Micro
OSTENDO

One system . **Complete** operations

Ostendo
Continuum Edition

Microsoft Graph API Email
Integration Setup Guide

24/02/2026

Revision 1.0.0

Table Of Contents

Overview

This guide walks you through configuring Microsoft Graph API to send emails from Ostendo Continuum. This replaces or supplements AWS SES as your email delivery method, using your organisation’s Microsoft 365 mailbox.

The integration uses Microsoft’s Client Credentials authentication flow, which allows Ostendo to send emails without requiring a user to sign in each time. The application authenticates with a Client ID and Secret, similar to an API key.

Prerequisites

- A Microsoft 365 subscription with Exchange Online mailboxes
- Administrator access to the Azure portal (portal.azure.com)
- The email address(es) you wish to send from (e.g. invoices@yourcompany.com, noreply@yourcompany.com)
- Access to Exchange Online PowerShell (for Application Access Policies)

Step 1: Register an Application in Azure

1. Sign in to the Azure portal at **portal.azure.com**
2. Navigate to **Microsoft Entra ID** (formerly Azure Active Directory)
3. Select **App registrations** from the left menu, then click **New registration**
4. Enter a name for the application (e.g. *Ostendo Continuum*)
5. Leave the Redirect URI blank (not required for this flow)
6. Click **Register**

Once registered, note the **Application (client) ID** and **Directory (tenant) ID** from the Overview page. You will need both of these values later.

Step 2: Create a Client Secret

1. In your app registration, select **Certificates & secrets** from the left menu
2. Click **New client secret**
3. Enter a description and select an expiry period (maximum 24 months)
4. Click **Add**

> **Important:** Copy the Value column immediately — it is only displayed once. Do not copy the Secret ID, which is a different value. If you lose the secret value, you will need to create a new one.

Step 3: Configure API Permissions

1. In your app registration, select **API permissions** from the left menu
2. Click **Add a permission**
3. Select **Microsoft Graph**
4. Select **Application permissions** (not Delegated)
5. Search for **Mail.Send** and select it
6. Click **Add permissions**
7. Click **Grant admin consent for [your organisation]** and confirm

> **Note:** Only the Mail.Send permission is required. Ostendo does not read or modify mailbox contents. This minimises the security impact if credentials are ever compromised.

Step 4: Restrict Sending to Specific Mailboxes

By default, the Mail.Send application permission allows the app to send email as any user in your organisation. To restrict this to only the intended sender addresses, configure an Application Access Policy in Exchange Online.

Connect to Exchange Online PowerShell

```
Connect-ExchangeOnline
```

Create a Policy for Each Sender Address

```
New-ApplicationAccessPolicy -AppId "your-client-id" `
-PolicyScopeGroupId "invoices@yourcompany.com" `
-AccessRight RestrictAccess `
-Description "Ostendo email sending"
```

Repeat for each sender address (e.g. noreply@yourcompany.com). Alternatively, create a mail-enabled security group containing all sender addresses and reference the group in a single policy.

Verify the Policy

```
Test-ApplicationAccessPolicy -AppId "your-client-id" `
-Identity "invoices@yourcompany.com"
```

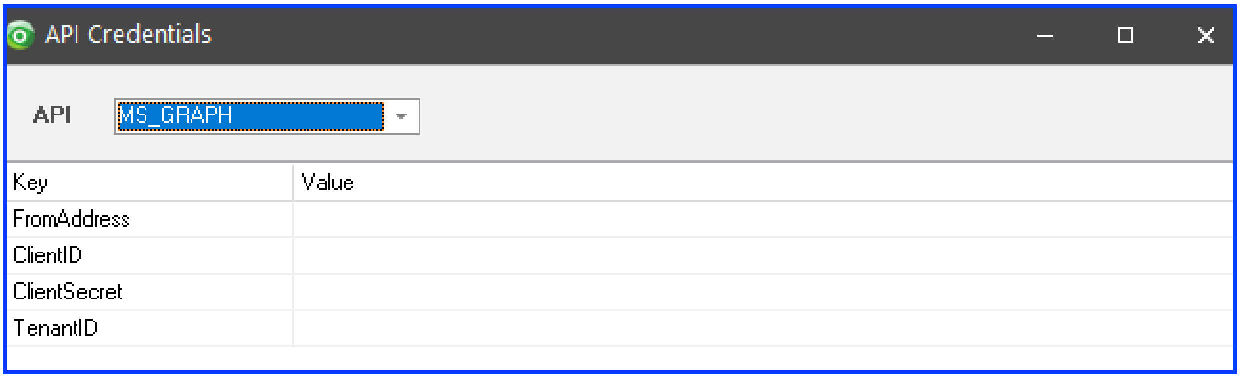
This should return **Granted** for your authorised sender addresses and **Denied** for all others.

Step 5: Configure Ostendo Continuum

1. In Ostendo, navigate to **File → System Configuration → API Credentials**
2. Select **MS_GRAPH** from the API dropdown
3. Enter the following values from your Azure app registration:

Key	Value
FromAddress	The email address to send from (e.g. invoices@yourcompany.com)
ClientID	Application (client) ID from the Azure app Overview page
ClientSecret	The secret Value you copied in Step 2
TenentID	Directory (tenant) ID from the Azure app Overview page

4. Tick the **Default** checkbox if this should be the primary email method
5. Exiting this screen will automatically save the record



API Credentials

API: MS_GRAPH

Key	Value
FromAddress	
ClientID	
ClientSecret	
TenantID	

Note: All credentials are stored encrypted in the Ostendo database.

Client Secret Expiry and Renewal

Azure client secrets have a maximum expiry of 24 months. When a secret expires, Ostendo will no longer be able to authenticate with Microsoft Graph and email sending will fail.

To avoid disruption, you should note the expiry date when creating the secret and schedule a renewal before it expires.

To Renew a Client Secret

1. In the Azure portal, go to your app registration and select **Certificates & secrets**
2. Create a new client secret (the old one will continue to work until it expires)
3. Copy the new secret **Value**
4. Update the **ClientSecret** in the Ostendo API Credentials screen
5. Delete the old secret from Azure once the new one is confirmed working

Important: Set a calendar reminder to renew the client secret before it expires. If it expires without renewal, email sending will stop until a new secret is configured.

Troubleshooting

Error	Solution
unauthorized_client / AADSTS700016	The Client ID or Tenant ID is incorrect. Verify both values match the app registration Overview page.
InvalidAuthenticationToken	The access token is invalid or expired. Check the Client Secret is the Value (not the Secret ID) and has not expired.
ErrorAccessDenied / 403	Mail.Send permission has not been granted, or admin consent has not been given. Check API permissions in Azure.
MailboxNotFound / 404	The FromAddress does not have a valid Exchange Online mailbox. Ensure the address has a Microsoft 365 licence assigned.
Access policy denied / 403	The Application Access Policy is restricting access. Verify the policy includes the sender address using Test-ApplicationAccessPolicy