

Setting up e-mail (OAUTH) in Microsoft Entra/Microsoft Azure

Introduction

This document briefly describes a general example of activating client secret authentication in Microsoft Entra/Microsoft Azure to use with e-mail in Exchange/Office365.

The document also describes how to test settings from Microsoft Entra/Microsoft Azure in the Monitor ERP client with the client secret method.

Table of Contents

Introduction	1
Microsoft Entra/Microsoft Azure.....	2
Limitations.....	2
Security considerations.....	2
Client secret authentication	3
Microsoft Azure setup	3
Monitor ERP setup (Client secret method).....	12
Settings for incoming e-mail (Client secret method)	17

Microsoft Entra/Microsoft Azure

- An account to Microsoft Entra/Microsoft Azure is required.
- To test e-mail, the required credentials must be added under "Users" in the Microsoft Entra/Microsoft Azure portal.

Limitations

- Only one authentication method can be active at a time.
- The setting for "Supported account type" may differ depending on company setup - this guide describes a setup with the "single tenant" account type.

Please note: **Further configuration and customization of settings according to each environment is required** to complete the setup. Also note that this document **does not cover the security aspect** of setting up e-mail using these settings in a tenant.

Security considerations

The document **does not cover settings or configurations for security**; it covers settings used to test that a configuration for the authentication method work in the Monitor ERP client on a basic level. Please note: **It is up to each IT department to select and configure appropriate security settings** in their respective environments.

Example: You may want to complement with suitable security settings if you configure a tenant with the Client secret authentication method according to guidelines from Microsoft:

<https://learn.microsoft.com/en-us/powershell/module/exchange/new-applicationaccesspolicy?view=exchange-ps>

Client secret authentication

Microsoft Azure setup

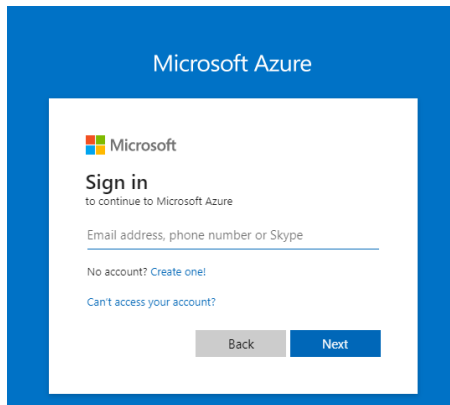
Please note: Microsoft currently provides two administrative portals:

- portal.azure.com
- entra.microsoft.com

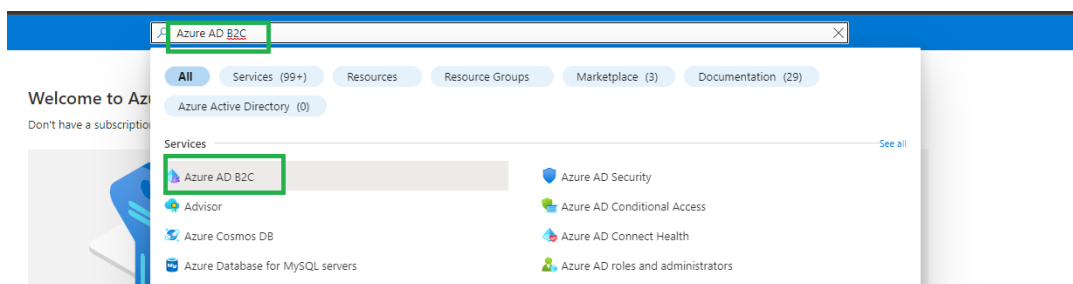
The guide below describes the setup process in Microsoft Azure.

*For an existing EWS-based setup that is being migrated to Microsoft Graph, continue from step 10.

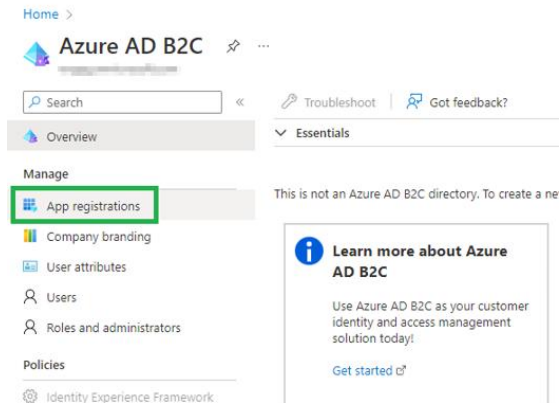
1. Sign in with an existing account at <https://portal.azure.com>.



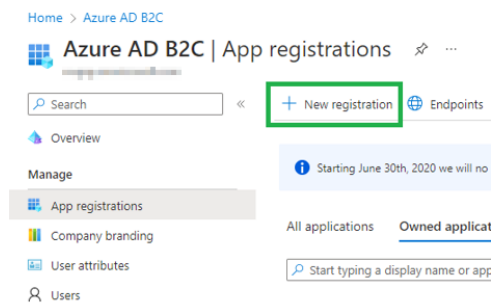
2. Once signed in, search for and access "Azure AD B2C".



3. Click on "App registrations".



4. Click on "New registration".



5. Enter a name and select your preferred account type (single tenant by default).

Home > Azure AD B2C | App registrations

Register an application

* Name

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

Monitor G5 1

Supported account types

Choose the account types that can use this application or access this API

Single tenant only - 2 Help me choose

6. Enter the appropriate "Redirect URI" – for example, select "Public client/native (mobile & desktop)" and at the URL <https://login.microsoftonline.com/common/oauth2/nativeclient>.

Refer to — <https://learn.microsoft.com/en-us/azure/active-directory/develop/reply-url>.

Home > Azure AD B2C | App registrations

Register an application

* Name

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

Monitor G5 ✓

Supported account types

Choose the account types that can use this application or access this API

Single tenant 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://login.microsoftonline.com/common/oauth2/nativeclient> ✓

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. Click on the "Register" button.

Home > Azure AD B2C | App registrations

Register an application

* Name

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

Monitor G5 ✓

Supported account types

Choose the account types that can use this application or access this API

Single tenant 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.

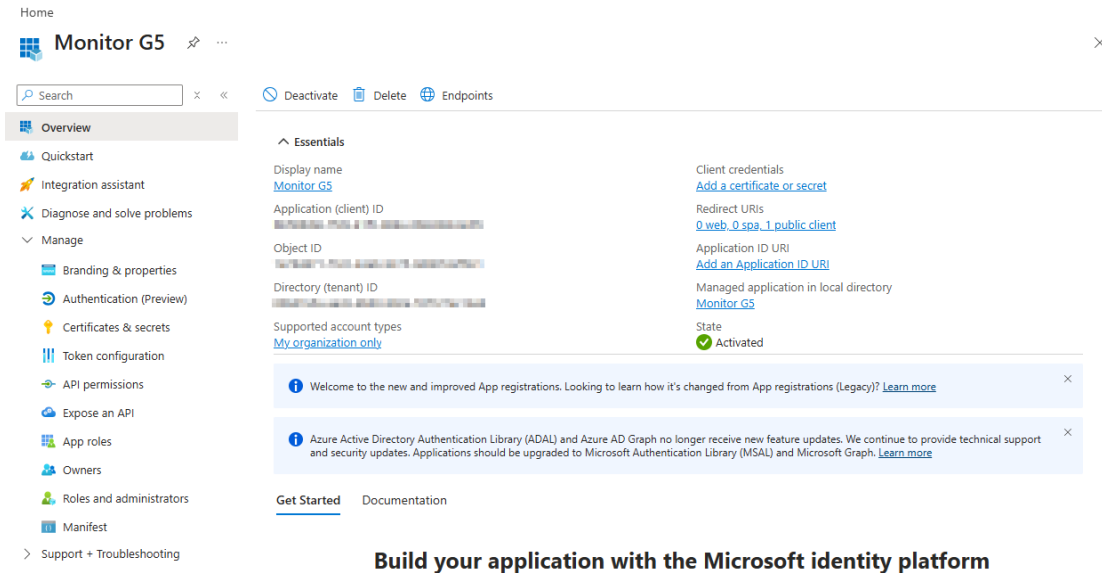
Public client/native (mobile ...) ✓ <https://login.microsoftonline.com/common/oauth2/nativeclient> ✓

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

8. You will be forwarded to the menu of the application you just registered, if not – click on the application.



Home

Monitor G5

Search

Deactivate Delete Endpoints

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication (Preview)
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

Essentials

Display name	Client credentials
Monitor G5	Add a certificate or secret
Application (client) ID	Redirect URIs
0.web.0.spa.1.public.client	0.web.0.spa.1.public.client
Object ID	Application ID URI
Add an Application ID URI	Managed application in local directory
Directory (tenant) ID	Monitor G5
Supported account types	State
My organization only	Activated

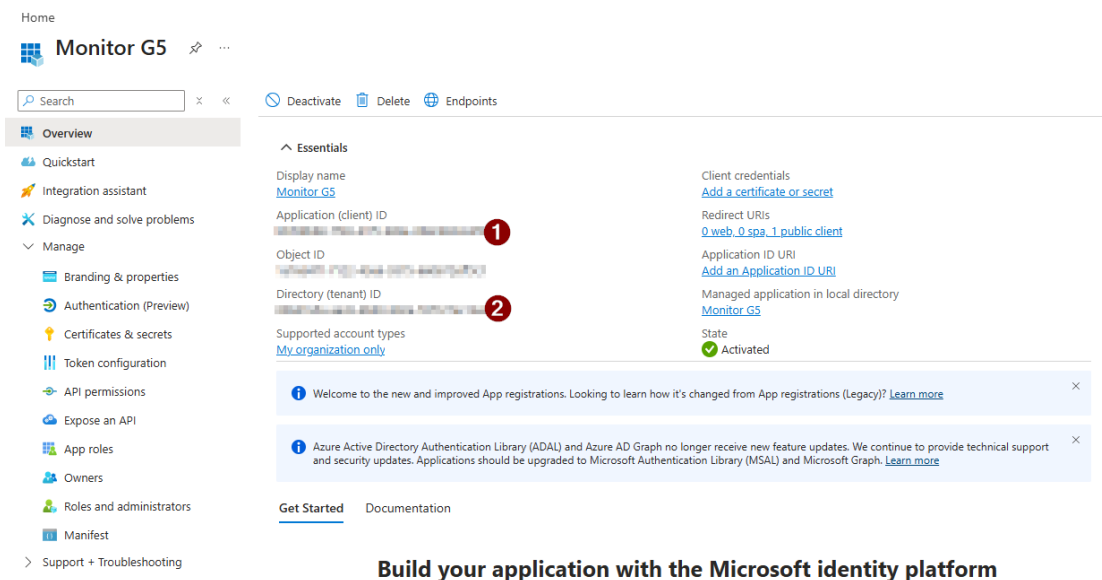
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

Build your application with the Microsoft identity platform

9. Copy the values of the Application (client) ID and Directory (tenant) ID and save them, you will need them later.



Home

Monitor G5

Search

Deactivate Delete Endpoints

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication (Preview)
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

Essentials

Display name	Client credentials
Monitor G5	Add a certificate or secret
Application (client) ID	Redirect URIs
0.web.0.spa.1.public.client	0.web.0.spa.1.public.client
Object ID	Application ID URI
Add an Application ID URI	Managed application in local directory
Directory (tenant) ID	Monitor G5
Supported account types	State
My organization only	Activated

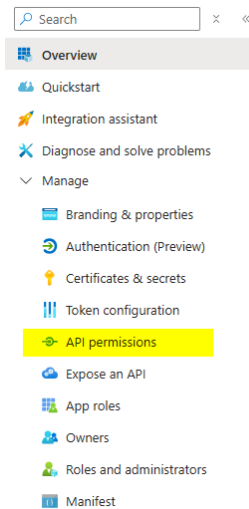
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

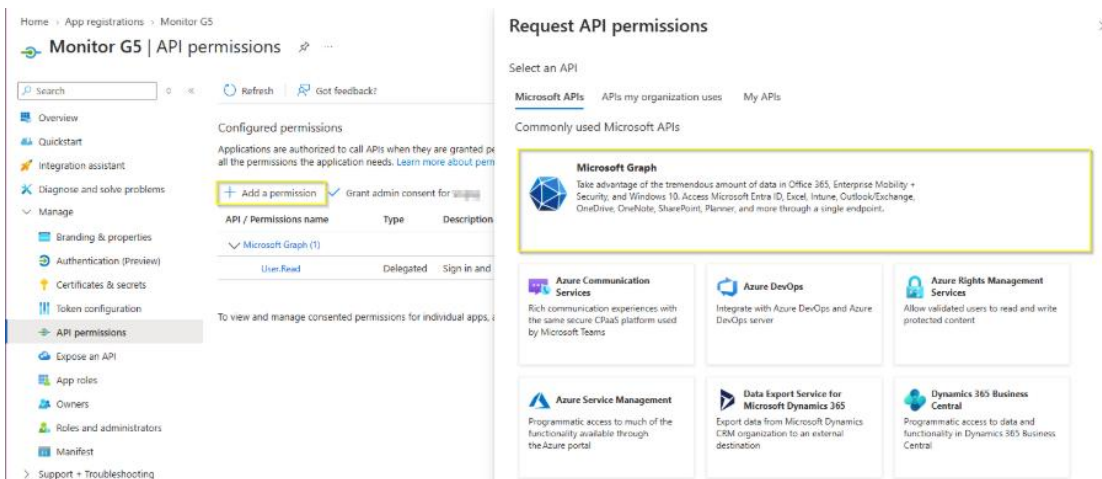
Get Started Documentation

Build your application with the Microsoft identity platform

10. Click on “API permissions” in the left-hand menu.



11. Click the “Add a permission” button and continue with “Microsoft Graph” as the API.



12. Select Application permissions

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.

13. Add permissions:

Calendars.ReadWrite to read and write calendars in all mailboxes,
Mail.ReadWrite to read and write mail in all mailboxes (used for incoming e-mail M2M), and **Mail.Send** to send mail as any user.

Then click the “add permissions” button.

The screenshot shows the 'Request API permissions' dialog in the Azure portal. The 'Mail' category is expanded, showing the following permissions:

Permission	Description	Consent
Mail.Read	Read mail in all mailboxes	Yes
Mail.ReadBasic	Read basic mail in all mailboxes	Yes
Mail.ReadBasic.All	Read basic mail in all mailboxes	Yes
☒ Mail.ReadWrite	Read and write mail in all mailboxes	Yes
☒ Mail.Send	Send mail as any user	Yes

At the bottom of the dialog, there are two buttons: 'Add permissions' (highlighted in green) and 'Discard'.

14. Confirm that permission has been added.

+ Add a permission ✓ Grant admin consent for [User]

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes	Not granted for [User]
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Not granted for [User]
Mail.Send	Application	Send mail as any user	Yes	Not granted for [User]

15. Grant admin consent for the {tenant} and then click "Yes".

Home > App registrations > Monitor G5

Monitor G5 | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication (Preview)
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in [tenant]? This will update any existing admin consent records this application already has to match what is listed below.

Yes No

of configured permissions should include

+ Add a permission Grant admin consent for [tenant]

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				...
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes	Not granted for [tenant] ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Not granted for [tenant] ...
Mail.Send	Application	Send mail as any user	Yes	Not granted for [tenant] ...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Earlier versions of Monitor ERP used Exchange Web Services (EWS). Following Microsoft's retirement of EWS October 1st 2026, Monitor ERP now supports Microsoft Graph for Microsoft 365 integrations.

16. Verify that the icons are green.

+ Add a permission Grant admin consent for [tenant]

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				...
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes	Granted for [tenant] ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Granted for [tenant] ...
Mail.Send	Application	Send mail as any user	Yes	Granted for [tenant] ...
User.Read	Delegated	Sign in and read user profile	No	Granted for [tenant] ...

17. Click on "Authentication" in the left-hand menu.

Home > Monitor G5

Monitor G5 | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration

The "Admin consent required" column shows the

Configured permissions

Applications are authorized to call APIs when they have all the permissions the application needs. [Learn more](#)

+ Add a permission Grant admin consent

API / Permissions name	Type
------------------------	------

18. Under "Advanced settings", set "Enable the following mobile and desktop flows" to "No".

Home > Azure AD B2C | App registrations > Monitor G5

Monitor G5 | Authentication

Search

Got feedback?

editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows: Yes **No**

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock ⓘ

Configure the application instance modification lock. [Learn more](#) Configure

Save Discard

19. Save the settings.

Home > Azure AD B2C | App registrations > Monitor G5

Monitor G5 | Authentication

Search

Got feedback?

editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows: Yes **No**

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock ⓘ

Configure the application instance modification lock. [Learn more](#) Configure

Save Discard

20. Access "Certificates & secrets" in the left-hand menu and click on "New client secret".

Home > Azure AD B2C | App registrations > Monitor G5

Monitor G5 | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets** ⓘ
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

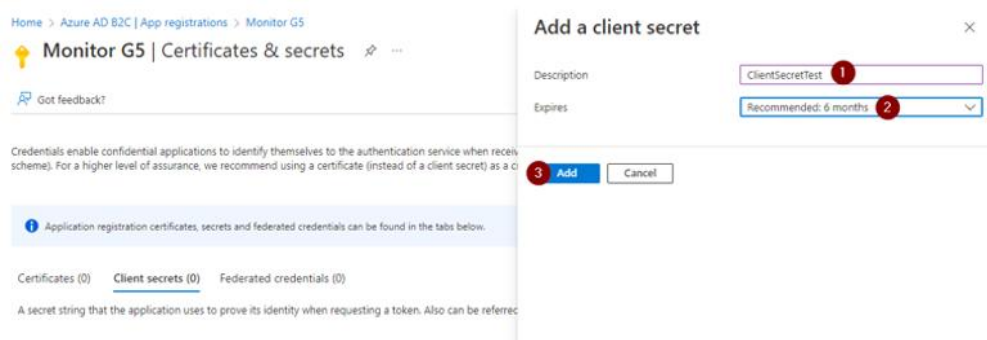
Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

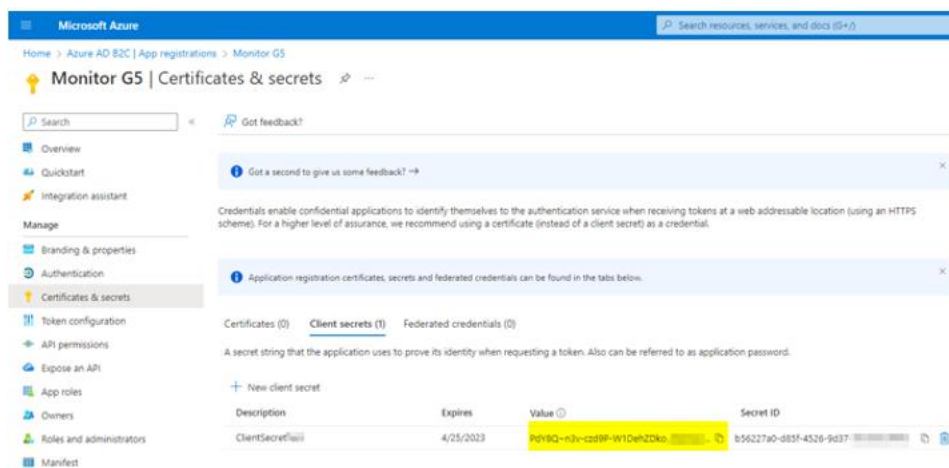
+ New client secret ⓘ

Description	New client secret	Expires	Value ⓘ	Secret ID
No client secrets have been created for this application.				

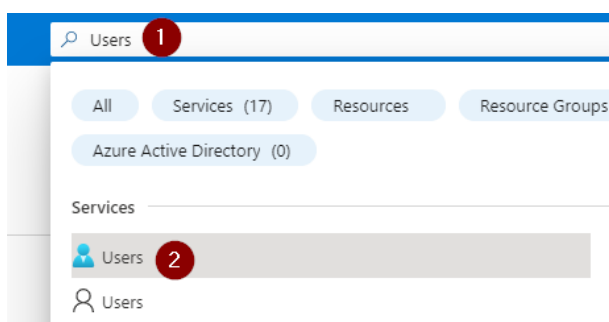
21. Enter a name and set a preferred client secret expiration, then click “Add”.



22. Note that **the client secret can only be copied once** – copy the content in “Value” and store it in a safe place, you will need it later.



23. Go to "Users", copy an existing e-mail address, then test it in the Monitor ERP client according to the next part.

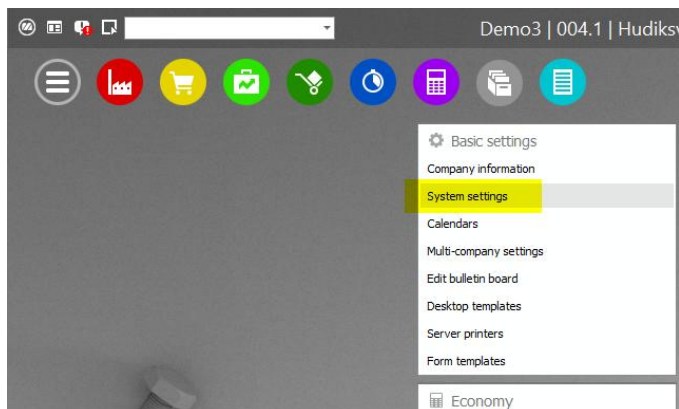


Monitor ERP setup (Client secret method)

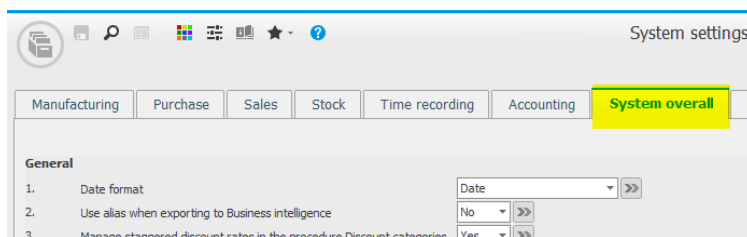
1. Start the Monitor ERP client and sign in with the appropriate admin account.



2. Access the "System settings" procedure.



3. Click on the "System overall" tab.



4. In "E-mail method" select "Server based, via Microsoft Exchange Online".

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Monitor Mobile Agent

General

1. Date format: Date
2. Use alias when exporting to Business intelligence: No
3. Manage staggered discount rates in the procedure Discount categories: Yes
4. Part grouping term for discount categories: Product group
5. Company is approved for F-tax: Yes
6. Time when order day/start day changes to next day: 12:00
7. Show identifier for external programs (Extra fields): No
8. Search indexing (Monitor search): Yes
9. Warn if part name does not have a translation: Yes
10. Use modern connection (Microsoft Graph) for Exchange Online: No

Backup

11. Number of days before warning: 3
12. E-mail sender of backup notification:
13. User name (Exchange):
14. Password (Exchange):

E-mail

15. E-mail method: **Server based, via Microsoft Exchange Online**
16. Server address (Exchange/SMTP): 192.168.100.13
17. Port (Exchange/SMTP): 0
18. User name (SMTP):
19. Password (SMTP):
20. Use SSL: No

5. In "Use modern connection for Exchange Online (Microsoft Graph)", select "Yes".

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Monitor Mobile Agent

General

1. Date format: Date
2. Use alias when exporting to Business intelligence: No
3. Manage staggered discount rates in the procedure Discount categories: Yes
4. Part grouping term for discount categories: Product group
5. Company is approved for F-tax: Yes
6. Time when order day/start day changes to next day: 12:00
7. Show identifier for external programs (Extra fields): No
8. Search indexing (Monitor search): Yes
9. Warn if part name does not have a translation: Yes
10. **Use modern connection (Microsoft Graph) for Exchange Online: Yes**

Backup

11. Number of days before warning: 3
12. E-mail sender of backup notification:
13. User name (Exchange):
14. Password (Exchange):

E-mail

15. E-mail method: Server based, via Microsoft Exchange Online
16. Server address (Exchange/SMTP): 192.168.100.13
17. Port (Exchange/SMTP): 0
18. User name (SMTP):
19. Password (SMTP):
20. Use SSL: No

6. Set the server address – outlook.office365.com.

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Monitor Mobile Agent

General

1. Date format: Date
2. Use alias when exporting to Business intelligence: No
3. Manage staggered discount rates in the procedure Discount categories: Yes
4. Part grouping term for discount categories: Product group
5. Company is approved for F-tax: Yes
6. Time when order day/start day changes to next day: 12:00
7. Show identifier for external programs (Extra fields): No
8. Search indexing (Monitor search): Yes
9. Warn if part name does not have a translation: Yes
10. Use modern connection (Microsoft Graph) for Exchange Online: Yes

Backup

11. Number of days before warning: 3
12. E-mail sender of backup notification:
13. User name (Exchange):
14. Password (Exchange):

E-mail

15. E-mail method: Server based, via Microsoft Exchange Online
16. Server address (Exchange/SMTP): outlook.office365.com
17. Port (Exchange/SMTP): 0
18. User name (SMTP):
19. Password (SMTP):
20. Use SSL: No

7. Paste the Application (client) ID previously saved from Microsoft Azure in the corresponding field.

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Mobile client Agent

E-mail

13. E-mail method: Server based, via Microsoft Exchange Online
14. Server address (Exchange/SMTP): outlook.office365.com
15. Port (Exchange/SMTP): 0
16. User name (SMTP):
17. Password (SMTP):
18. Use SSL: No
19. Maximum size for files in e-mail: 10

Microsoft Entra ID (Azure Exchange/SharePoint)

20. Application (client) ID:
21. Directory (tenant) ID:
22. Authentication flow: User name/Password
23. Client secret:

8. Paste the Directory (tenant) ID previously saved from Microsoft Azure in the corresponding field.

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Mobile client Agent

E-mail

13. E-mail method: Server based, via Microsoft Exchange Online
14. Server address (Exchange/SMTP): outlook.office365.com
15. Port (Exchange/SMTP): 0
16. User name (SMTP):
17. Password (SMTP):
18. Use SSL: No
19. Maximum size for files in e-mail: 10

Microsoft Entra ID (Azure Exchange/SharePoint)

20. Application (client) ID:
21. Directory (tenant) ID:
22. Authentication flow: User name/Password
23. Client secret:

9. In "Authentication flow" select "Client secret".

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Mobile client Agent

E-mail

13. E-mail method: Server based, via Microsoft Exchange Online

14. Server address (Exchange/SMTP): outlook.office365.com

15. Port (Exchange/SMTP): 443

16. User name (SMTP):

17. Password (SMTP):

18. Use SSL: No

19. Maximum size for files in e-mail: 10 MB

Microsoft Entra ID (Azure Exchange/SharePoint)

20. Application (client) ID: *****

21. Directory (tenant) ID: *****

22. Authentication flow: Client secret

23. Client secret: [Redacted]

10. Paste the Client secret previously saved from Microsoft Azure in the corresponding field.

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Mobile client Agent

E-mail

13. E-mail method: Server based, via Microsoft Exchange Online

14. Server address (Exchange/SMTP): outlook.office365.com

15. Port (Exchange/SMTP): 443

16. User name (SMTP):

17. Password (SMTP):

18. Use SSL: No

19. Maximum size for files in e-mail: 10 MB

Microsoft Entra ID (Azure Exchange/SharePoint)

20. Application (client) ID: *****

21. Directory (tenant) ID: *****

22. Authentication flow: Client secret

23. Client secret: [Redacted]

11. The port can be set, for more information refer to <https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>.

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Mobile client

E-mail

13. E-mail method: Server based, via Microsoft Exchange Online

14. Server address (Exchange/SMTP): outlook.office365.com

15. Port (Exchange/SMTP): 443

16. User name (SMTP):

17. Password (SMTP):

18. Use SSL: No

19. Maximum size for files in e-mail: 10 MB

12. Click on the green icon next to the server address to test the settings.

System settings

Manufacturing Purchase Sales Stock Time recording Accounting **System overall** Mobile client

E-mail

13. E-mail method: Server based, via Microsoft Exchange Online

14. Server address (Exchange/SMTP): outlook.office365.com

15. Port (Exchange/SMTP): 443

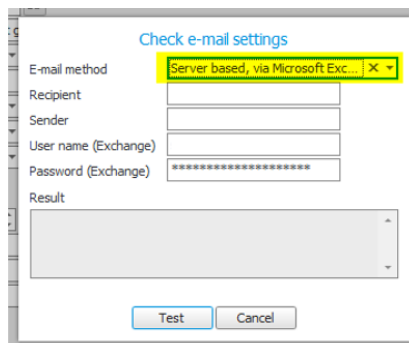
16. User name (SMTP):

17. Password (SMTP):

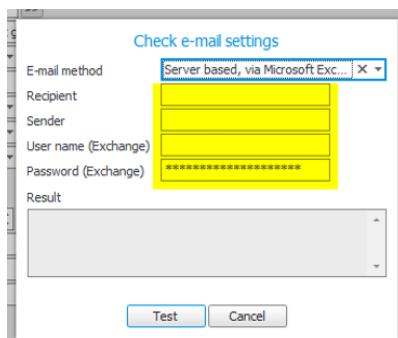
18. Use SSL: No

19. Maximum size for files in e-mail: 10 MB

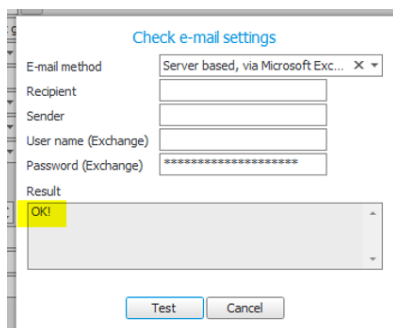
13. Set e-mail method to "Server based, via Microsoft Exchange Online".



14. Enter a valid recipient, sender, user name and password.



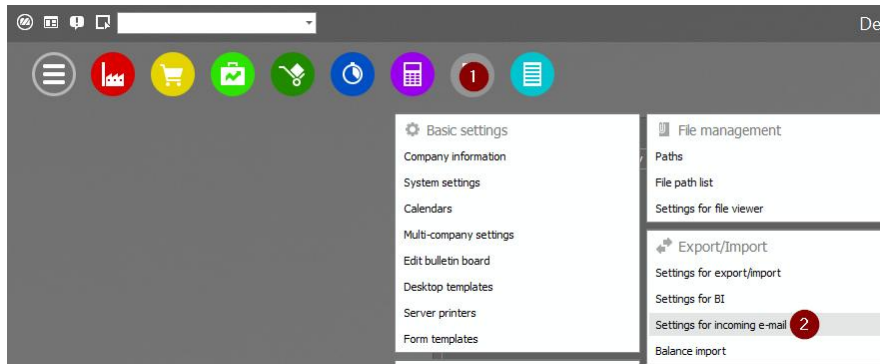
15. Press the "Test" button – the message "OK" will be displayed if everything is set up according to the examples in this document.



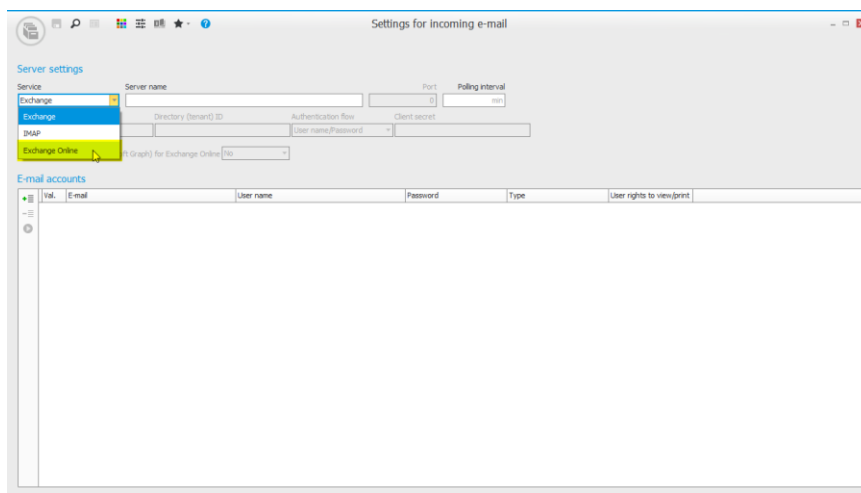
(Please note: If the service has been set up recently you may receive a **403 Forbidden message** due to delays when updating a tenant in Microsoft Azure portal. In this case, wait a moment then press "Test" again. If you encounter other messages in the "Result" box, please refer to the online documentation by Microsoft).

Settings for incoming e-mail (Client secret method)

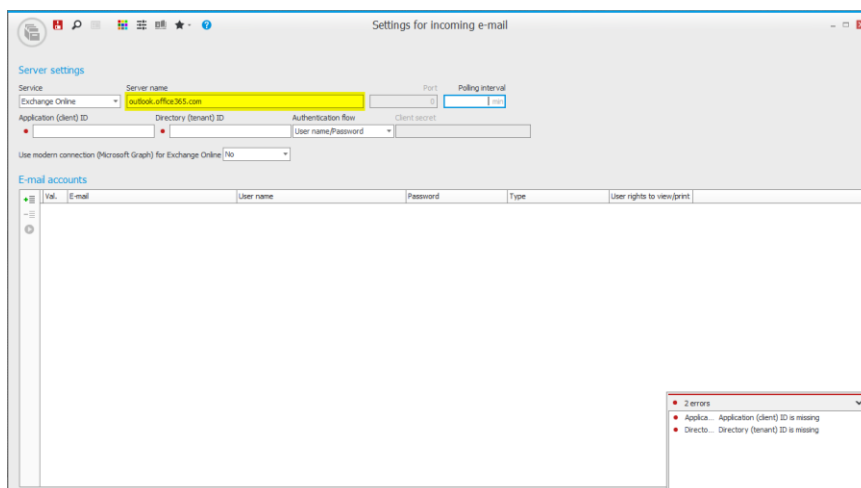
1. Access the "Settings for incoming e-mail" procedure.



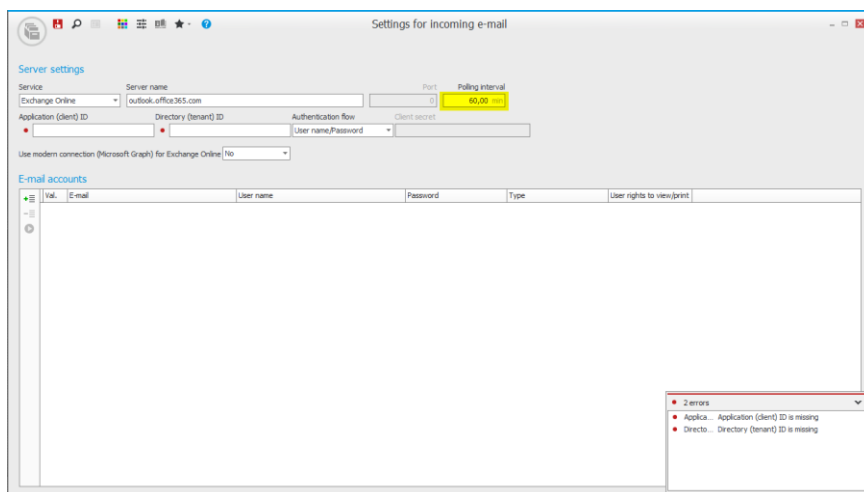
2. Under "Service" select "Exchange Online".



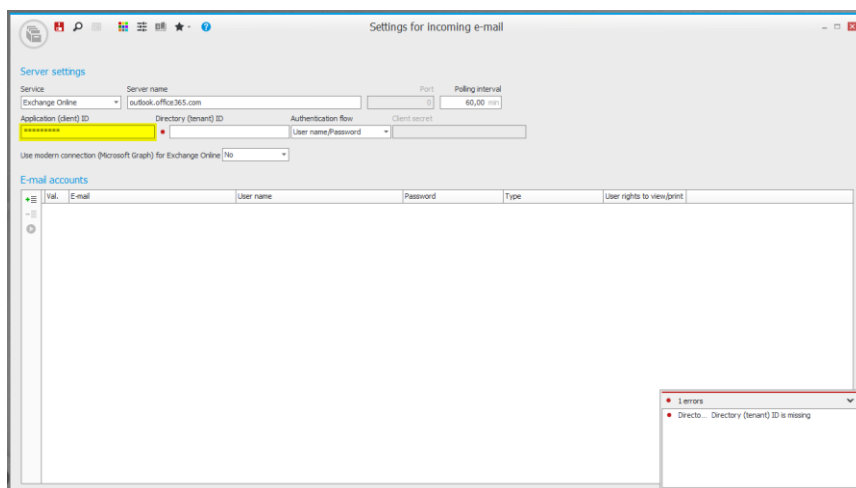
3. Enter the URL to the server – for example outlook.office365.com.



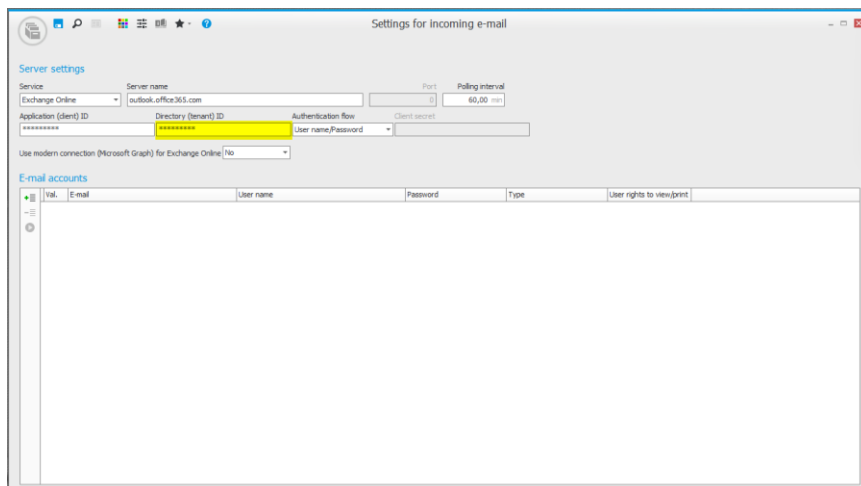
4. Set a polling interval (in minutes) according to your requirements, in our example we set this to 60,00 to check for new e-mails on the server once every hour.



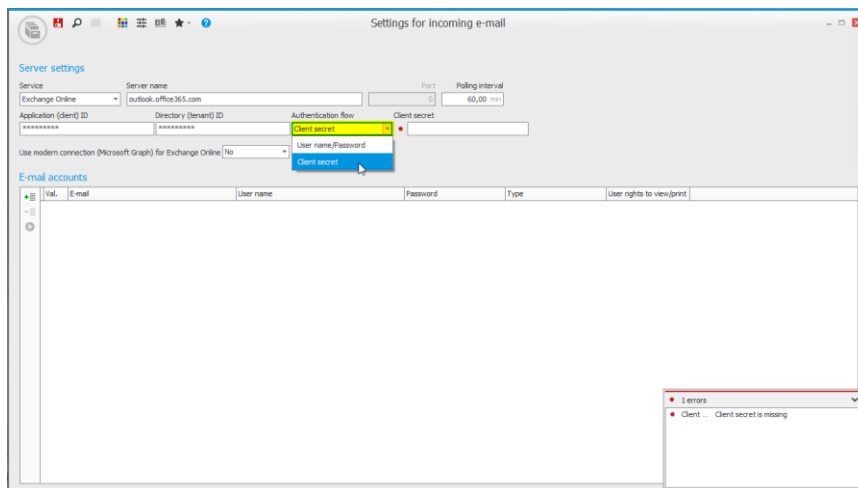
5. Enter the Application (client) ID.



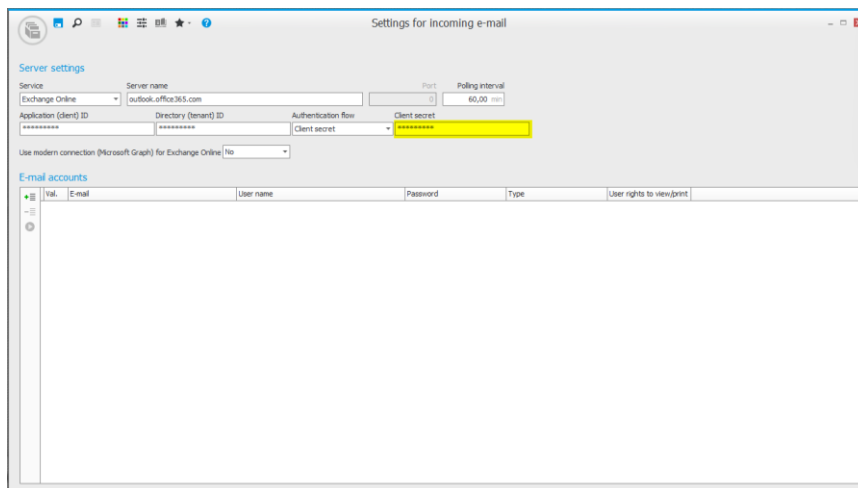
6. Enter the Directory (tenant) ID.



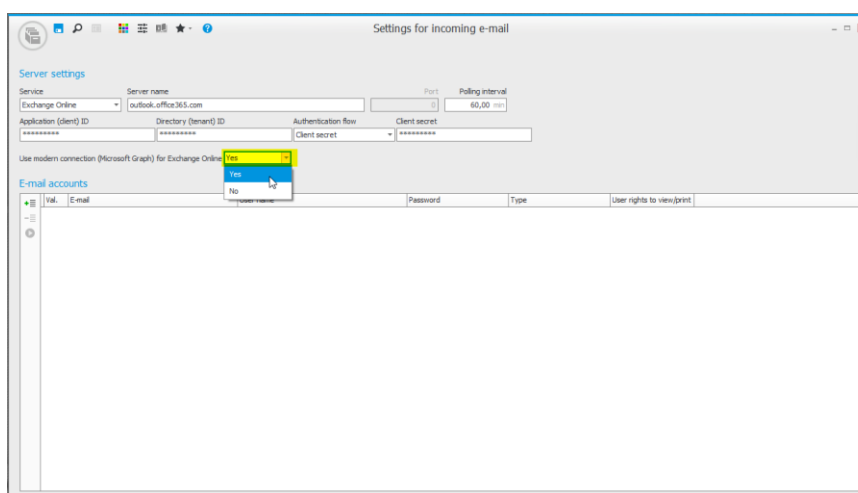
7. "Authentication flow" should be set to "Client secret".



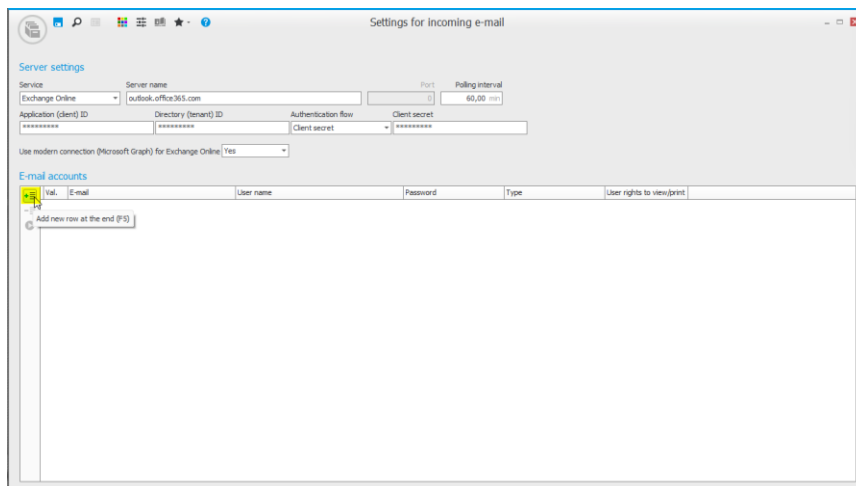
8. Enter the client secret.



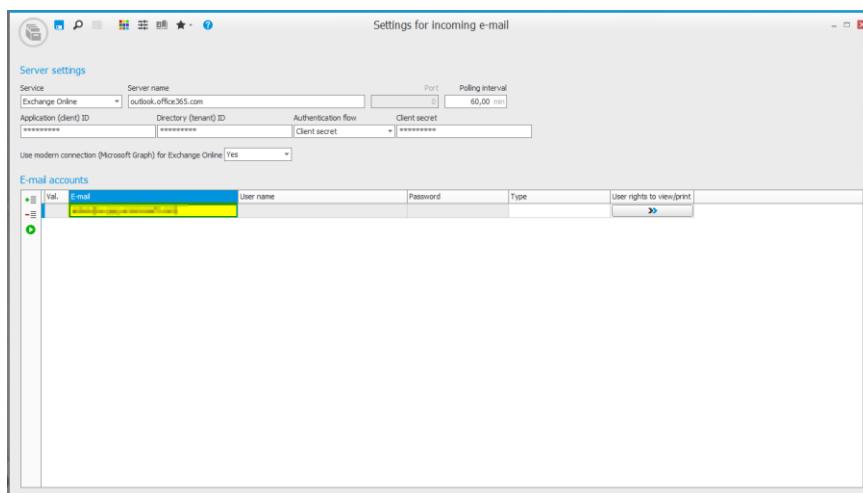
9. In "Use modern connection (Microsoft Graph) for Exchange Online", select "Yes".



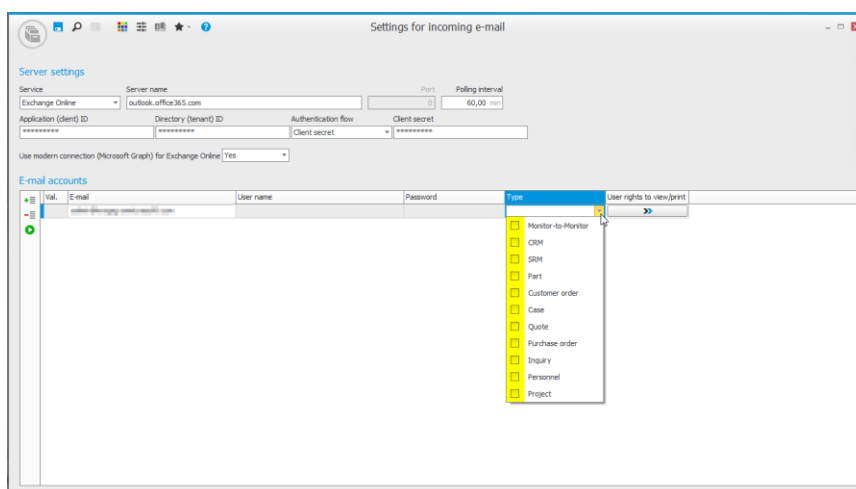
10. Add an e-mail account by pressing the plus icon or F5 on your keyboard.



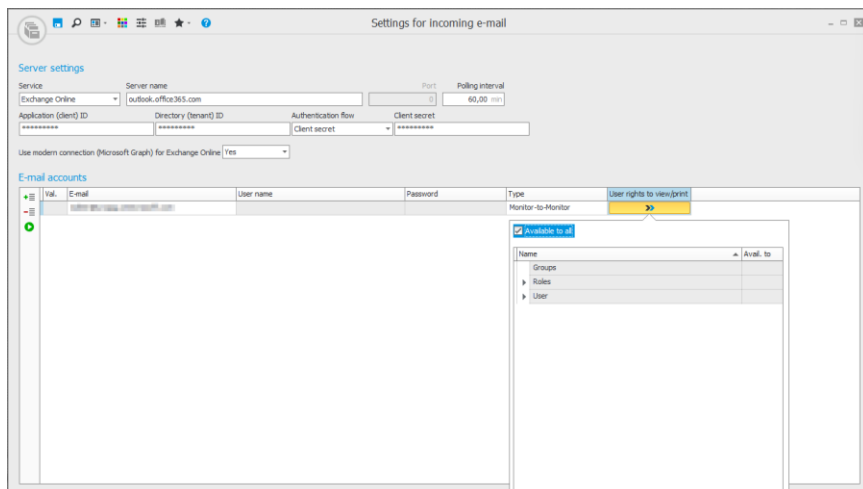
11. Enter the e-mail address.



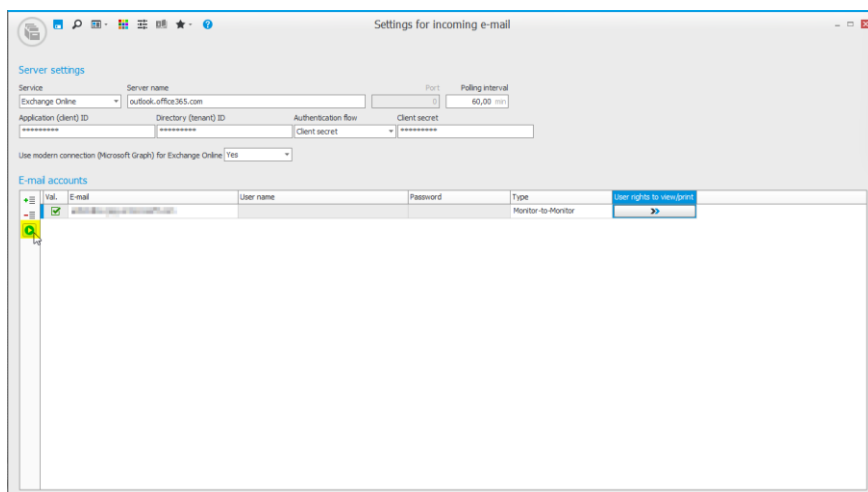
12. Select all "Types" that apply to your configuration of Monitor ERP, for example "Monitor-to-Monitor".



13. Click on “User rights to view/print” and set your preferred permissions (“Available to all” by default).



14. Press the green icon to validate the selected address.



15. Press “Save” then close the procedure.

