Office 365

SYSPRO 8

Reference Guide

Published: January 2023

CONTENTS

Office 365

Exploring 1

Starting 2

Solving 4

Using 7

Office 365

Exploring

Where it fits in?

Microsoft Office 365 lets you access the latest versions of **Word**, **Excel**, **PowerPoint**, **Outlook**, **OneNote**, etc., wherever you go and across all your devices.

With **Microsoft Office 365** integrated to SYSPRO, you don't need a separate desktop installation of **Office 365**; you can integrate or combine SYSPRO data into an **Office 365** document directly from **Office 365**.

Terminology

Microsoft Azure

Microsoft Azure is a cloud computing service created by **Microsoft** to build, test, deploy, and manage applications and services through Microsoft-managed data centers.

It caters for:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

In addition, **Microsoft Azure** supports different programming languages, tools and frameworks (including **Microsoft**-specific and third-party software and systems).

Microsoft O365 Tenant

A **Microsoft Office 365** tenant is a regional location that provides cloud services dedicated to an organization (e.g. **Exchange Online**, **SharePoint Online**, **Teams**, etc). It falls within the overall **O365 Data Center** and can be seen as an organization's sandbox environment, housing all its digital assets (e.g. users, domains, subscriptions and data).

Starting

Prerequisites

- A valid SYSPRO login, with SYSPRO administrator access rights.
- A valid **Microsoft Azure** subscription.
- A valid **Microsoft Office 365** account.

> Ensure that you save the appropriate entries within the **AUTHORITY** and **DISCOVERY RESOURCE ID** setup options (*Setup Options* > *System Setup* > *Connectivity*). Although both fields already contain valid pre-populated entries, you must open the **Setup Options** program and save the settings for these to take effect.

Configuring

The following configuration options in SYSPRO may affect processing within this program or feature, including whether certain fields and options are accessible.

Setup Options

The **Setup Options** program lets you configure how SYSPRO behaves across all modules. These settings can affect processing within this program.

Company General

Setup Options > *Company* > *General*

- Email/SMTP settings:
  - Method when emailing
  - Use system-wide SMTP details
  - SMTP server IP address
  - Outgoing email address
  - Username
  - Password
  - Server port
  - Use SSL

Connectivity System Setup

Setup Options > System Setup > Connectivity

- Email/SMTP settings:
  - SMTP server IP address
  - Outgoing email address
  - Username
  - Password
  - Server port
  - Use SSL
  - Use system-wide settings
- Office 365:
  - Tenant id
  - Exchange web service
  - Client id
  - Authority
  - Discovery resource id

Restrictions and Limits

- SYSPRO's **Multi-Factor Authentication** feature is not currently available with **Microsoft Office 365** integration.

  For **Microsoft Office 365** Multi Factor Authentication, an app password can be configured in Office 365 against the user's account, which can then be captured within SYSPRO's SMTP sections (**Personal Settings** / **Setup Options**). This is then used when sending email via SMTP in a server-side environment.

Solving

System messages

Error messages

AADSTS7000218: The request body must contain the following parameter: 'client_assertion' or 'client_secret'

Synopsis

Full error message:

```
One or more errors occurred.

AADSTS7000218: The request body must contain the following parameter: 'client_assertion' or 'client_secret'.

Trace ID: d63025eb-0e48-4f4e-9e25-273c45269c00

Correlation ID: e4497a70-e9a9-4783-ae08-7e45bcd62cc9

Timestamp: 2020-06-15 12:04:21Z
```

Cause

This error message appears when emailing or exporting to **Excel** after configuring a new native application in **Microsoft Azure**, if the **Default Client Type** is not configured as public.

Solution

Update the configuration of your application in **Microsoft Azure** as follows:

1. Go to the **App Registration** for your application.
2. Select **Authentication** from the **Manage** menu.
3. Locate the **Default client type** section under **Advanced Settings** and enable the **Treat application as a public client** option.
4. Save your changes.

FAQs

How do I configure different Microsoft Office 365 tenants for operators?

1. Open the **Office 365 Tenant Maintenance** program (*Program List* > *Administration* > *General Setup*) and add the multiple tenant records according to your requirements.
2. Open the **Personal Settings** program (*SYSPRO Ribbon bar* > *Home* > *Personal Settings*) to indicate which tenant SYSPRO must for the operator use when communicating with **Microsoft Office 365**).

What happens if I define an email output option in SRS?

If email is defined as an output option in SRS, then Office Integration lets you browse on contacts defined in **Office 365** when you browse on **To**, **Cc** or **Bcc** email addresses.

Which platform is used when exporting information from SYSPRO?

Office 365 Excel is used when exporting information from a SYSPRO grid view or list view to **Microsoft Excel**.

How do I configure an app password for SMTP emailing and Microsoft Office 365 integration?

If you use Office 365 credentials to send email using SMTP (using server-side reporting) then you'll need to configure an app password to use when sending email via SMTP. This is because basic authentication has been deprecated by **Microsoft**.

1. Microsoft Office 365 configuration:
   a. Sign into the Microsoft Office 365 portal:
      `portal.office.com`
   b. Select the **View Account** option or navigate to
      `https://myaccount.microsoft.com/?ref=MeControl`
   c. From the **Security Info** section, select the **Update info** option.
   d. Select **Add sign-in method**.
   e. Indicate **App password** as the method that you want to add.
   f. Select **Add** to proceed.
   g. Enter the relevant **App password** name.
   h. Once you have entered the app password name, the **Next** button becomes enabled.

      Select **Next** for your app password to be generated.
   i. Copy the generated password for use within SYSPRO to update your Office 365 integration password.
2. Log into SYSPRO:
   a. Open the**Personal Settings** program (*SYSPRO Ribbon bar* > *Home* > *Personal Settings*).
   b. Update the password entry against the **Password** field of the **Office 365 Credentials** section with the app password created for the specific Office 365 account.
   c. Save your changes.

The configured operator then uses the app password when sending email via SMTP using Office 365 Integration, thereby allowing SMTP emailing in a personalized way.

Alternatively, if you have a generic system-wide account used by all operators, then you can define this app password against your system-wide settings (*Setup Options* > *System Setup* > *Connectivity*).

For more information regarding Microsoft's deprecation of Basic authentication:

`https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online`

Using

Microsoft Azure Configuration

How to register your application in Microsoft Azure

Before you can enable **Microsoft Office 365** support within SYSPRO, you must register your application within **Microsoft Azure**.

> This provides you with an **Application ID** that is required when configuring SYSPRO.

1. Access the **Microsoft Azure** portal:

   `https://portal.azure.com`

2. Select the **Azure Active Directory** option from the main menu.
3. From the **Manage** menu, select the **App registrations** option.
4. Select the specific application you want to maintain.

   Alternatively, select the **New Registration** option if you want to create a new application.

   > For detailed information on how to create a new application registration, please view the Microsoft documentation site: https://learn.microsoft.com/en-us/power-apps/developer/data-platform/walkthrough-register-app-azure-active-directory.

5. Ensure that the following **Advanced Settings** options (accessible from the **Authentication** section) are enabled against your application:

   - Access tokens
   - ID tokens
   - Treat application as a public client

6. Add the required APIs to your application:

   Select **View API permissions** followed by the **Add a permission** option.

   The **Request API Permissions** screen is displayed.

7. From the **Microsoft APIs** pane, add the following APIs:

   - Azure Active Directory Graph
   - Exchange
   - SharePoint

8. Set up the permissions for each API:

   Azure Active Directory Graph

a. Select the **Azure Active Directory Graph** API.

   The **Request API Permissions** screen is displayed.

b. Select **Delegated permissions** and enable the following permissions:

   - **Directory**
     - Directory.AccessAsUser.All
     - Directory.Read.All
   - **Group**
     - Group.Read.All
   - **User**
     - User.Read

c. Select the **Add permissions** option to save your changes.

d. Enable the **Grant Admin Consent** option for the API.

Exchange

a. Select the **Exchange** API.

   The **Request API Permissions** screen is displayed.

b. Select **Delegated permissions** and enable the following permissions:

   - **Calendars**
     - Calendars.Read
     - Calendars.ReadWrite
   - **Contacts**
     - Contacts.Read
     - Contacts.ReadWrite
   - **Mail**
     - Mail.Read
     - Mail.ReadWrite
     - Mail.Send

c. Select the **Add permissions** option to save your changes.

d. Enable the **Grant Admin Consent** option for the API.

SharePoint

   a. Select the **SharePoint** API.

      The **Request API Permissions** screen is displayed.

   b. Select **Delegated permissions** and enable the following permissions:

      - **MyFiles**
        - MyFiles.Read
        - MyFiles.Write

   c. Select the **Add permissions** option to save your changes.

   d. Enable the **Grant Admin Consent** option for the API.

9. Once you have successfully configured the required permissions, save your application.

SYSPRO Configuration

How to configure SYSPRO for Office 365

Once you have registered and configured your application within **Microsoft Azure**, you need to configure details within SYSPRO.

1. Obtain the **Application ID** from the **Microsoft Azure** platform for your newly created application.
2. Launch SYSPRO and open the **Setup Options** program (*Setup Options* > *System Setup* > *Connectivity*).
    a. Ensure the following fields are configured correctly with your details:
        - Email/SMTP settings:

SMTP server IP address

This is the default IP address of the specific SMTP server that SYSPRO will use to send messages when the user requests a password reset.

Outgoing email address

This is the default email address of the sender of the message.

This entry must contain a valid email structure (e.g. `auto.generated.mail@company.com`).

Username

This the user name of the email account.

Password

This is the password of the email account.

Server port

This indicates the server port to be used.

We recommend using **Port 587** for SMTP communications in SYSPRO, as it includes TLS encryption and adheres to IETF guidelines.

We advise against using **Port 25** and **Port 465**:

- **Port 25** is typically used for SMTP relaying, but is traditionally blocked by Internet Service and Cloud Hosting Providers to curb the amount of spam relayed from compromised computers or servers. We don't recommend any email traffic using this port unless you're specifically managing your

- - own mail server.
  - **Port 465** is not compliant. IANA has reassigned a new service to this port, so you shouldn't use this port for SMTP communications anymore. It's typically only used if your email server demands it.

- Office 365:

Tenant id

This indicates the id of your active directory in the **Microsoft Azure** portal.

Your **SYSPROOfficeCloud** application will be added to this directory.

Exchange web service

This indicates the `URI` to your exchange web service address.

If you don't have an exchange server, you can use the default provided by **Microsoft Office 365** (i.e. `https://outlook.office365.com/ews/exchange.asmx`).

Client id

This indicates the client ID of the **SYSPROOfficeCloud** application added to your active directory in **Microsoft Azure**.

Authority

This is pre-populated with `https://login.microsoftonline.com`.

> The **System Setup** program needs to be accessed and saved so that the pre-populated entry in this field can take effect.

Discovery resource id

This is pre-populated with `https://graph.microsoft.com`.

> The **System Setup** program needs to be accessed and saved so that the pre-populated entry in this field can take effect.

b. Save your changes and exit the program.

3. Open the **Personal Settings** program in SYSPRO (*SYSPRO Ribbon bar > Home > Personal Settings*).

a. Configure the **Office 365 credentials** per operator as follows:

   - Enable the **Microsoft Office 365** option.
   - Capture the operator's **Office 365** credentials (i.e. **User name** and **Password**).
   - Indicate which tenant must be used when communicating with **Office 365**.

b. Save your changes and exit the program.

Your **Office 365** support is now configured for support within SYSPRO.

Affected programs

The following indicates areas in the product that may be affected by implementing this feature:

Office 365 Tenant Maintenance

Program List > Administration > General Setup

This program lets you maintain multiple tenants for **Microsoft Office 365**, which then stores the information in the AdmOfficeTenants system-wide table.

Once this is configured, you can use the **Personal Settings** program (*SYSPRO Ribbon bar > Home > Personal Settings*) to define which tenant SYSPRO must use for each operator when communicating with **Microsoft Office 365**.

Setup Options

Setup Options > System Setup > Connectivity

This program lets you configure the **EMAIL/SMTP SETTINGS** and **OFFICE 365** for the company.

Personal Settings

SYSPRO Ribbon bar > Home > Personal Settings

This program lets you maintain the **Microsoft Office 365** credentials per operator.

SYSPRO™

www.syspro.com