

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)	13
Settings for incoming e-mail (Client secret method)	18

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

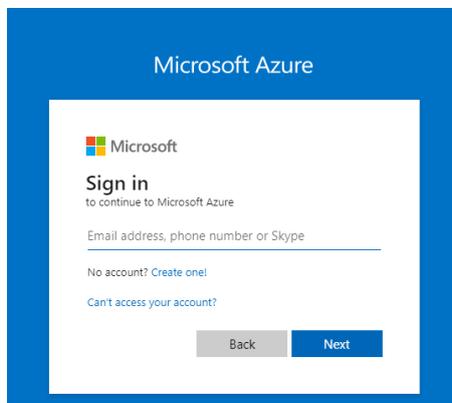
Microsoft Azure setup

Please note: Microsoft currently provides two administrative portals:

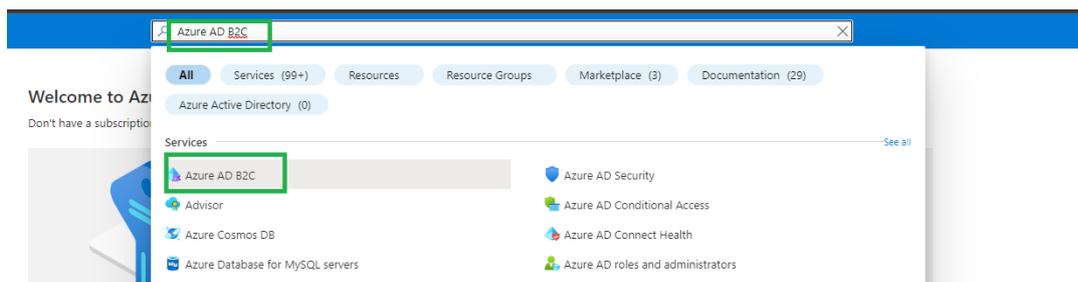
- portal.azure.com
- entra.microsoft.com

The guide below describes the setup process in Microsoft Azure.

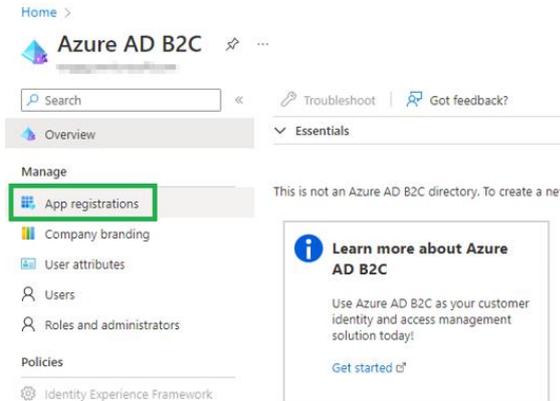
1. Sign in with an existing account at <https://portal.azure.com>.



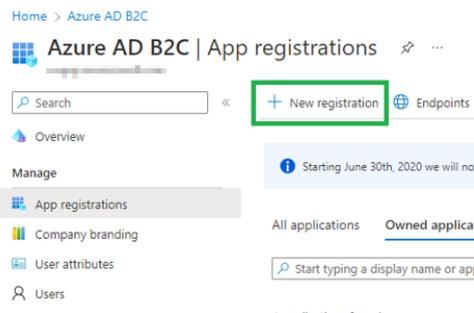
2. Once signed in, search for and access "Azure AD B2C".



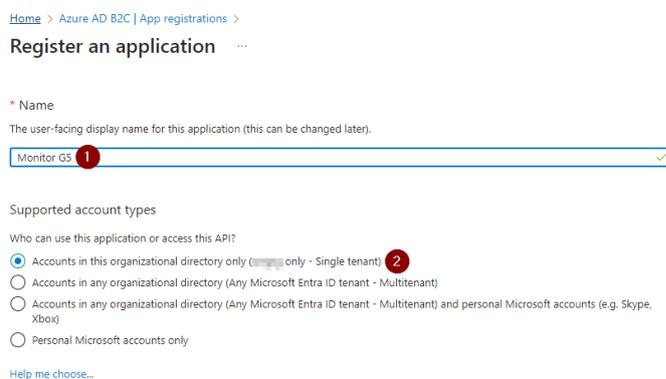
3. Click on "App registrations".



4. Click on "New registration".



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



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).

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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.

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](#)

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).

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

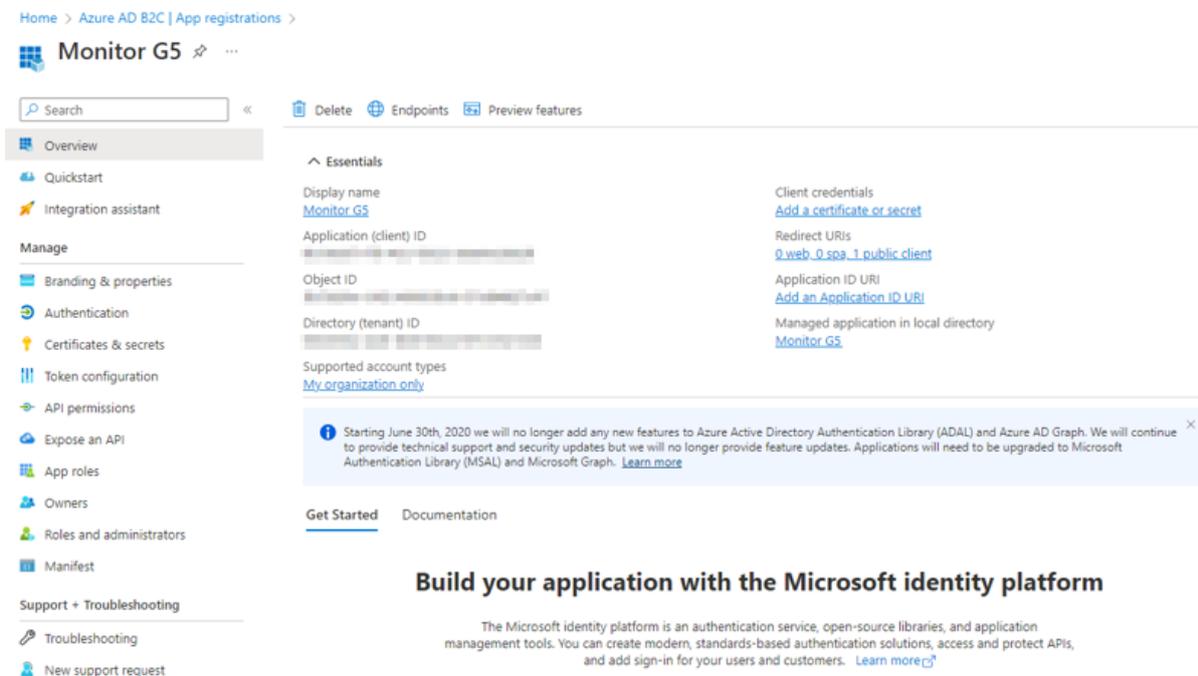
Redirect URI (optional)

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.

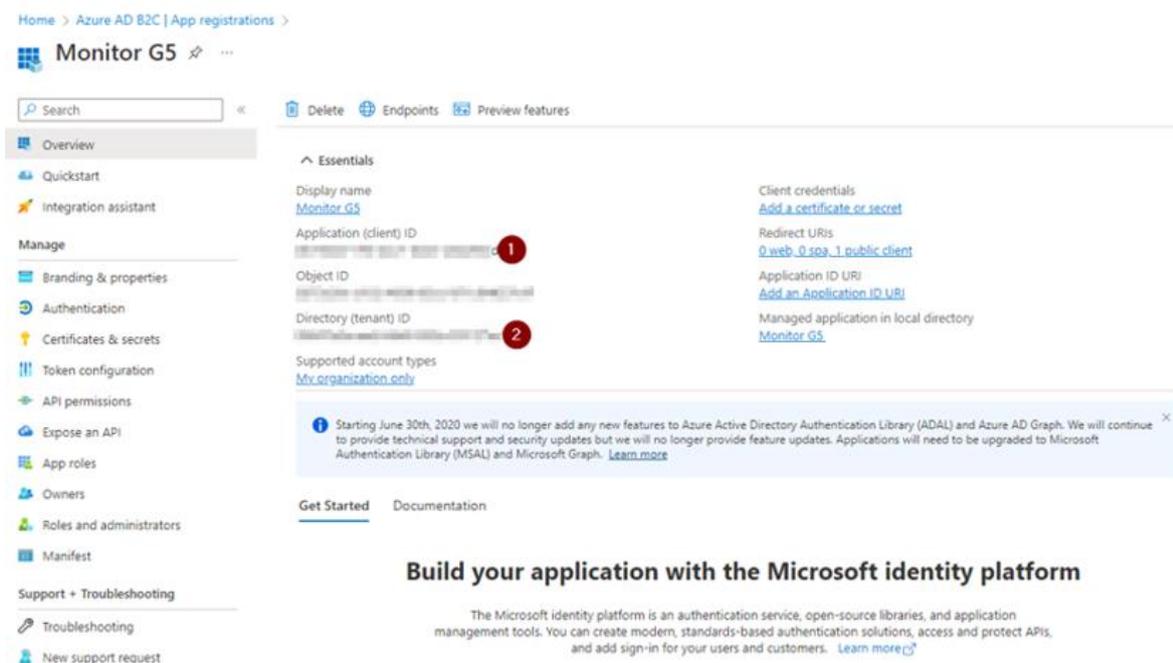
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

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



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



10. Click on "Manifest" in the left-hand menu.

Home > Azure AD B2C | App registrations >

Monitor G5

Search

Delete Endpoints Preview features

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest**
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Essentials

Display name	Client credentials
Monitor G5	Add a certificate or secret
Application (client) ID	Redirect URIs
00000000-0000-0000-0000-000000000000	0 web, 0 spa, 1 public client
Object ID	Application ID URI
00000000-0000-0000-0000-000000000000	Add an Application ID URI
Directory (tenant) ID	Managed application in local directory
00000000-0000-0000-0000-000000000000	Monitor G5
Supported account types	
My organization only	

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#) [Documentation](#)

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

11. We need to add the authentication method to our manifest, this can be done by copying and pasting the code found under the section "Configure for app-only authentication" in the documentation from Microsoft.

Refer to – <https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-authenticate-an-ews-application-by-using-oauth#configure-for-app-only-authentication>

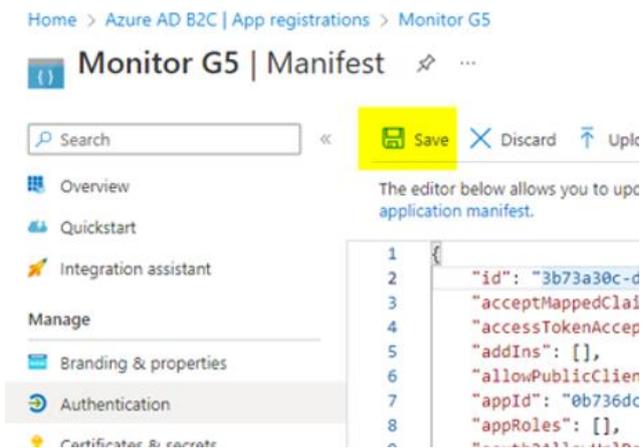
For example, copy and add the [app-only authentication code](#) to the "Manifest" then save.

```

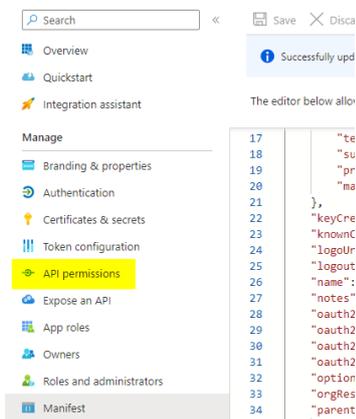
    ],
    "requiredResourceAccess": [
      {
        "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
        "resourceAccess": [
          {
            "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
            "type": "Role"
          }
        ]
      },
      {
        "resourceAppId": "00000003-0000-0000-c000-000000000000",
        "resourceAccess": [
          {
            "id": "e1fe6dd8-ba31-4d61-89e7-88639da4683d",
            "type": "Scope"
          }
        ]
      }
    ]
  },
],

```

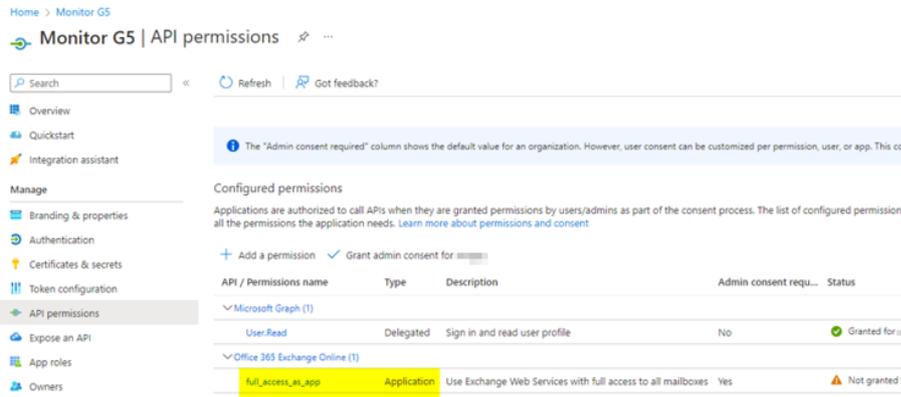
12. Save the "Manifest" settings.



13. Click on "API permissions" in the left-hand menu.

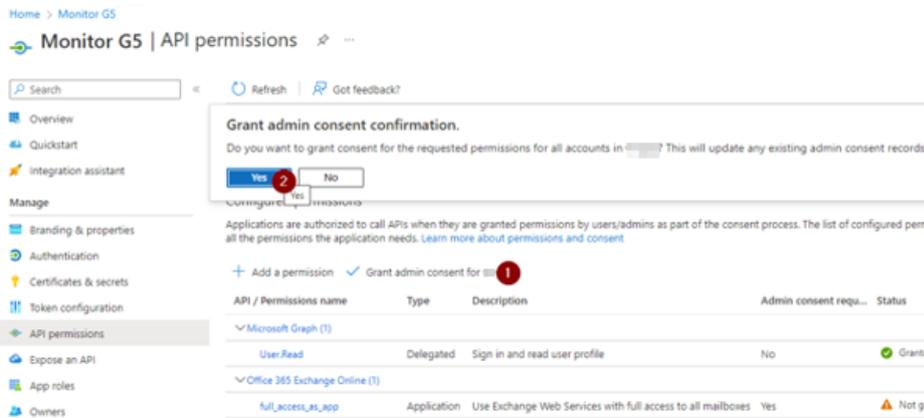


14. Confirm that the permissions have been added (**full_access_as_app**, Type: **Application**).



15. Grant admin consent.

Monitor ERP **requires full access** to Exchange Web Services, additional security settings can be applied to adapt the level of security.



16. Verify that the icon is green.

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 permission 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 requ...	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for v
▼ Office 365 Exchange Online (1)				
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes	Yes	✔ Granted for v

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 th

Configured permissions

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

+ 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?

Integration assistant

Manage

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

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

Advanced settings

Allow public client flows

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

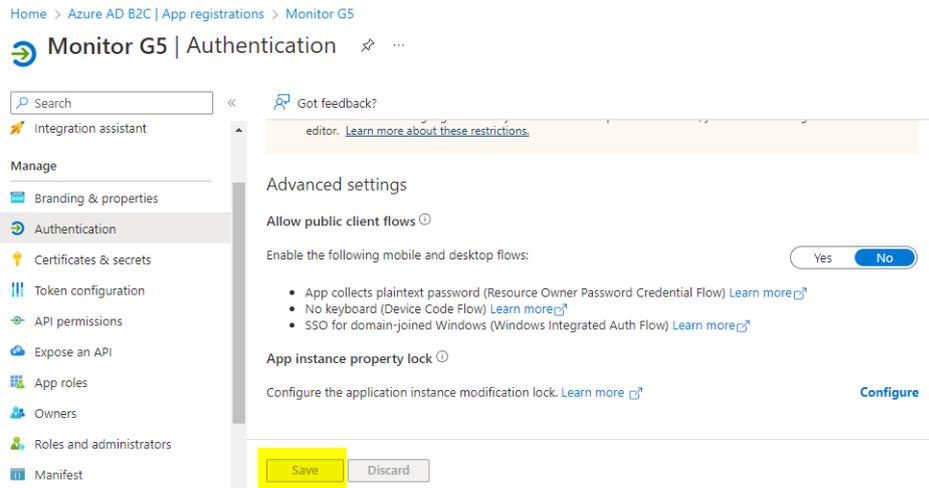
- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock

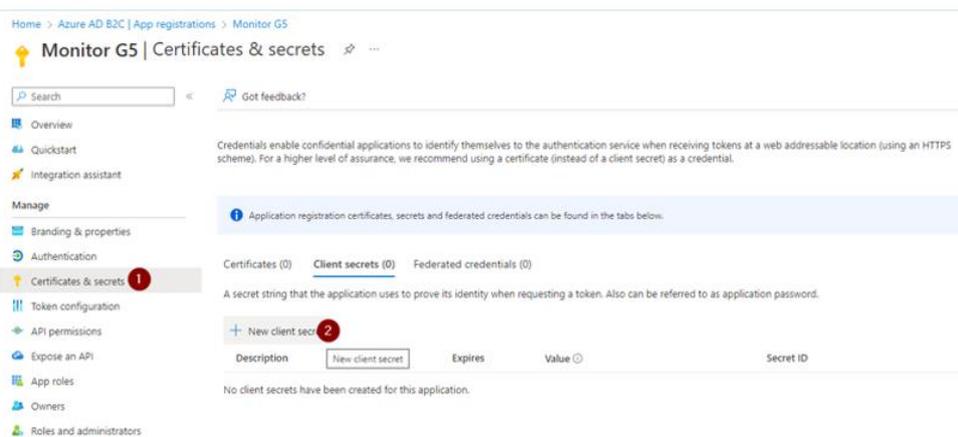
Configure the application instance modification lock. [Learn more](#) **Configure**

Save Discard

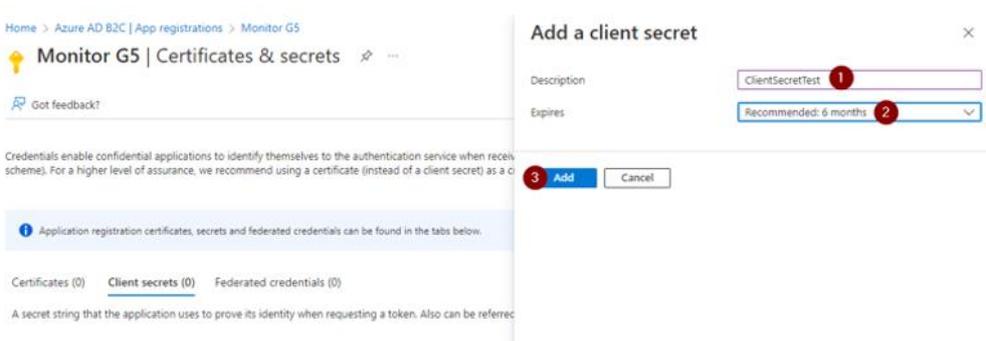
19. Save the settings.



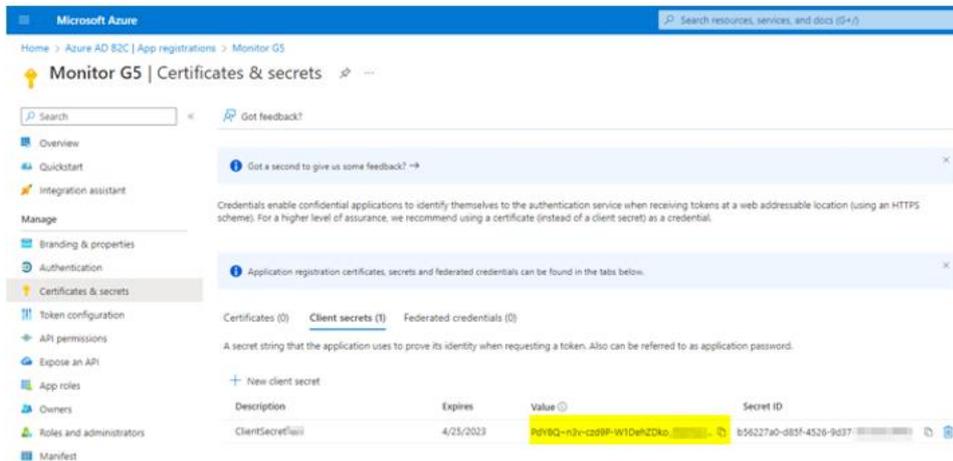
20. Access “Certificates & secrets” in the left-hand menu and click on “New client secret”.



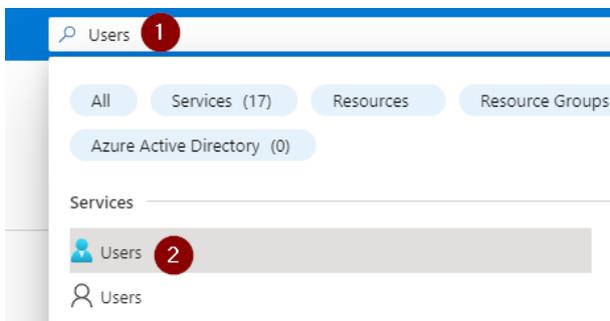
21. Enter a name and set a preferred client secret expiration, then click “Add”.



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.

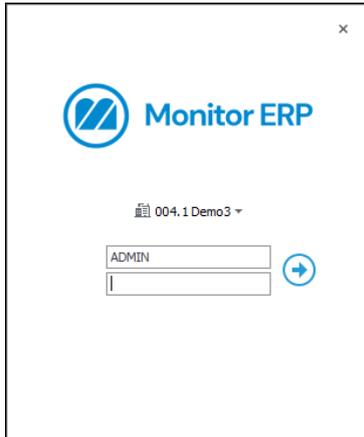


23. Go to “Users”, copy an existing e-mail address, then test it in the Monitor ERP client according to the next part.

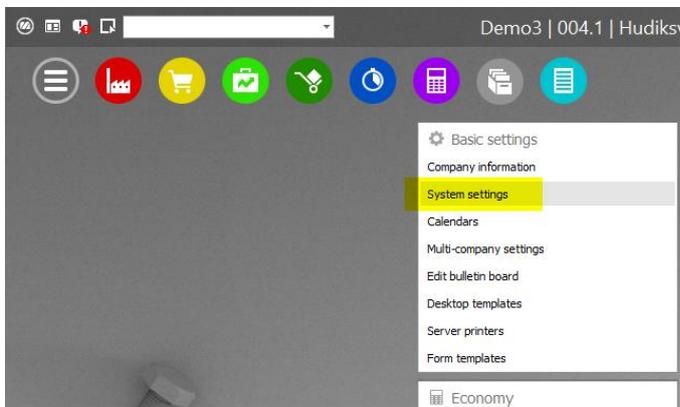


Monitor ERP setup (Client secret method)

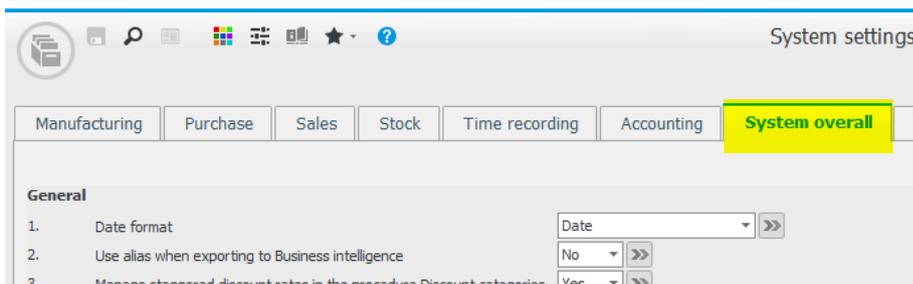
1. Start the Monitor ERP client and sign in with the appropriate admin account.



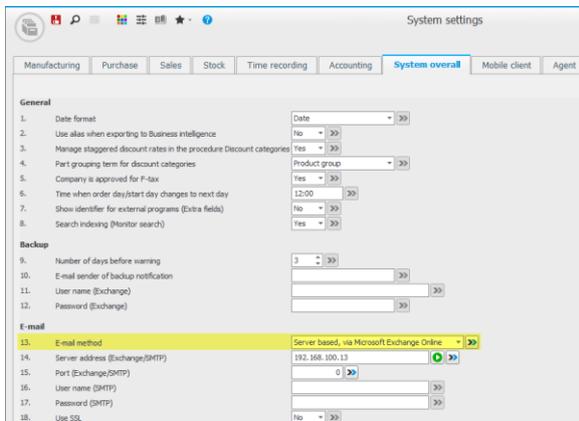
2. Access the "System settings" procedure.



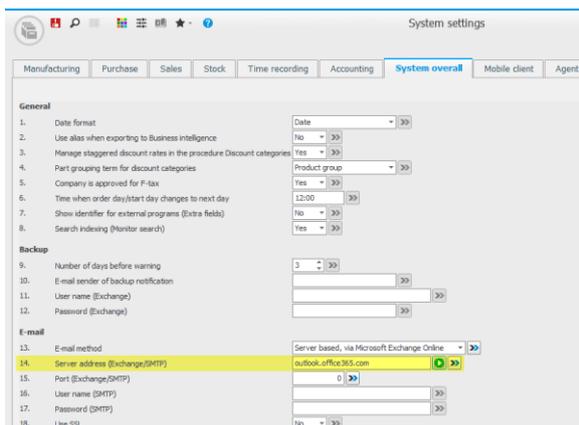
3. Click on the "System overall" tab.



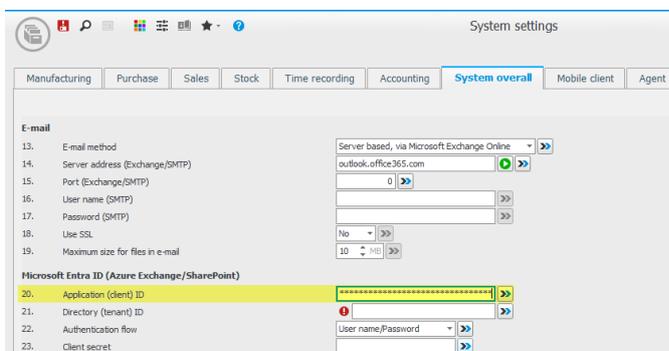
4. In "E-mail method" select "Server based, via Microsoft Exchange Online".



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



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



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

The screenshot shows the 'System settings' window with the 'System overall' tab selected. Under the 'Microsoft Entra ID (Azure Exchange/SharePoint)' section, field 21 'Directory (tenant) ID' is highlighted in yellow. It contains a red error icon and a masked value. Other fields include 'Application (client) ID', 'Authentication flow', and 'Client secret'.

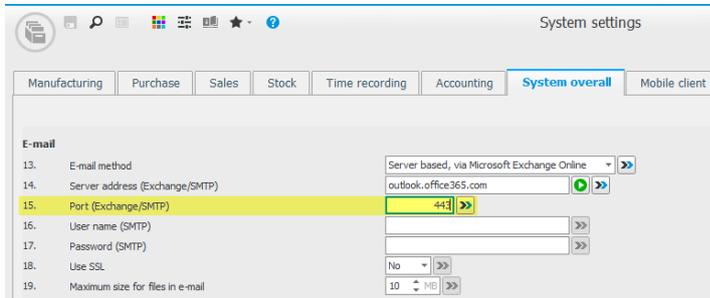
8. In "Authentication flow" select "Client secret".

The screenshot shows the 'System settings' window with the 'System overall' tab selected. Under the 'Microsoft Entra ID (Azure Exchange/SharePoint)' section, field 22 'Authentication flow' is highlighted in yellow and set to 'Client secret'. Field 21 'Directory (tenant) ID' is also highlighted in yellow and contains a red error icon and a masked value.

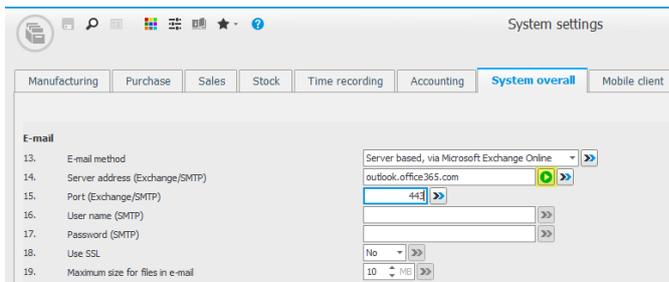
9. Paste the Client secret previously saved from Microsoft Azure in the corresponding field.

The screenshot shows the 'System settings' window with the 'System overall' tab selected. Under the 'Microsoft Entra ID (Azure Exchange/SharePoint)' section, field 23 'Client secret' is highlighted in yellow. It contains a red error icon and a masked value. Field 22 'Authentication flow' is also highlighted in yellow and set to 'Client secret'.

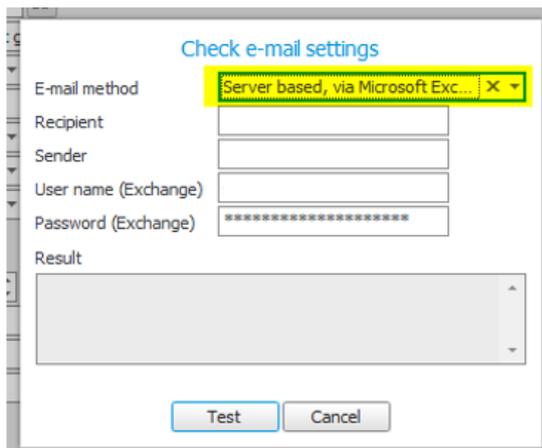
10. The port can be set, for more information refer to <https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>.



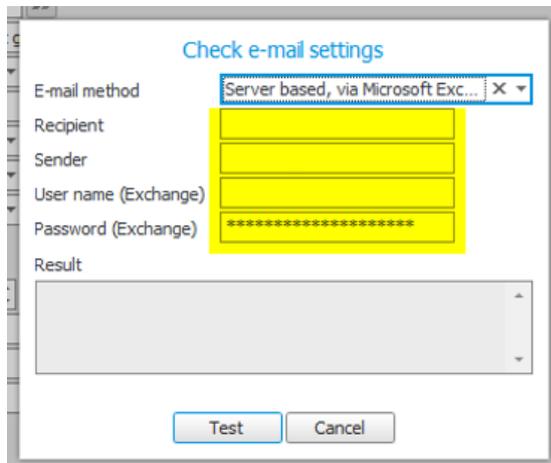
11. Click on the green icon next to the server address to test the settings.



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



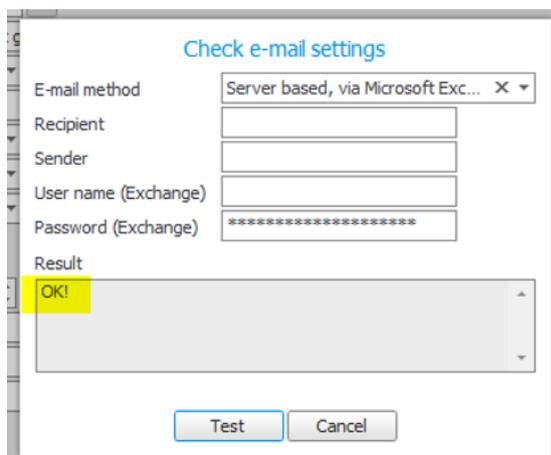
13. Enter a valid recipient, sender, user name and password.



The screenshot shows a dialog box titled "Check e-mail settings". It contains the following fields and controls:

- E-mail method:** A dropdown menu showing "Server based, via Microsoft Exc..." with a close button (X).
- Recipient:** A text input field highlighted in yellow.
- Sender:** A text input field highlighted in yellow.
- User name (Exchange):** A text input field highlighted in yellow.
- Password (Exchange):** A text input field containing asterisks, highlighted in yellow.
- Result:** A large text area for displaying the test outcome.
- Buttons:** "Test" and "Cancel" buttons at the bottom.

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



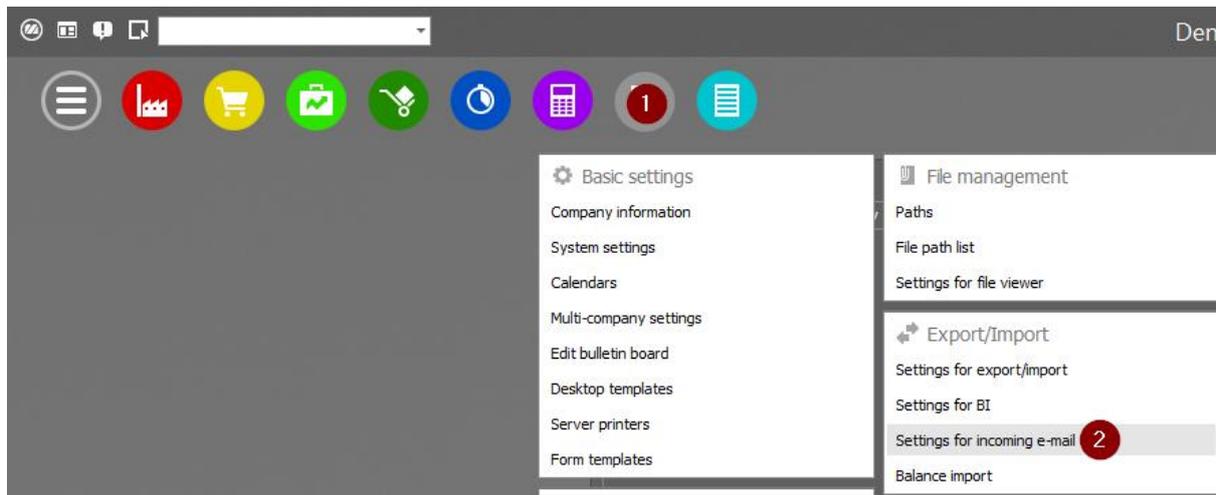
The screenshot shows the same "Check e-mail settings" dialog box as in the previous image, but with the following changes:

- The "Recipient", "Sender", "User name (Exchange)", and "Password (Exchange)" fields are now empty.
- The "Result" field now displays "OK!" in a yellow highlight.
- The "Test" button is highlighted in blue, indicating it was just pressed.

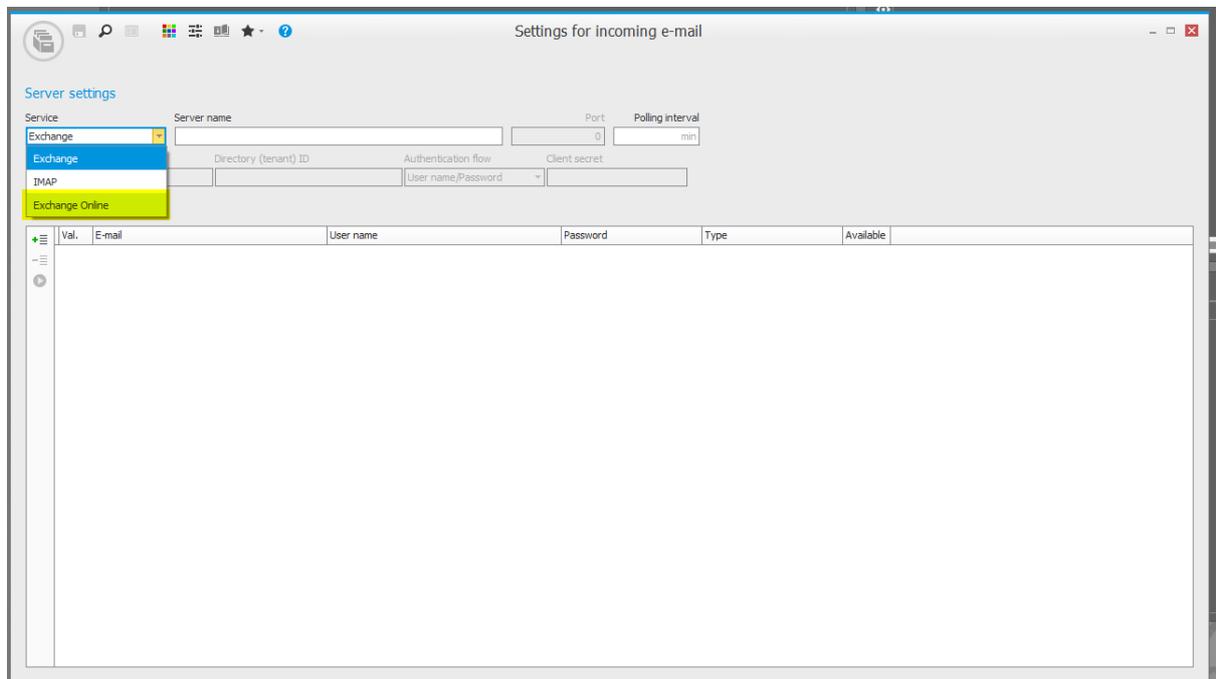
(Please note: If the service has been set up recently you may receive a **403 Forbidden message** due to delays when updating a tenant in Microsoft Azure portal. In this case, wait a moment then press "Test" again. If you encounter other messages in the "Result" box, please refer to the online documentation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

Settings for incoming e-mail (Client secret method)

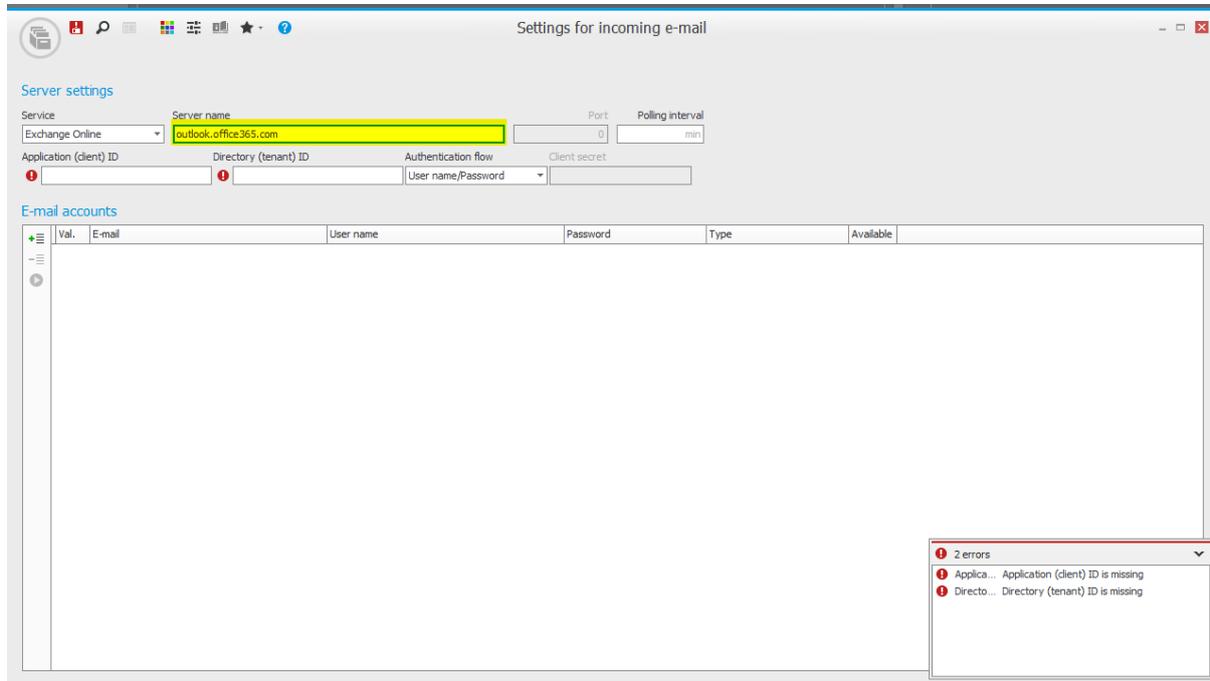
1. Access the "Settings for incoming e-mail" procedure.



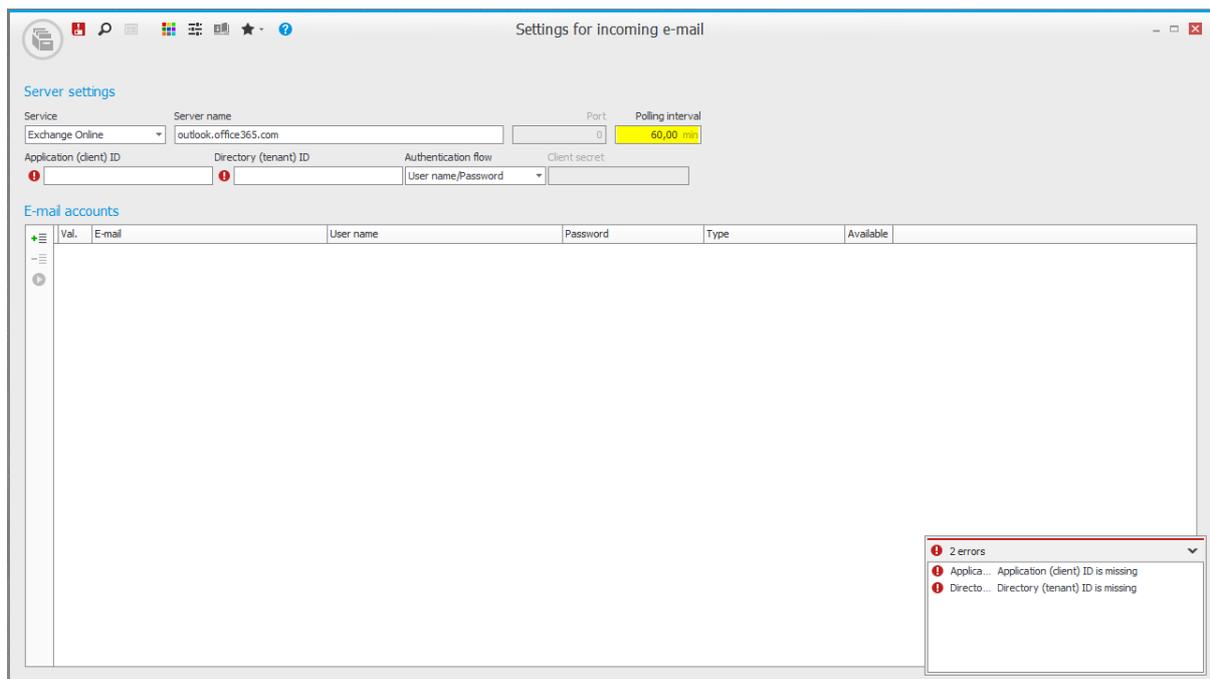
2. Under "Service" select "Exchange Online".



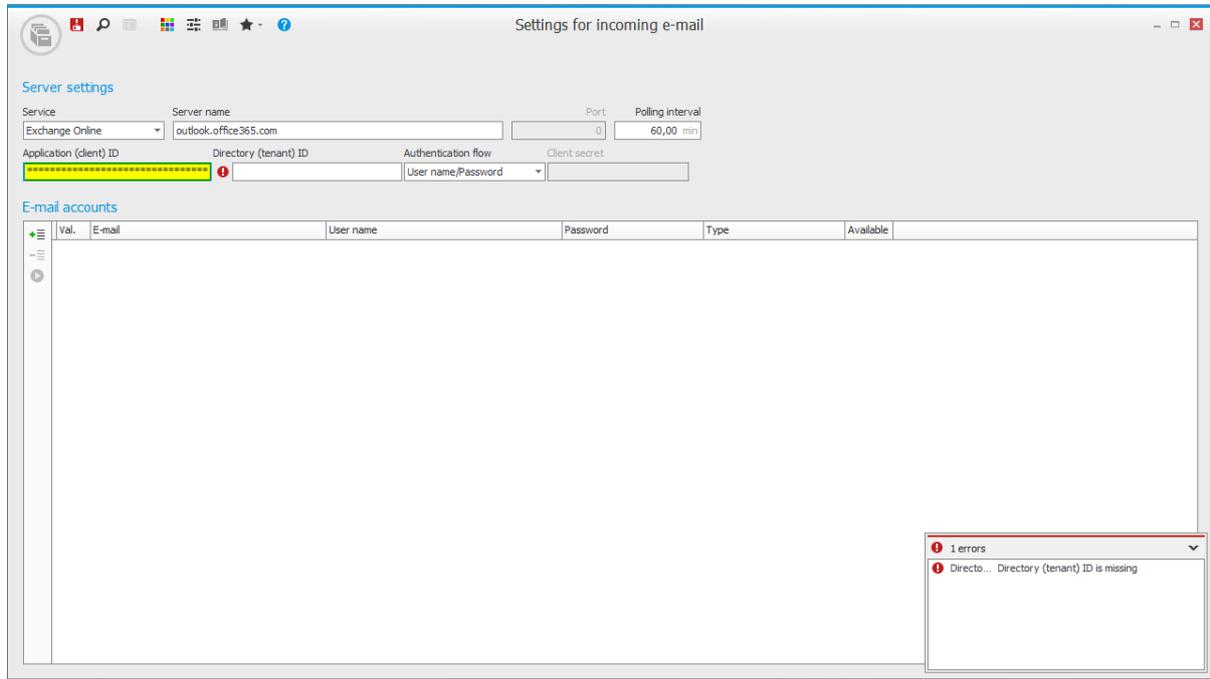
3. Enter the URL to the server – for example outlook.office365.com.



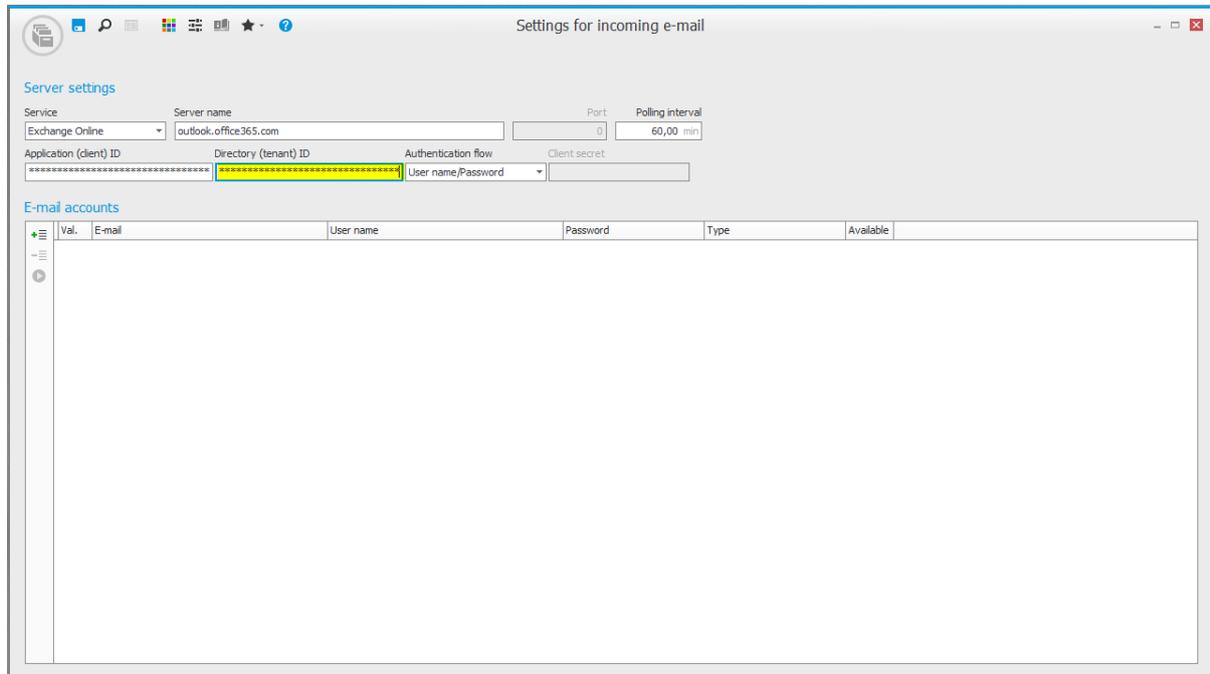
4. Set a pooling interval (in minutes) according to your requirements, in our example we set this to 60,00 to check for new e-mails on the server once every hour.



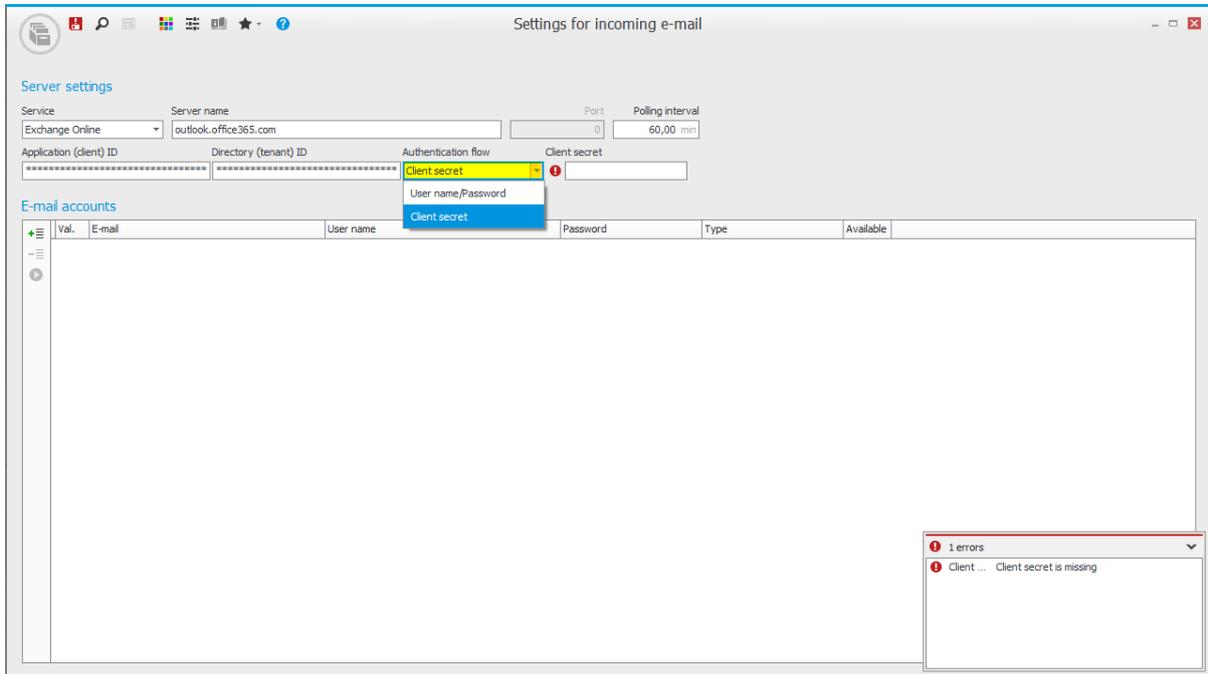
5. Enter the Application (client) ID.



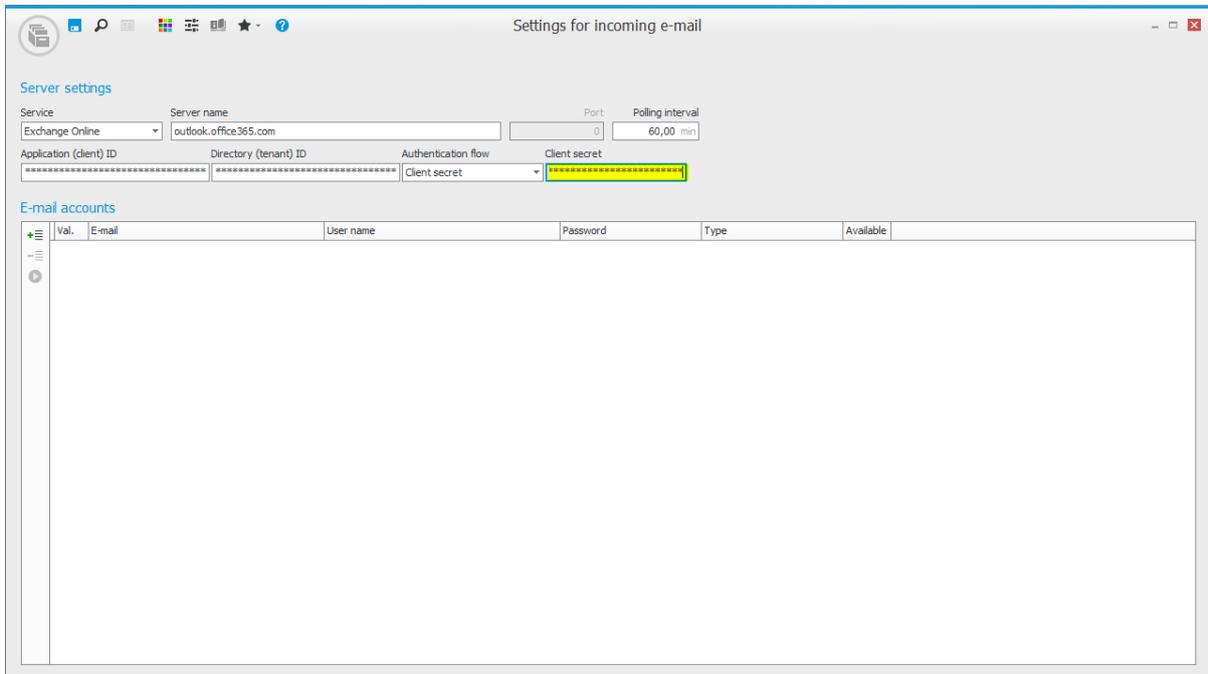
6. Enter the Directory (tenant) ID.



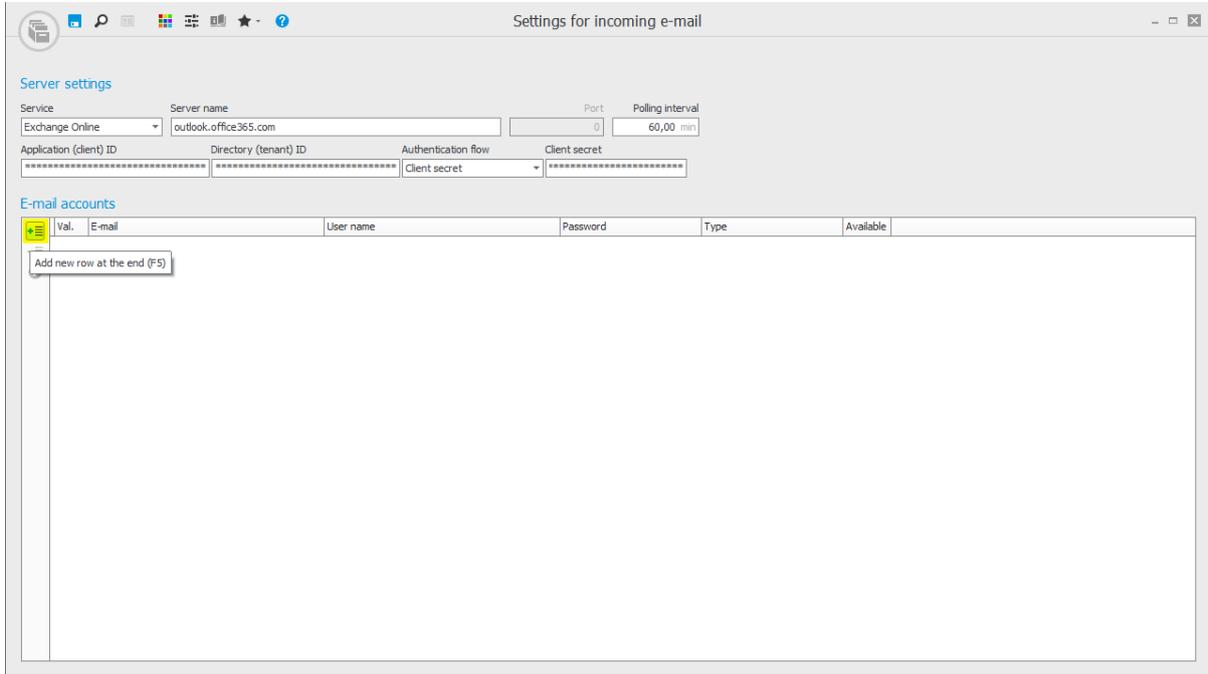
7. "Authentication flow" should be set to "Client secret".



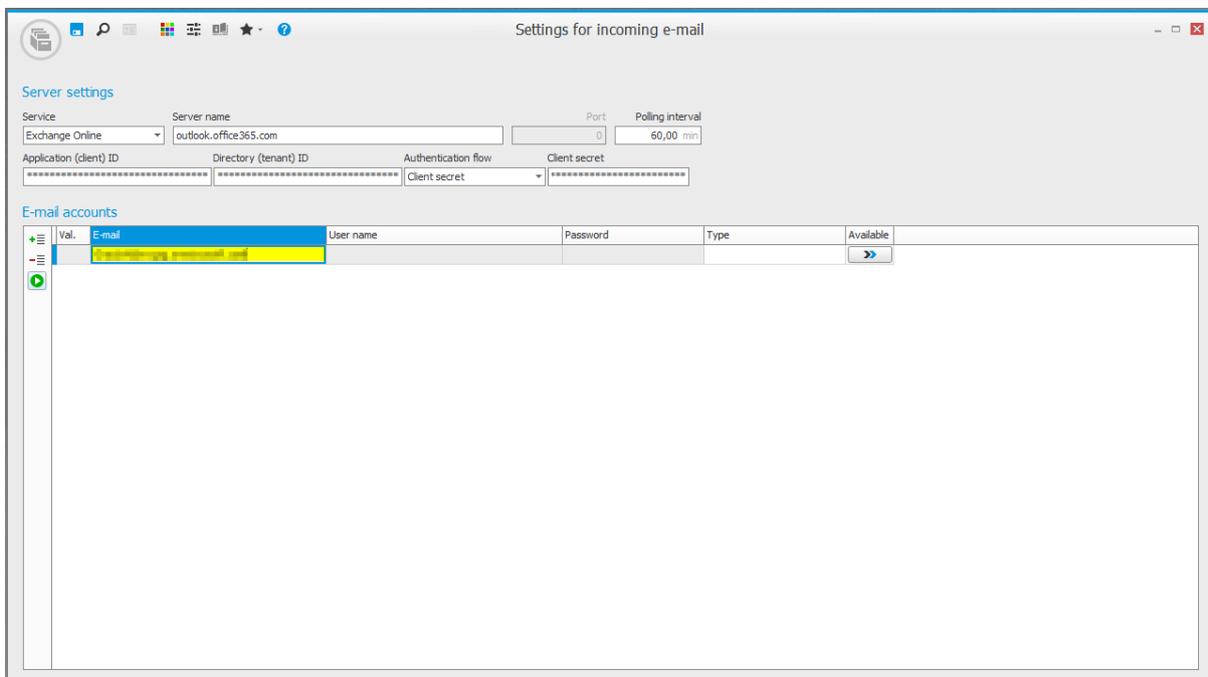
8. Enter the client secret.



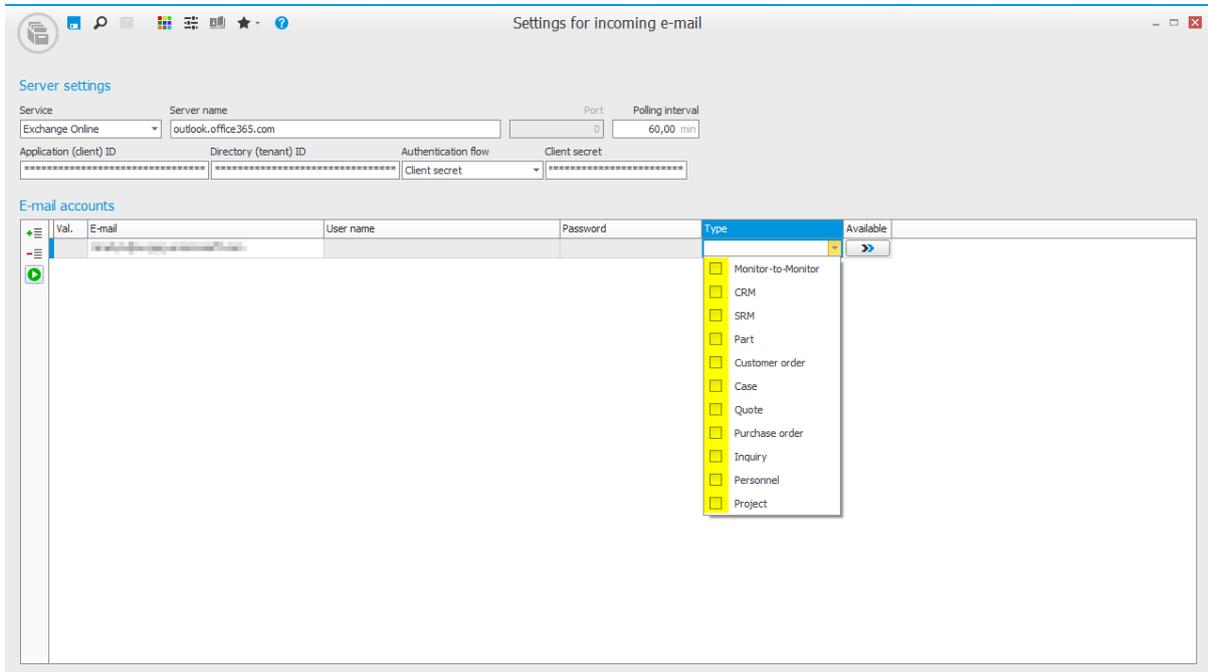
9. Add an e-mail account by pressing the plus icon or F5 on your keyboard.



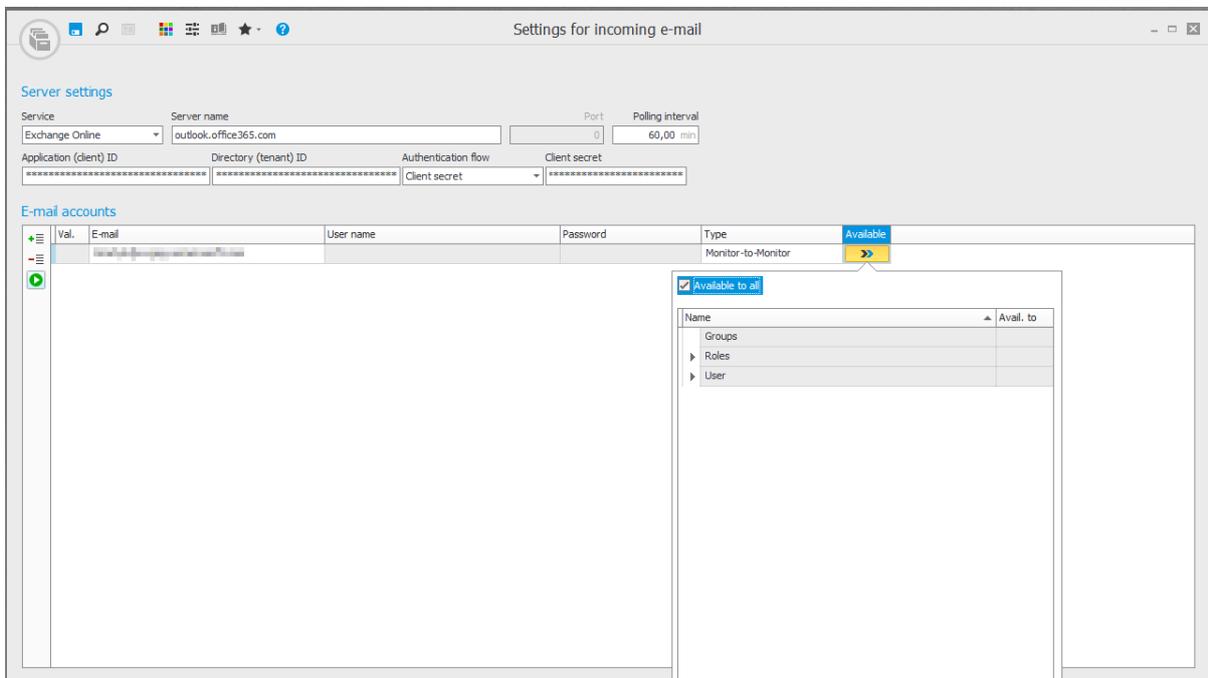
10. Enter the e-mail address.



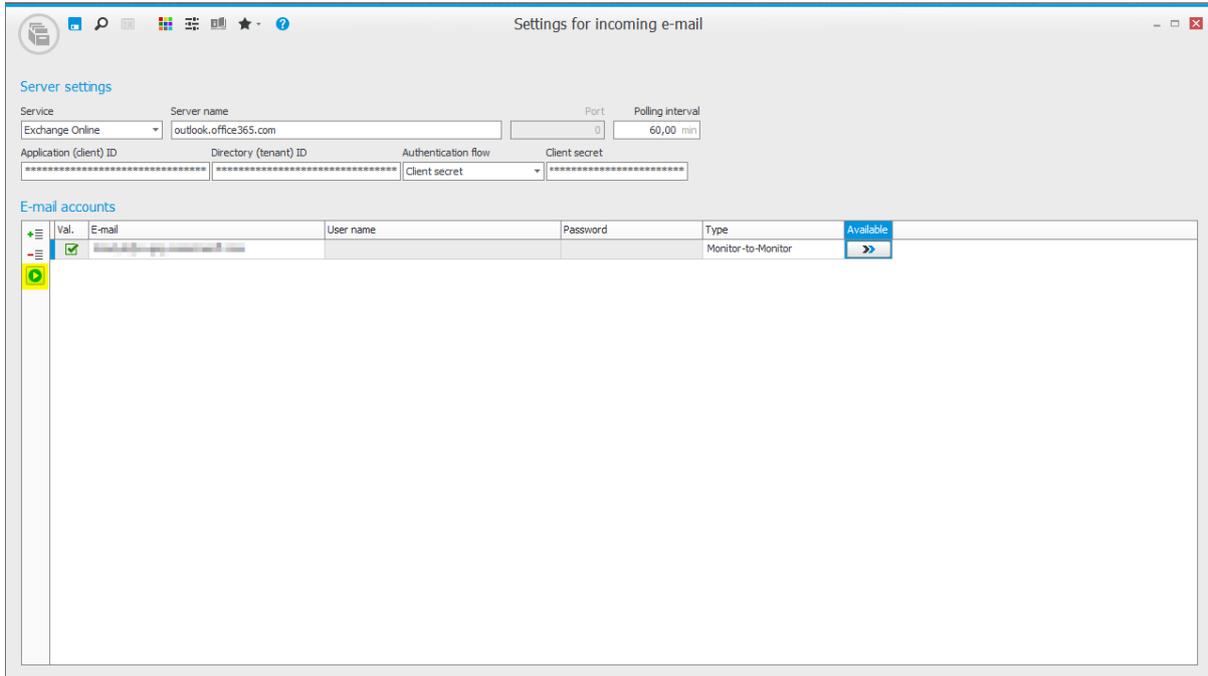
11. Select all "Types" that apply to your configuration of Monitor ERP, for example "Monitor-to-Monitor".



12. Click on "Available" and set your preferred permissions ("Available to all" by default).



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



14. Press "Save" then close the procedure.

