

Email setup using Token-based authentication with Microsoft 365

Prerequisites

Before proceeding with the setup, ensure the following:

1. Microsoft 365 Admin Access

- You must have **Global Administrator** or **Application Administrator** rights to:
 - Register an app in **Microsoft Entra ID** (formerly Azure AD).
 - Grant **admin consent** for API permissions.

2. Exchange Online License

- The tenant must, at minimum, have an **active Exchange Online subscription** for sending emails via SMTP.

3. SMTP Authentication Enabled (If Required)

- Modern authentication (OAuth2) is used, but ensure that **SMTP AUTH is not disabled** for the tenant if needed.
 - You can check this in **Microsoft Entra ID** under Security → Authentication Policies.

4. Microsoft Graph API Access

- The **Mail.Send** permission must be enabled in Microsoft Graph API.
- Ensure that admin consent is granted.

5. Service Account (Optional but Recommended)

- It is best practice to create a **dedicated service account** for email sending.
 - This prevents access issues if an employee leaves or credentials change.

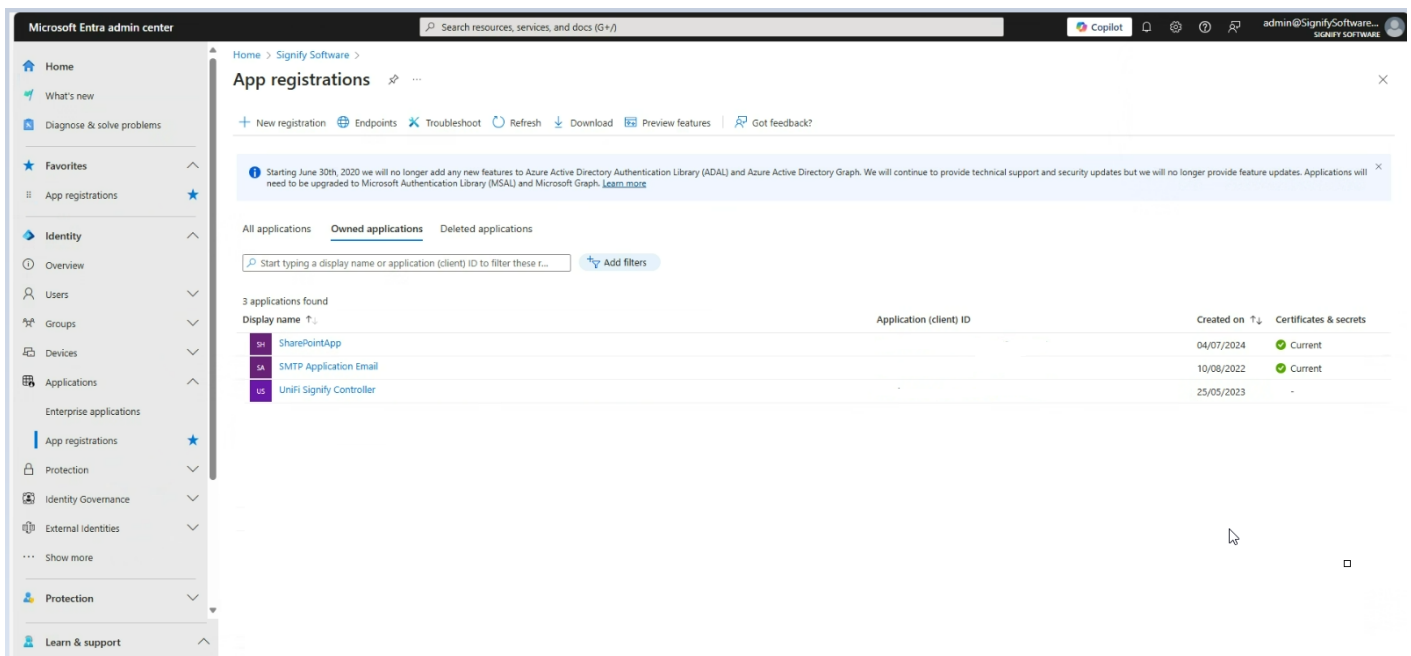
6. Firewall and Network Rules

- Allow outbound traffic on **port 587** (SMTP with STARTTLS).
 - Ensure no outbound filtering that blocks Microsoft's SMTP servers.
-

Microsoft 365 App Registration and Setup

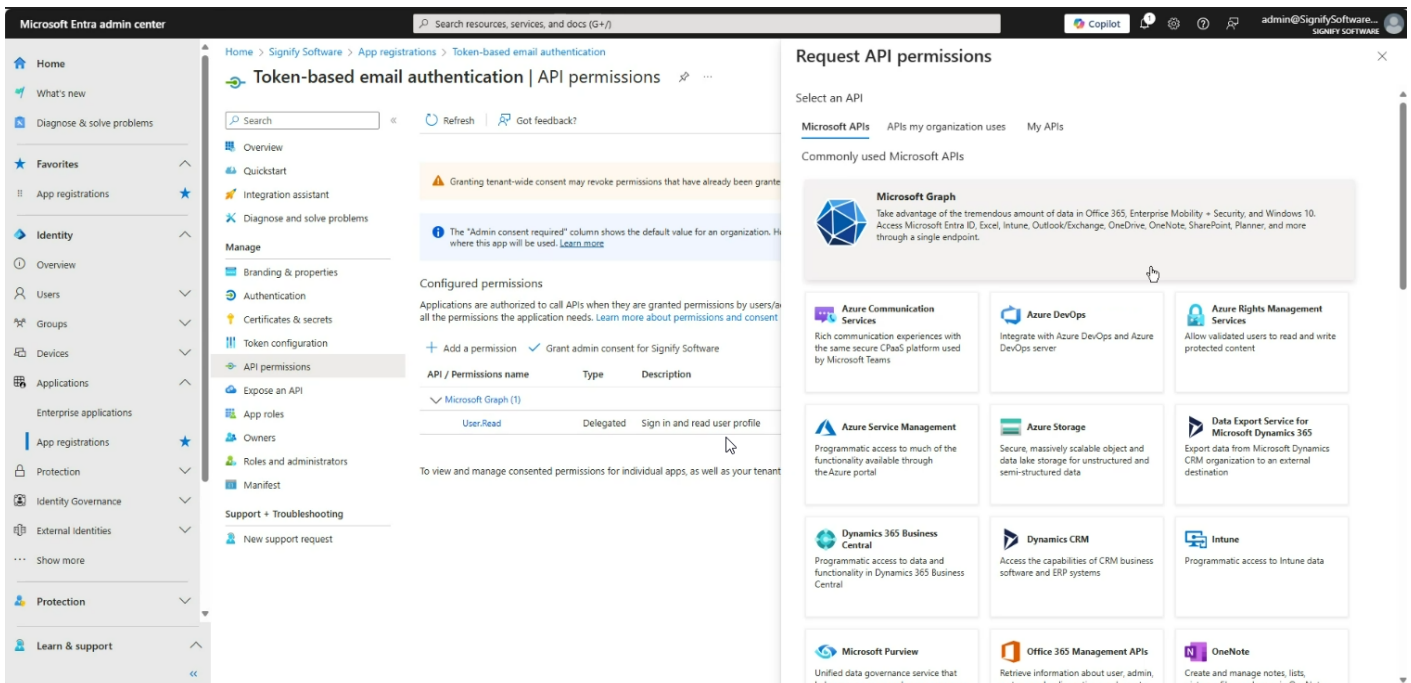
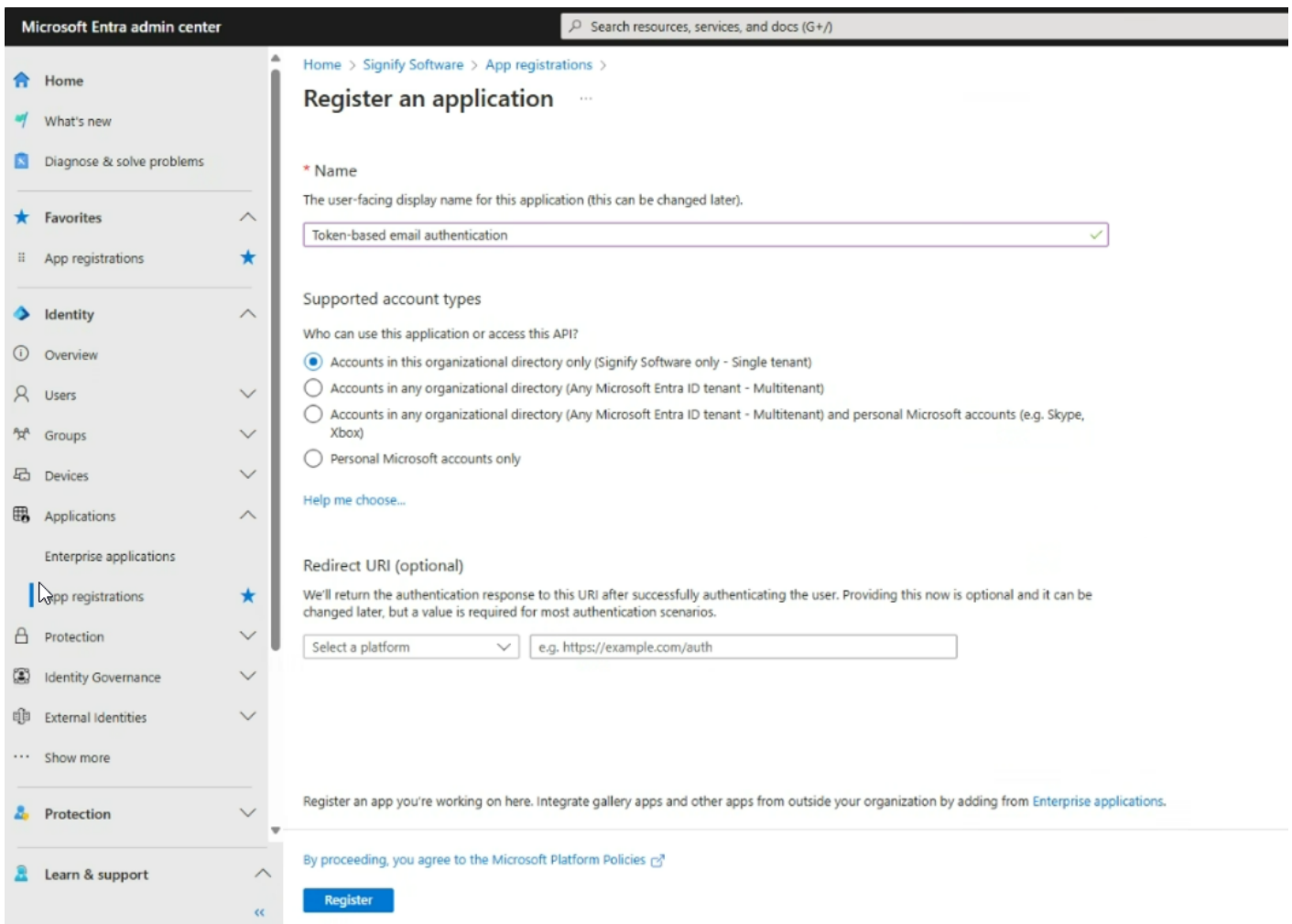
Step 1: Open the Microsoft Entra Admin Portal

1. Navigate to the **Microsoft Entra admin center**.
2. Go to **Applications** → **App Registrations** → **Owned Applications**.



Step 2: Register a New Application

1. Click **New App Registration**.
2. Open the newly created app registration.
3. Navigate to **API Permissions** in the menu.



Step 3: Configure API Permissions

1. If an SMTP exchange does not exist, set up a new one.
2. Click **Add a Permission**.

3. Select **Microsoft Graph** → **Application Permissions**.
4. Search for **Mail.Send** and select it.
5. Click **Add Permission**.

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.

Select permissions

[expand all](#)

| Permission | Admin consent required |
|--|------------------------|
| Mail (1) | |
| <input checked="" type="checkbox"/> Mail.Send ⓘ Send mail as any user | Yes |

Add permissions

Discard

Step 4: Grant Admin Consent

1. Under **API Permissions**, locate the **Mail.Send** permission.

2. Click **Grant Admin Consent**.

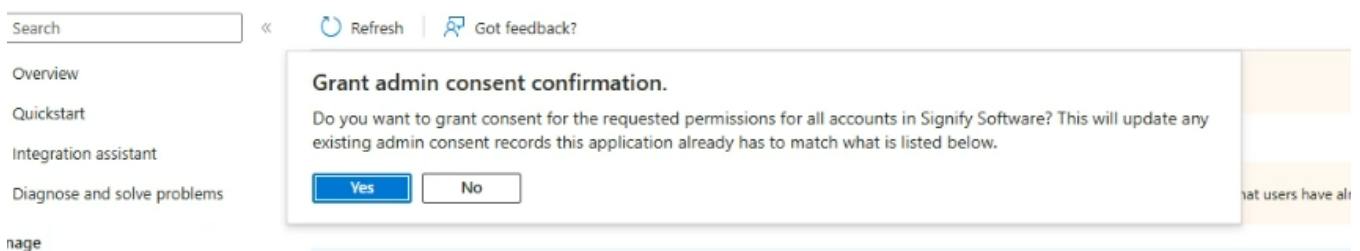
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/all the permissions the application needs. [Learn more about permissions and consent](#)



3. Confirm by clicking **Yes**.

Token-based email authentication | API permissions ⚙️ ...

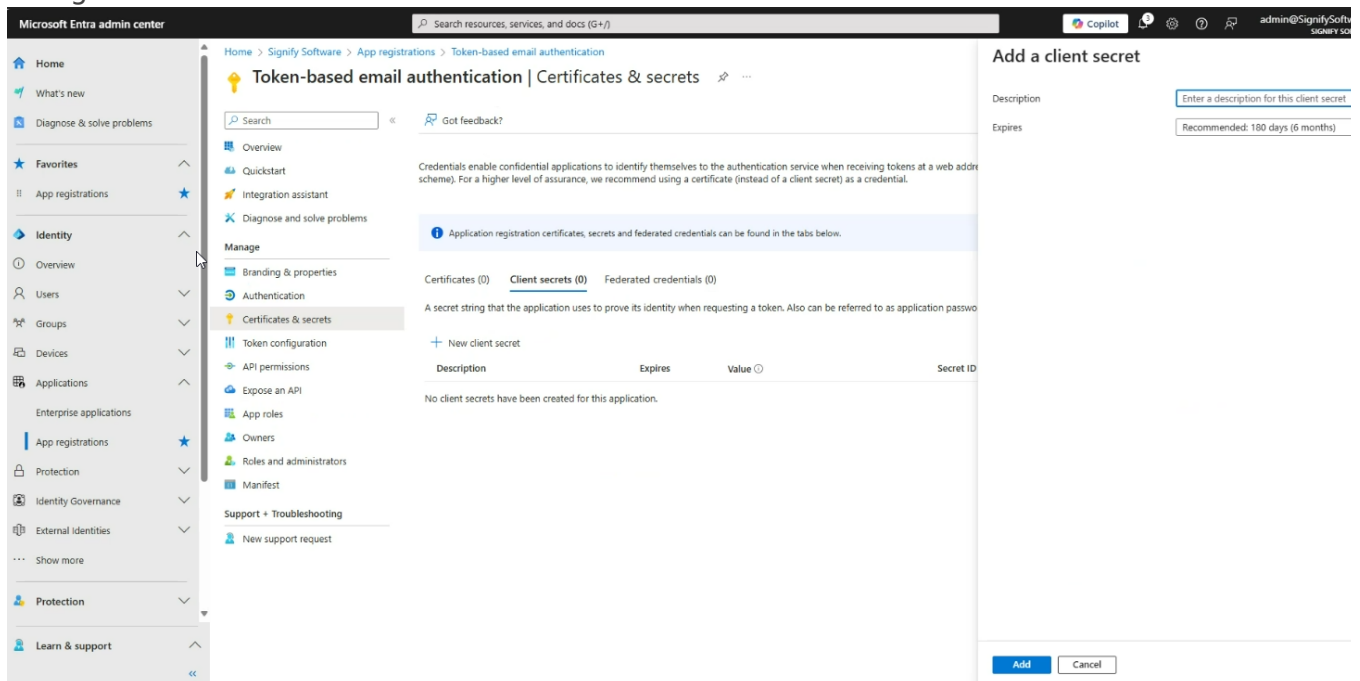


4. The interface will confirm that consent has been granted.



Step 5: Generate Client Secret

1. Navigate to **Certificates & Secrets → Client Secrets**.



2. Click **New Client Secret**.

Add a client secret

Description

Enter a description for this client secret

Expires

Recommended: 180 days (6 months) ▾

Recommended: 180 days (6 months)

90 days (3 months)

365 days (12 months)

545 days (18 months)

730 days (24 months)

Custom

3. Enter a **description** and set an expiration period (24 months recommended).
4. Click **Add**.
5. Copy and store the **Client Secret Value** immediately (it will not be available later).

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

Certificates (0) Client secrets (1) 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 | Expires | Value ⓘ | Secret ID |
|--------------|------------|-----------------------------------|--------------------------------------|
| Token Secret | 14/02/2027 | 1Wd8Q~Fc_p40IHVThQWMNELZROrBf7... | 1c9e1dca-912d-4b11-8e99-5713c7a80bac |

Step 6: Retrieve App Credentials

1. Go to the **Overview** section of your app registration.
2. Copy the following details:
 - **Application (Client) ID**
 - **Directory (Tenant) ID**

Token-based email authentication

Search << Delete Endpoints Preview features

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles

Essentials

Display name : [Token-based email authentication](#)

Application (client) ID : 8eddb659-72aa-46ed-a79d-...

Object ID : c4a9d463-8d31-4c7c-9124-

Directory (tenant) ID : a94ed6b1-9207-4541-971d-

Supported account types : [Any organization only](#)

Get Started Documentation

Welcome to the new and improved App registrations. Looking to learn how it's...

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory. We will no longer provide feature updates. Applications will need to be upgraded.

Signify Email Setup Using Token-Based Authentication

1. Open **Signify System**.
2. Navigate to **Gear** → **Ruleset** → **Notifications**.
3. Enable **Use Own SMTP Details**.
4. Activate **Credentials Required | Token-Based Authentication**.
5. Enter the details obtained from Microsoft Entra:

| Field | Value |
|---------------|----------------------------------|
| Server Name | Any logical name |
| Port | 587 |
| Timeout | 120 |
| Batch Size | Medium (Recommended) |
| From Email | Any user within the tenant |
| Client ID | Application (Client) ID (Step 6) |
| Client Secret | Token Secret Value (Step 5) |

| Field | Value |
|-----------|--------------------------------|
| Tenant ID | Directory (Tenant) ID (Step 6) |

- 6. Click **Save** to store and validate credentials.
- 7. If validation fails, review your configuration settings.

GENERAL

THEMES

PRODUCTS

SYSTEM MENU

DASHBOARD WIDGETS

SYSTEM ACCESS

NOTIFICATIONS

INTEGRATIONS

TEMPLATES

EMAIL SETUP

SMS SETUP

SCHEDULE SETUP

NOTIFICATION EVENTS

STATISTICS

The default SMTP configuration will be used if the current Ruleset's configuration settings are blank. Once the settings have been updated, this will be used to process notifications.

Use Own SMTP Details

Server name *
Azure

The server connection must be secured using an SSL certificate.

Port *
587

Time Out (Seconds) *
120

Batch Size

Medium (Up to 100 emails/min)

The maximum number of emails to be sent in a batch per minute.

From Email Address *

nardus.vaneyk@signify.co.za

From email address that will be used when sending notifications.

Enable email notifications

Credentials Required

Basic Authentication

Token-based Authentication

Client Id *

8eddb659-72aa-46ed-a79d

Client Secret *

1Wd8Q~Fc

Tenant Id *

a94ed6b1-9207-4541-

Revision #13

Created 14 February 2025 06:48:42 by Nardus van Eyk

Updated 17 February 2025 10:16:42 by Hendré van der Berg