

# Office 365 OAuth2 (konfigurace pro odesílání e-mailů přes Office365)

## Konfigurace SW AktionNEXT pro odesílání emailů přes Office365 (Azure AD)

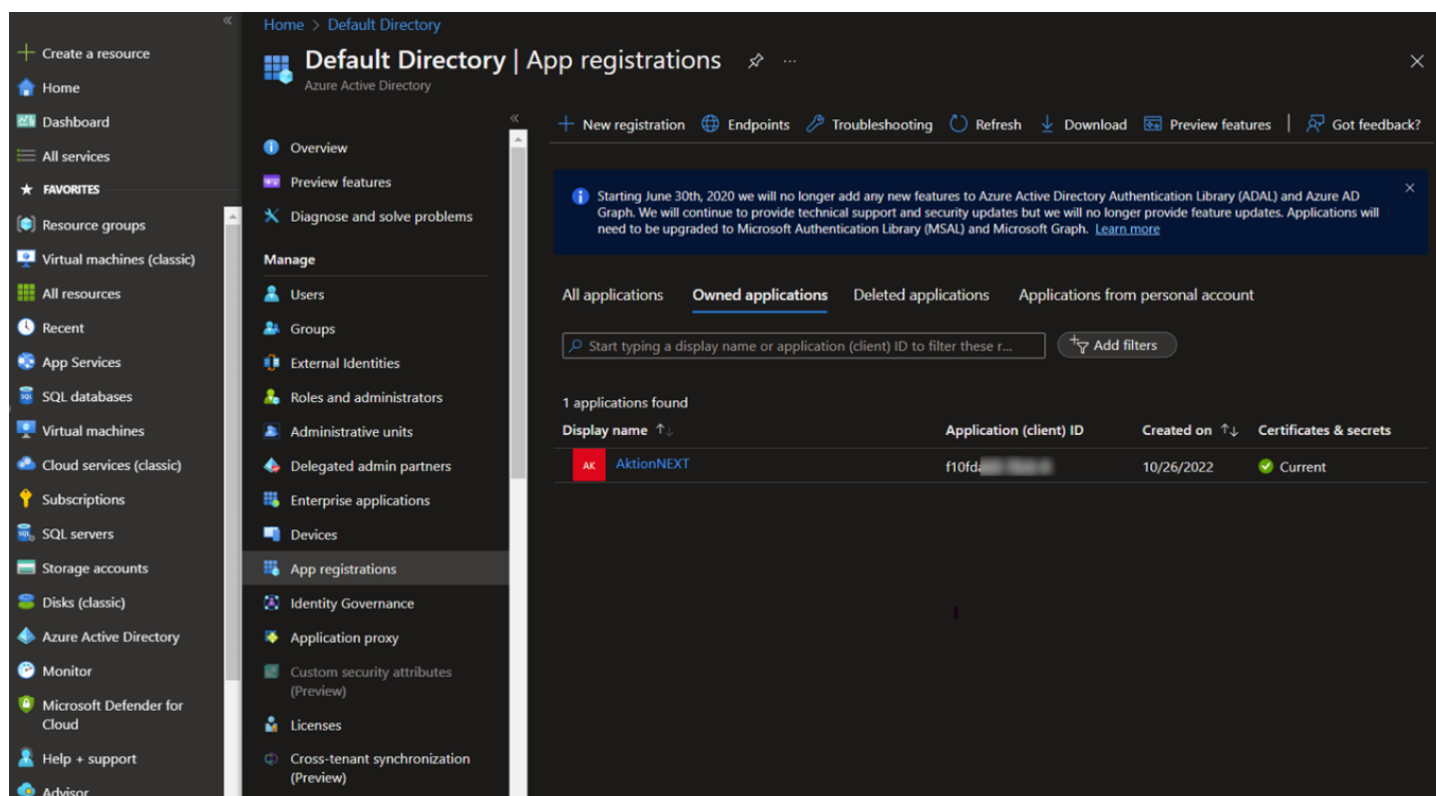
Ujistěte se, že máte k dispozici účet AzureAD, ke kterému se můžete přihlásit.

1. Přihlaste se k účtu Microsoft Azure v roli uživatele – administrátora.

- Otevře se domovská obrazovka **Microsoft Azure**.

2. Vytvoření nové aplikace:

- Vyhledejte a vyberte službu Azure Active Directory.



- Přejděte do nabídky **Registrace aplikace (App registration) > Nová registrace (New registration)**.

## Register an application

### \* Name

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

vcd 

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Velocloud Networks, Incit@velo)
- ☐ Accounts in any organizational directory
- ☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[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  e.g. `https://myapp.com/auth`

- V poli **Název (Name)** zadejte název aplikace AktionNEXT.
- K vytvoření tajného klíče klienta pro aplikaci AktionNEXT klikněte na kartě **Vlastněné aplikace (Owned applications)** na vaši aplikaci AktionNEXT.
- Přejděte do nabídky Certifikáty a tajné klíče (**Certificates & secrets**) > **Nový tajný klíč klienta (New client secret)**. **Otevře se obrazovka Přidání tajného klíče klienta (Add a client secret)**.

### VCO - Certificates & secrets

Overview

Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets**
- API permissions
- Expose an API
- Owners
- Manifest

Support + Troubleshooting

- Troubleshooting

#### Add a client secret

Description

Expires

☒ In 1 year  
☐ In 2 years  
☐ Never

#### Client secrets

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

| DESCRIPTION | EXPIRES | VALUE |
|-------------|---------|-------|
|-------------|---------|-------|

- Zadejte podrobnosti tajného klíče, jako je popis a vypršení jeho platnosti, a klikněte na tlačítko **Přidat (Add)**. Pro aplikaci se vytvoří tajný klíč klienta. Poznamenejte si nový tajný klíč klienta, který budete potřebovat během konfigurace jednotného přihlašování v aplikaci AktionNEXT.
- Při konfiguraci oprávnění vaší aplikace AktionNEXT klikněte na aplikaci AktionNEXT a přejděte do nabídky **Oprávnění API (API permissions) > Přidat oprávnění (Add a permission)**. Otevře se obrazovka **Vyžádání oprávnění API (Request API permissions)**.

Home > Velocloud Networks, Incit@velo - App registrations > VCO - API permissions

### VCO - API permissions

Overview

Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions**
- Expose an API
- Owners
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

#### API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show grant/deny access.

| API / PERMISSIONS NAME | TYPE      | DESCRIPTION    |
|------------------------|-----------|----------------|
| ▼ Microsoft Graph (1)  |           |                |
| User.Read              | Delegated | Sign in and re |

These are the permissions that this application requests statically. You may also request user able permissions dynamically through code. [See best practices for requesting permissions](#)

#### Grant consent

To consent to permissions that require admin consent, please sign in with an account that is directory.

Grant admin consent for Velocloud Networks, Incit@velo

#### Request API permissions

Select an API

[Microsoft APIs](#)
[APIs my organization uses](#)
[My APIs](#)

#### Commonly used Microsoft APIs

**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Service Management**

Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Dynamics 365 Business Central**

Programmatic access to data and functionality in Dynamics 365 Business Central

**Intune**

Programmatic access to Intune data

**Office 365 Management APIs**

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

**OneNote**

Create and manage notes, lists, pictures, files, and more in OneNote notebooks

**Power BI Service**

Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

**SharePoint**

Interact remotely with SharePoint data

**Skype for Business**

Integrate real-time presence, secure messaging, calling, and conference capabilities

- Klikněte na možnost **Microsoft Graph** a jako typ oprávnění pro vaši aplikaci vyberte možnost **Oprávnění aplikace (Application permissions)**. V části **Vybrat oprávnění (Select permissions)** v rozevírací nabídce zaškrtnout **Mail.Send** Klikněte na tlačítko **Přidat oprávnění (Add 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 signed-in user.

Select permissions

| <input type="text" value="Mail."/>                                                |                        |
|-----------------------------------------------------------------------------------|------------------------|
| Permission                                                                        | Admin consent required |
| ✓ Mail (1)                                                                        |                        |
| <input type="checkbox"/> Mail.Read ⓘ<br>Read mail in all mailboxes                | Yes                    |
| <input type="checkbox"/> Mail.ReadBasic ⓘ<br>Read basic mail in all mailboxes     | Yes                    |
| <input type="checkbox"/> Mail.ReadBasic.All ⓘ<br>Read basic mail in all mailboxes | Yes                    |
| <input type="checkbox"/> Mail.ReadWrite ⓘ<br>Read and write mail in all mailboxes | Yes                    |
| <input checked="" type="checkbox"/> Mail.Send ⓘ<br>Send mail as any user          | Yes                    |

### 3. Nastavení oprávnění

## Configured permissions

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

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

| API / Permissions n...                | Type        | Description           | Admin consent req... |
|---------------------------------------|-------------|-----------------------|----------------------|
| ▼ <a href="#">Microsoft Graph (1)</a> |             |                       |                      |
| <a href="#">Mail.Send</a>             | Application | Send mail as any user | Yes                  |

### 4. Nastavení SW AktionNEXT

V aplikaci WinClient, konfigurace aplikace, záložka "Konfigurace systému", nastavte hodnoty pro odesílání, dle získaných údajů z AzureAD. Následně ověřte tlačítkem test funkcionalitu odesílání emailů.

### Konfigurace odesílání emailů

Autentifikace

Office365 OAuth2

Odesílatel:

#### SMTP

Server:

193.1...

Port:

25

Login:
Heslo:

Zabezpečení:

Žá...

☐ Přijímat všechny certifikáty

#### Office365 OAuth2

Directory (Tenant) ID:

Application (Client) ID:

Client secret ID:

Test