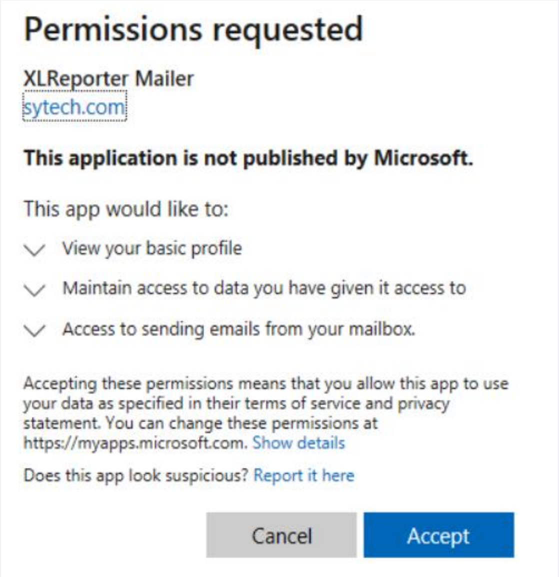
Secret: **

Endpoints

Authorization (v2): https://login.microsoftonline.com/xxxxxxx-yyyyyyyy-12342345

Token (v2): https://login.microsoftonline.com/xxxxxxx-yyyyyyyy-12342345

Specify the information recorded from the previous step. When completed click **Get Token**.



Permissions requested

XLReporter Mailer
sytech.com

This application is not published by Microsoft.

This app would like to:

- View your basic profile
- Maintain access to data you have given it access to
- Access to sending emails from your mailbox.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

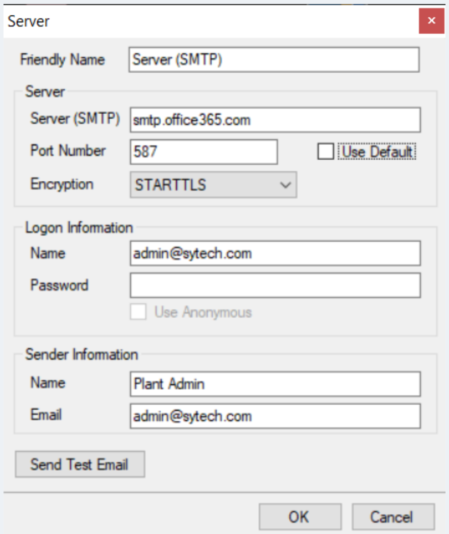
Does this app look suspicious? Report it here

The **Office 365 Verification** window opens. If you are not logged in, log in as the user to send email through. For **Permissions requested**, click **Accept**. This will retrieve your token and close the verification window. Click **OK** to save the settings.

The token generated will expire at some point in the future. During runtime, if the token is expired it will be automatically refreshed with Office 365 without any user intervention. If you would like to manually refresh the token, you can access these settings and click the **Refresh** button to do so. Click **OK** to save the settings.

If you need to generate a new token (for instance, if you want to change the account with which to send email or your **Client Secret** has expired), you can do so by accessing these settings and clicking the Reset button. You can then enter the required information and click **Get Token** to generate a new token. Click **OK** to save the settings.

Server Setup



Friendly Name: Server (SMTP)

Server

Server (SMTP): smtp.office365.com

Port Number: 587 □ Use Default

Encryption: STARTTLS

Logon Information

Name: admin@sytech.com

Password:

□ Use Anonymous

Sender Information

Name: Plant Admin

Email: admin@sytech.com

When configuring the SMTP server, under **Logon Information**, the **Password** does not need to be specified because authenication is now done using the token established in the previous step.

Expired Client Secret

The client secret set up in the Azure Active Directory must be set with an expiration. When this secret expires, the Mailer will fail to send emails, logging the error "Failed to refresh access token", followed by "The provided client secret keys for app "xxxxx" are expired".

At this point, you must return to the **Azure Active Directory** and select the **XLReporter Mailer** application by clicking **App registrations** on the left and then clicking the application itself.

Click the **Certificates & secrets** on the left and define a new client secret. You can also delete the expired secret listed since it is no longer valid. Be sure to record the new secret **Value**.

In XLReporter's **Mail Designer** (**Project Explorer, Tools, Email and SMS**) select **Edit**, **Office** 365. Click **Reset** to enable the settings and set the **Client Secret** to the new secret generated. Click **Get Token** to generate a new token and **OK** to save the settings.

Email and text messages should now send again.