

Grandstream Networks, Inc.

**Grandstream IPPBX – Microsoft Outlook
Authentication Guide**



OVERVIEW

Grandstream IPPBX supports integration with Microsoft Outlook, allowing users to receive important email notifications directly from the PBX.

This guide describes setting up and configuring the authentication between Grandstream IPPBX and Microsoft 365, ensuring efficient and secure email communication using modern OAuth2 authentication.

This guide is divided into three parts, each performed in a different administrative portal:

- Microsoft 365 Admin Center
- Azure Portal / Microsoft Entra ID
- Grandstream PBX Web UI

PREREQUISITES

Before starting, confirm the following:

- A Microsoft account with **global administrator permissions** is available.
- The **global administrator account** has been assigned a Microsoft Entra ID P1 or P2 license.
- The **email sending account** that will be used by the PBX has an Exchange Online license.

This integration requires two separate Microsoft licenses that serve different purposes and must not be confused:

- **Microsoft Entra ID:** Required for the administrator account performing the Azure app registration and authentication configuration. This is an identity and access management license only. It does NOT include email or mailbox functionality.
- **Exchange Online license:** Required for the account that will be used to send emails from the PBX. This provides the actual mailbox and SMTP sending capability.

MICROSOFT 365 ADMIN CENTER SETUP

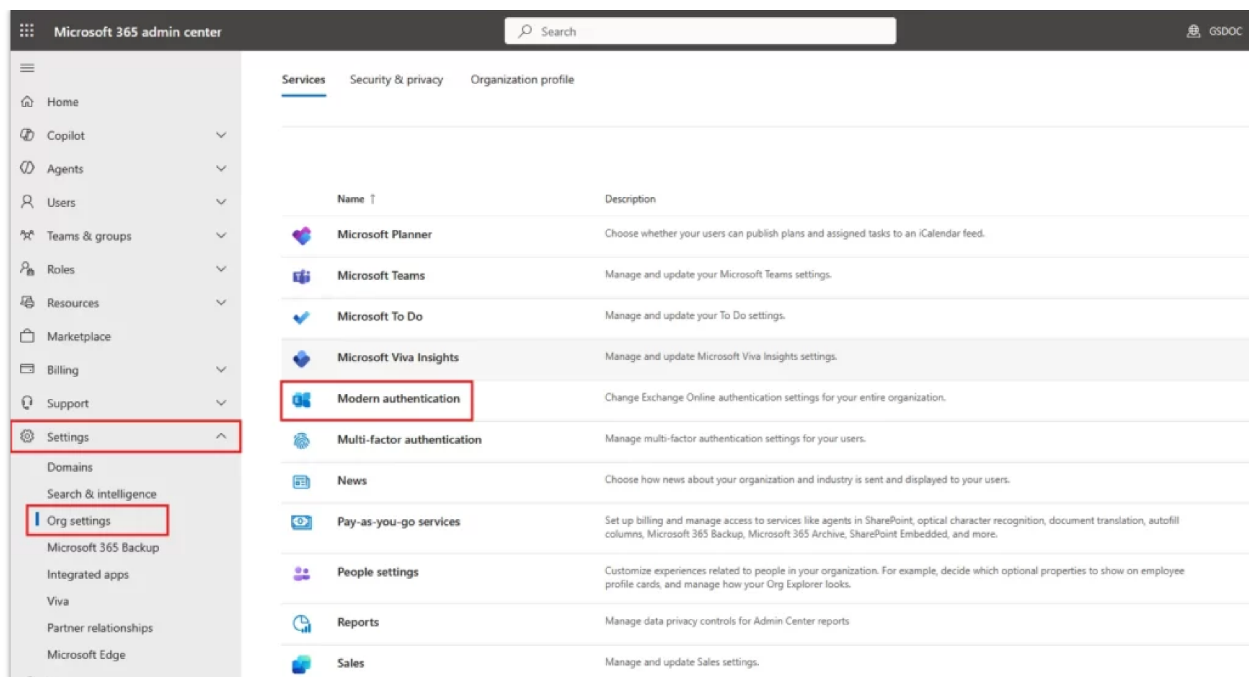
This part covers three tasks that must be completed before touching the Azure Portal:

1. Enabling Modern Authentication
2. Verifying licenses
3. Enabling Authenticated SMTP on the sending account

Step 1: Enable Modern Authentication

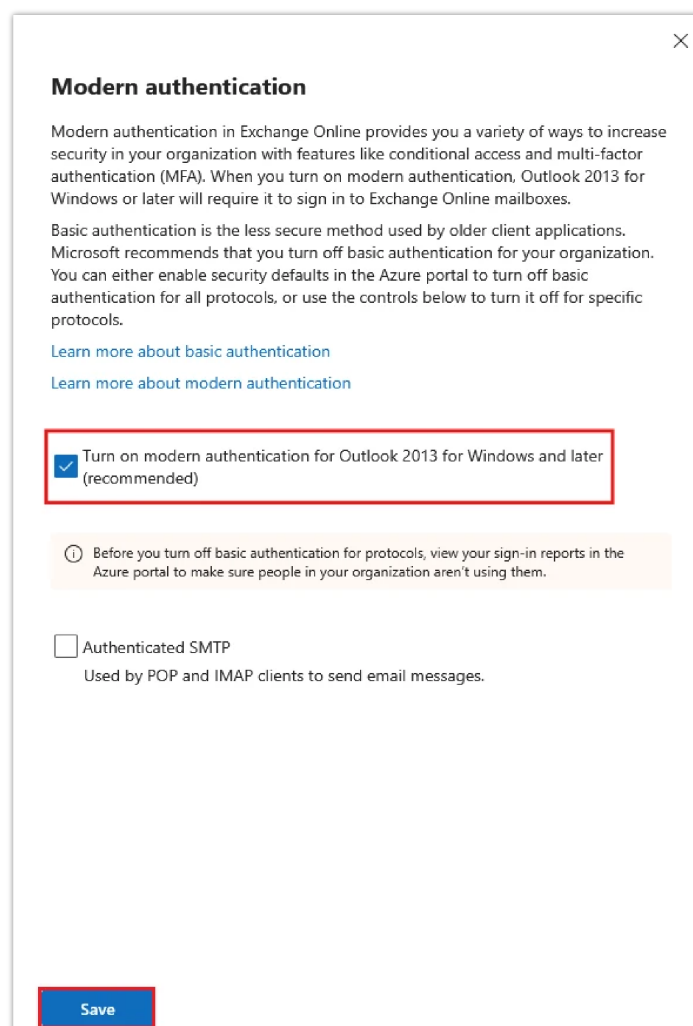
Modern authentication is the foundation of the OAuth2 flow used in this guide. Without it, the authorization process will not work.

1. Log in to the [Microsoft 365 Admin Center](#) using your global administrator account.
2. In the left navigation menu, go to **Settings** → **Org Settings**.
3. Under the **Services** tab, locate and click **Modern Authentication**.



Microsoft 365 Admin Center Org Settings

4. In the Modern Authentication panel that appears, check the box for *Turn on modern authentication for Outlook 2013 for Windows and later (recommended)*.
5. Click Save.

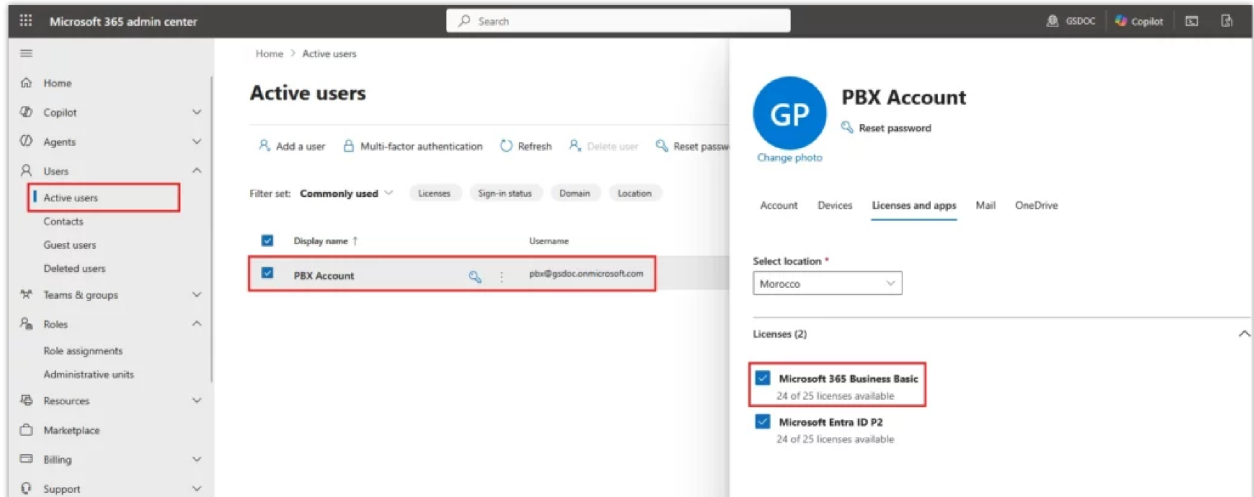


Modern Authentication Configuration Tab

Step 2: Verify License Assignment

Before enabling Authenticated SMTP, confirm that the email sending account has the correct Exchange Online license assigned.

1. In the left navigation menu, go to **Users** → **Active Users**.
2. Locate and click on the account that will be used to send emails from the PBX.
3. In the user details panel, click the **Licenses and apps** tab.



User Details Panel Licenses and apps Tab

4. Confirm that an Exchange Online license is listed and enabled. Acceptable licenses include:
 - Exchange Online Plan 1
 - Exchange Online Plan 2
 - Microsoft 365 Business Basic
 - Microsoft 365 Business Standard
 - Microsoft 365 Business Premium

Step 3: Enable Authenticated SMTP

This step grants the account permission to connect to Microsoft's SMTP server and send emails on behalf of the PBX.

1. On the same user account, click the **Mail** tab.
2. Click **Manage email apps**.





PBX Account

 [Reset password](#)

[Change photo](#)

Account

Devices

Licenses and apps

Mail

OneDrive

Mailbox storage

0% (477.7KB/100GB)

[Learn more about mailbox storage quotas](#)

Mailbox permissions

[Read and manage permissions \(0\)](#)

[Send as permissions \(0\)](#)

[Send on behalf of permissions \(0\)](#)

Show in global address list

Yes

[Manage global address list visibility](#)

Automatic replies

Off

[Manage automatic replies](#)

Email apps

POP blocked

OWA blocked

IMAP blocked

Other email apps allowed

[Manage email apps](#)

Email forwarding

None

[Manage email forwarding](#)

More actions

[Convert to shared mailbox](#)

[Edit Exchange properties](#)

User Details Panel Mail Tab

3. In the Manage email apps panel, check the box for **Authenticated SMTP**.
4. Click Save changes.

←

×

Manage email apps

Choose the apps where PBX Account can access Microsoft 365 email.

☐ Outlook on the web

☐ Outlook desktop (MAPI)

☐ Exchange web services

☐ Mobile (Exchange ActiveSync)

☐ IMAP

☐ Pop

☒ Authenticated SMTP

Save changes

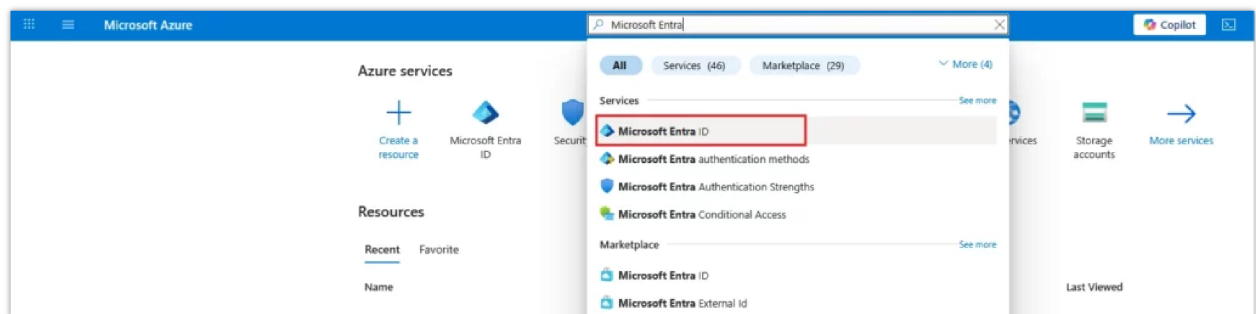
Authenticated SMTP Checkbox

MICROSOFT ENTRA ID SETUP

This part registers the Grandstream PBX as an application in Microsoft Entra ID, grants it the necessary permissions to send email, and generates the credentials the PBX will use to authenticate.

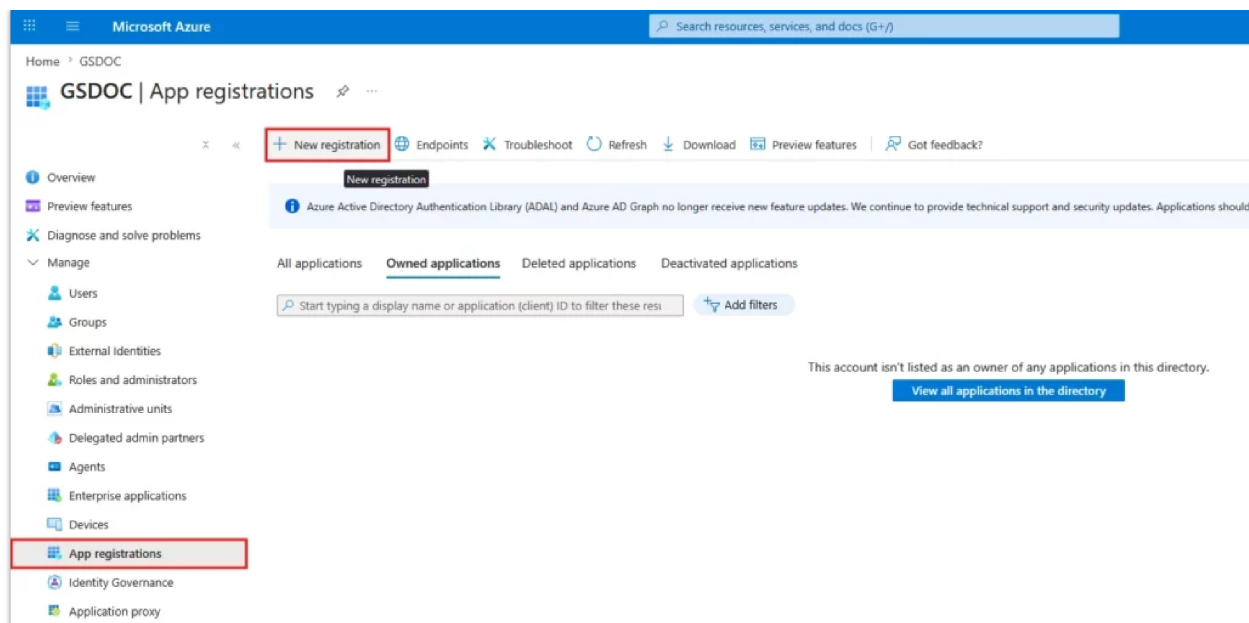
Step 1: Register the Application in Microsoft Entra ID

1. Log in to the [Azure Portal](#) using your global administrator account.
2. In the top search bar, search for and select **Microsoft Entra ID**.



Azure Portal Search Bar with Microsoft Entra ID

3. In the left navigation of the Microsoft Entra ID page, click **App registrations**, then click **New registration**.



App Registrations Page

4. On the Register an application page, fill in the following fields:

Field	Value
Name	Enter a display name for the application (e.g. "Grandstream UCM")
Supported account types	Select Accounts in this organization's directory only.
Redirect URI	Select Web from the platform dropdown and enter the Redirect URI (see note below).

Redirect URI

The Redirect URI is a landing page where Microsoft sends your browser after a successful login, with the authorization code appended to the URL as a parameter.

You will manually copy this authorization code from the browser and paste it into the PBX. The Redirect URI you enter here in Azure must exactly match the URI you later enter in the PBX Email Settings.

- **Recommended URI:** Use Grandstream's dedicated OAuth landing page (<https://ucm.grandstream.com/googleoauth/>). After login, this page automatically extracts and displays the authorization code for easy copying.
- **Alternative URIs:** Any HTTPS URL can be used (<https://example.grandstream.com>). After login, Microsoft redirects your browser to that page with the code in the URL. You will need to manually copy it from the address bar. See [Step 3: Get the Authorization Code] section for detailed instructions on extracting the code.

Microsoft Azure

Home > GSDOC | App registrations

Register an application

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

Supported account types
Choose the account types that can use this application or access this API
Single tenant only - GSDOC [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 [https://ucm.grandstream.com/googleoauth/](#)

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

Register an Application Page

5. Click **Register**.

6. After registration is complete, you will be taken to the application overview page. **Note down the following values** as you will need them in Part 3:

- **Application (Client) ID**
- **Directory (Tenant) ID**

Microsoft Azure

Home > GSDOC | App registrations

Grandstream UCM

Search

Deactivate Delete Endpoints Preview features

Overview

Quickstart
Integration assistant
Diagnose and solve problems
Manage
Support + Troubleshooting

Essentials

Display name	: Grandstream UCM	Client credentials	: Add a certificate or secret
Application (client) ID	: a4e0fbd2-5bce-473c-...	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: 3ad1150e-df88-4839-...	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 7b76bdc4-4a50-49d0-...	Managed application in...	: Grandstream UCM
Supported account types	: My organization only	State	: Activated

Application Overview Page

Step 2: Assign API Permissions

1. In the left navigation of the application page, click **API permissions**, then click Add a permission.

Microsoft Azure

Home > GSDOC | App registrations > Grandstream UCM

Grandstream UCM | 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

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf will remain.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the actual consent status.

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 permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

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

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				...
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](#).

API Permissions Page

2. In the Request API permissions panel, click APIs my organization uses, then search for and select **Office 365 Exchange Online**.

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

Office 365

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000

Request API Permissions Panel

3. Select Application permissions.
4. In the permissions list, search for SMTP and expand the SMTP section. Check **SMTP.SendAsApp**.

Request API permissions

< All APIs

Office 365 Exchange Online
https://outlook.office.com

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

SMTP

Permission	Admin consent required
SMTP (1)	
☒ SMTP.SendAsApp ⓘ Application access for sending emails via SMTP AUTH	Yes

Add permissions Discard

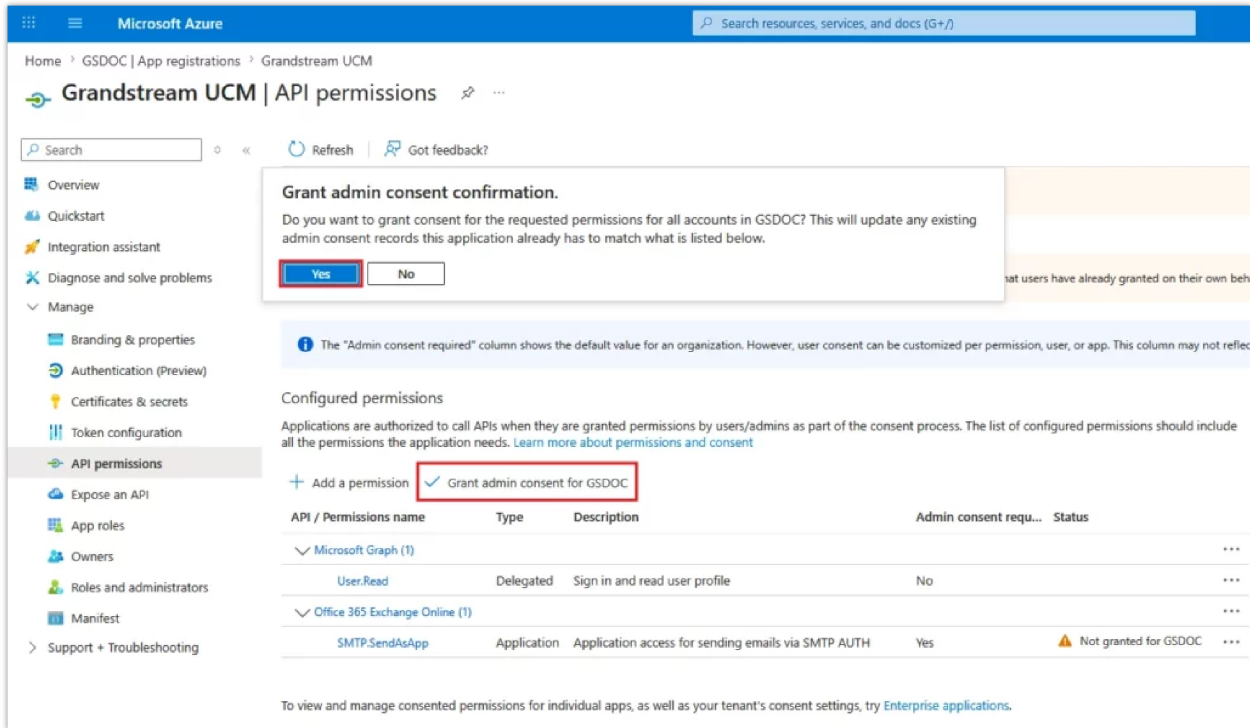
SMTPSendAsApp Permission

5. Click **Add permissions**.

Step 3: Grant Admin Consent

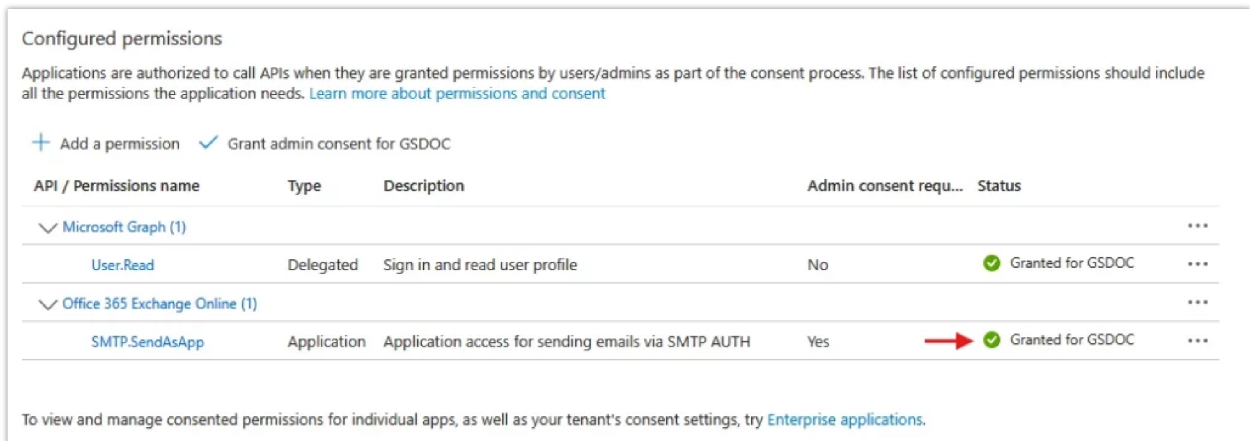
This step requires you to be logged in to the Azure Portal with a global administrator account. If the account currently logged in is not a global administrator, log out and sign back in with the correct account, or contact your organization's global administrator to complete this step on your behalf

- 1. Back on the API permissions page, click **Grant admin consent for [your organization name]**.
- 2. Click Yes to confirm.



Grant Admin Consent for API Permission

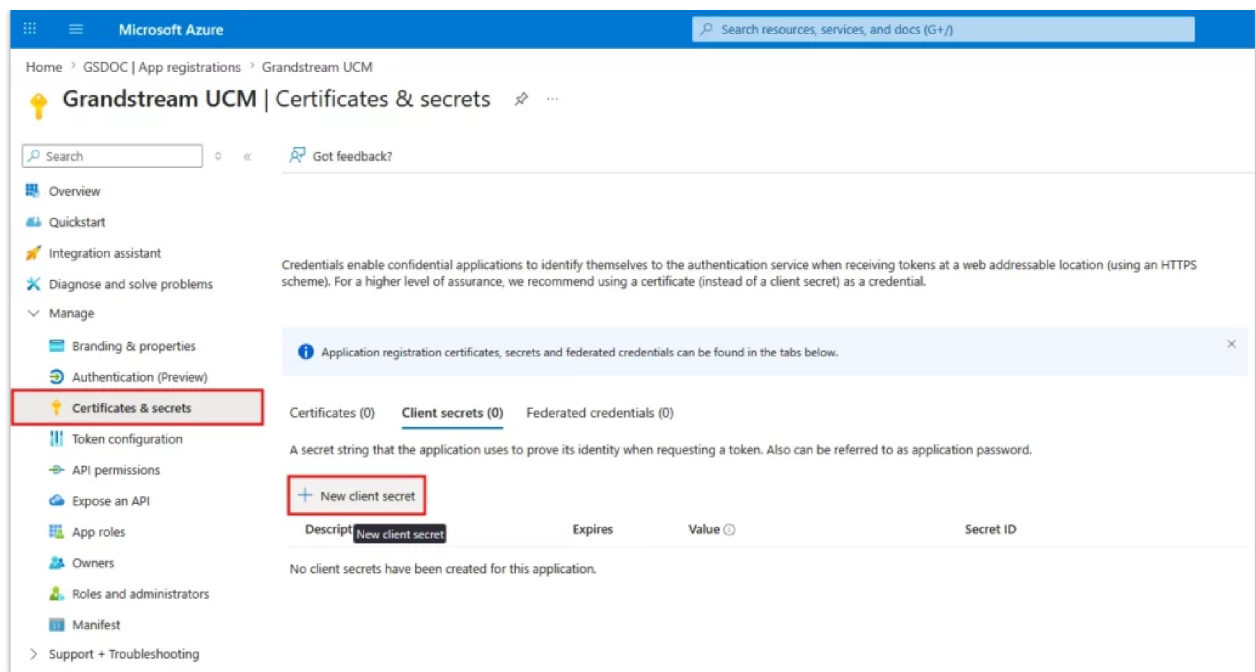
- 3. After granting consent, the status column for **SMTP.SendAsApp** should show a green checkmark indicating **"Granted for [organization]"**.



Admin Consent Granted Successfully

Step 4: Create a Client Secret

- 1. In the left navigation of the application page, click **Certificates & secrets**, then click **New client secret**.



Certificates Secrets Page

2. In the Add a client secret panel, fill in the following:

Field	Value
Description	Enter a description label (e.g. "Grandstream UCM Outlook")
Expires	Select an expiration period (recommended: 180 days/6 months)

Add a client secret

Description

Grandstream UCM Outlook

Expires

Recommended: 180 days (6 months) ▾

Add

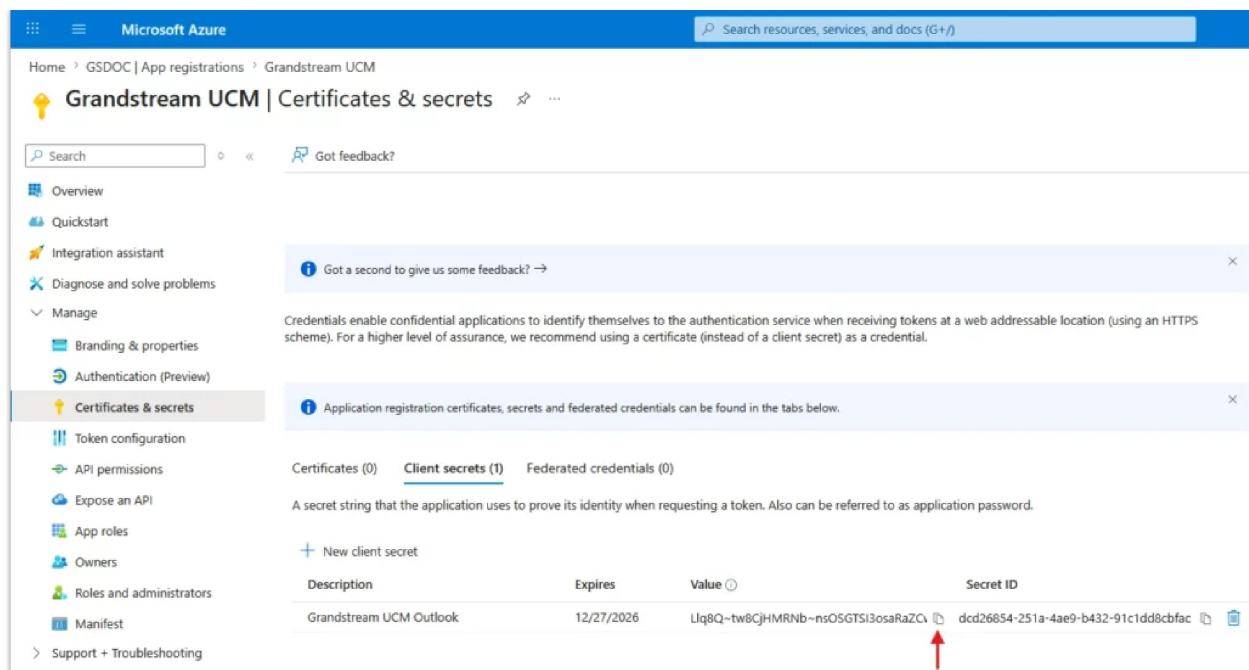
Cancel

Add a Client Secret Panel

3. Click **Add**.
4. The new client secret will appear in the list. Copy the value shown in the “*Value*” column and store it securely.

Note:

This value is only displayed in full immediately after creation. Once you navigate away from this page, the value will be permanently hidden and cannot be retrieved. If lost, you must create a new client secret.



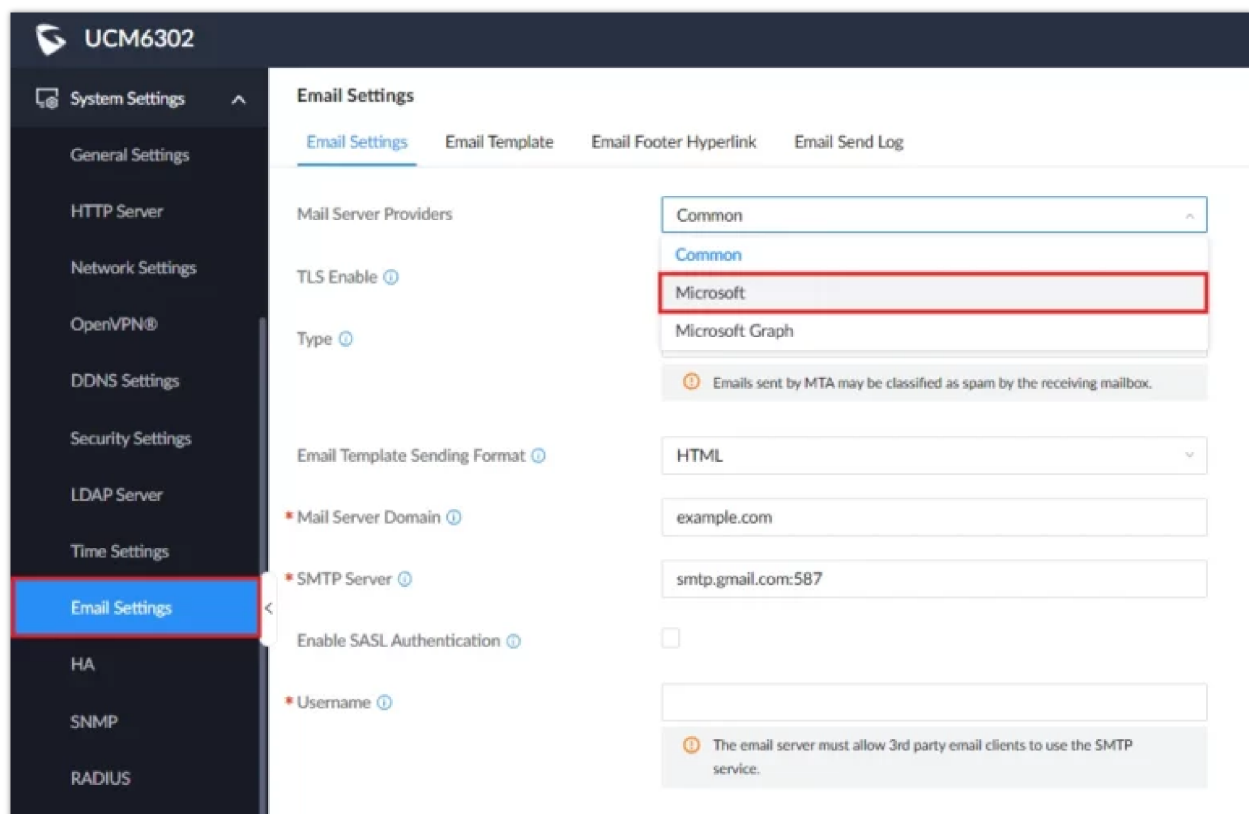
Client Secret Created

GRANDSTREAM PBX CONFIGURATION

This part enters all the credentials gathered into the PBX, completes the OAuth authorization flow, and verifies the configuration with a test email.

Step 1: Configure Email Settings

1. Log in to the PBX Web UI.
2. Navigate to **System Settings** → **Email Settings**.
3. In the **Mail Server Providers** drop-down, select **Microsoft**.



PBX Web UI System Settings → Email Settings page

4. The Server Authorization section will appear showing that authentication is incomplete. Click **De-authorization** to open the Microsoft Server Licensing configuration dialog.

Step 2: Enter Authorization Information

In the Microsoft Server Licensing dialog, fill in the following fields:

Field	Value
Redirect URIs	The exact same URI registered in Microsoft Entra ID Setup, Step 1 (e.g. https://ucm.grandstream.com/googleoauth/)
Tenant ID	The Directory (Tenant) ID from the Azure application overview page
Username	The Microsoft 365 email address of the sending account that was configured in Microsoft 365 Admin Center Setup
The Application (Client) ID	The Application (Client) ID from the Azure application overview page
The client password	The client secret Value copied in Step 4 (Create a Client Secret)

Microsoft Server Licensing

1 Fill in the information — 2 Authorization

* Redirect URIs

* Tenant ID

* Username

* Application (Client) ID

* Client Password

Cancel Get Authorization Code

Microsoft Server Licensing Dialog

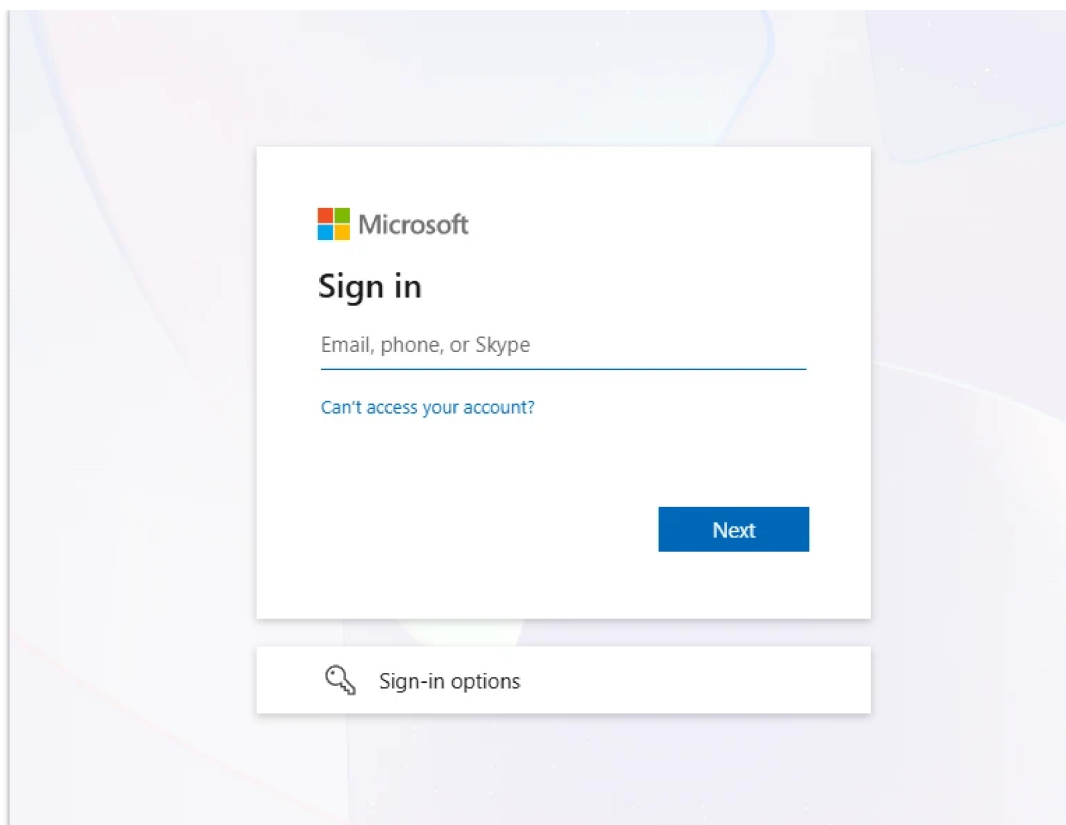
Note:

The Redirect URI entered here must be identical to the one registered in Azure. Any mismatch including an extra slash will cause the authorization to fail.

Step 3: Get the Authorization Code

Once the information is correctly entered, please follow the steps below to complete the authorization flow:

1. Click **Get Authorization Code**.
2. A new browser window or tab will open and redirect you to Microsoft's login page.
3. Sign in using the email sending account (the Microsoft 365 account configured).



Microsoft Login Page

4. After successfully signing in, Microsoft will redirect your browser to the Redirect URI you configured. What you see next depends on which Redirect URI you used:

If you used the Grandstream redirect URI (<https://ucm.grandstream.com/googleoauth/>): The page will display the authorization code directly on screen in a text box, ready to copy.



Grandstream OAuth Page Displaying the Authorization Code

If you used any other HTTPS URI (e.g. <https://your.example.com>): Your browser will land on that page. Copy the link from the browser's address bar the full URL will look like this:

```
https://your.example.com/?code=1.AXoAxL12e1BK0Emw...LONGCODE...&state=GrandStream&session_state=xxxxx
```

Copy only the value that starts after `code=` and ends before `&state=`. This is your authorization code. Do not include `&state=` or anything after it.

If the page shows an error or "Server Not Found": This is expected if your Redirect URI points to a non-existent page. The authorization code is still present in the browser address bar. Copy the value as described above.

Step 4: Complete Authorization

1. Paste the copied authorization code into the **Authorization Code** field in the PBX dialog.

Microsoft Server Licensing

1 Fill in the information ——— 2 **Authorization**

Enter the Microsoft account and password you want to authorize in the newly opened authorization window and click "Accept" to get the authorization code. If the window does not pop up please [Click here](#) to copy the link to the authorization window.

*** Authorization Code**

JW8TvHUhJyAr5T38JK2RGtNopcK1pJVVMKWmUTgoyQtvd

Previous **Authorization**

Code Pasted Into The Authorization Code Field

2. Click **Authorization**.
3. Click **Save**, then click **Apply Changes** for the configuration to take effect.

After completing authorization, the Email Settings page will show the authorized Microsoft account under Server Authorization.

UCM6302

System Settings

General Settings

HTTP Server

Network Settings

OpenVPN®

DDNS Settings

Security Settings

LDAP Server

Time Settings

Email Settings

HA

Email Settings

Email Template

Email Footer Hyperlink

Email Send Log

Item is saved successfully. Please click **Apply Changes** to take effect.

Mail Server Providers: Microsoft

Server Authorization

Authorized Account: pbw@igxdoc.owenmicrosoft.com

De-authorization >

Email Delivery Settings

Email Template Sending Format: HTML

* Display Name: PBX

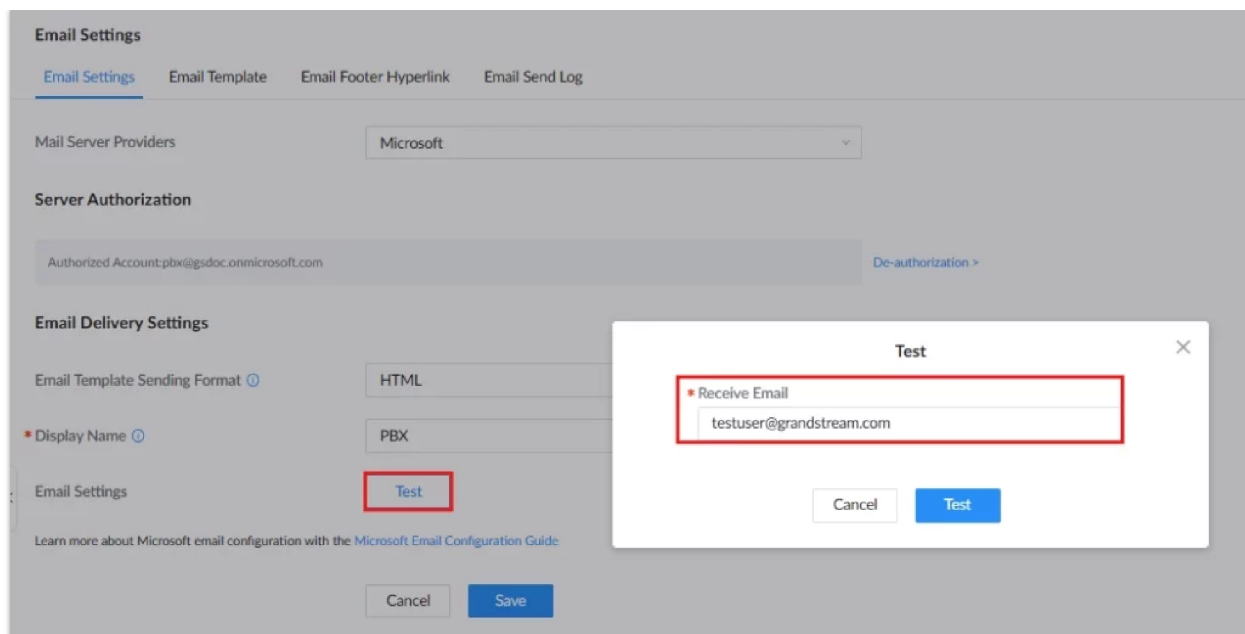
Test

Learn more about Microsoft email configuration with the [Microsoft Email Configuration Guide](#)

Email Settings Page Showing the Authorized Account

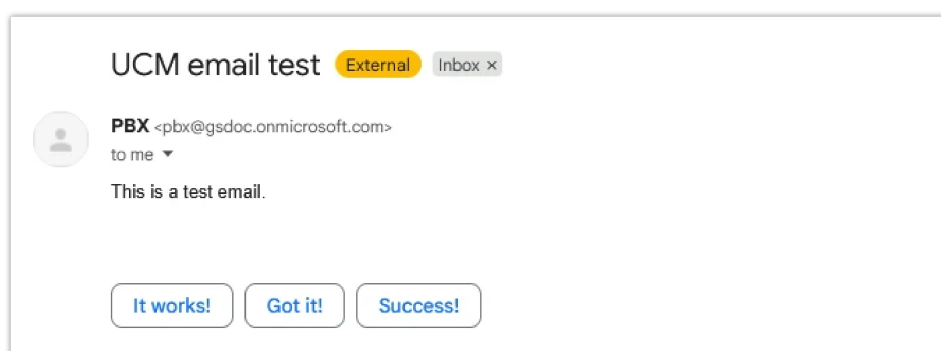
Step 5: Send a Test Email

1. On the Email Settings page, click **Test**.
2. In the Test dialog, enter a recipient email address in the **Receive Email** field.
3. Click **Test**.



Test Email Dialog with a Recipient Address

4. Check the recipient inbox to confirm the email was received. The sender will appear as your Microsoft sending account.



Test Email Received in Inbox

SUPPORTED MODELS

Supported Devices	Firmware version
SoftwareUCM	1.0.27.18+
UCM6300/A Series	1.0.27.20+
CloudUCM	1.0.29.7+