

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 Outlook, ensuring efficient and secure email communication.

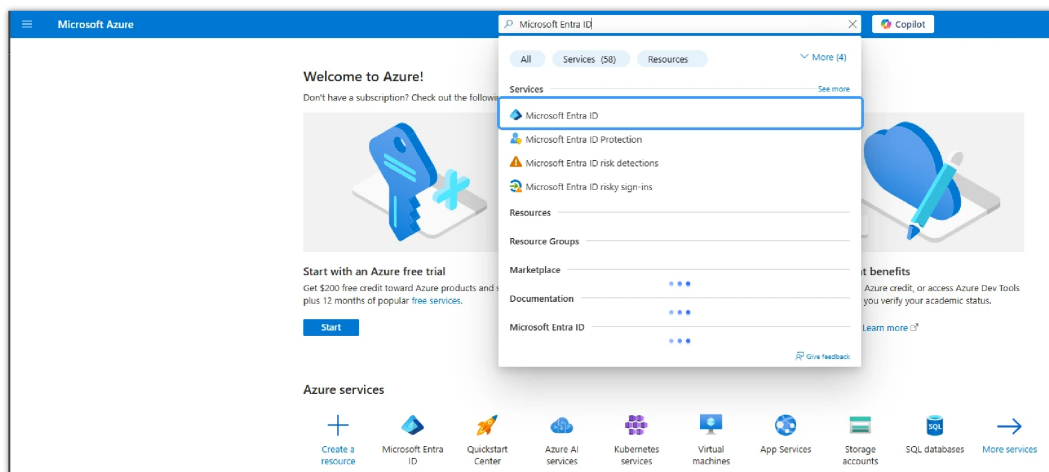
Usage Requirements

- Microsoft account with **global administrator permissions**.
- The account has been assigned a Microsoft 365 license. (Microsoft Entra ID P2)
- Modern authentication has been enabled in [the Microsoft 365 admin center](#).

Configuring the Application

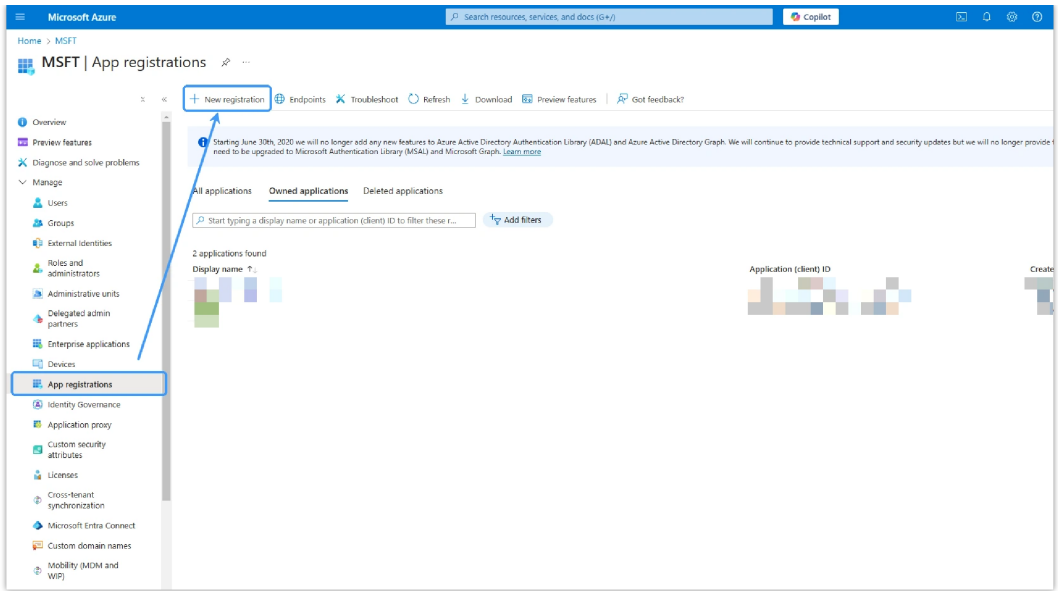
Registering the application with Microsoft Entra ID

1. Access the [Azure Portal](#) using the account with **global administrator privileges**.
2. In the search bar, search for and select the **Microsoft Entra ID** service to enter the organization's directory.



Azure Portal Search

3. In the left navigation of the organization directory, go to **App Registrations** and click **New Registration**.



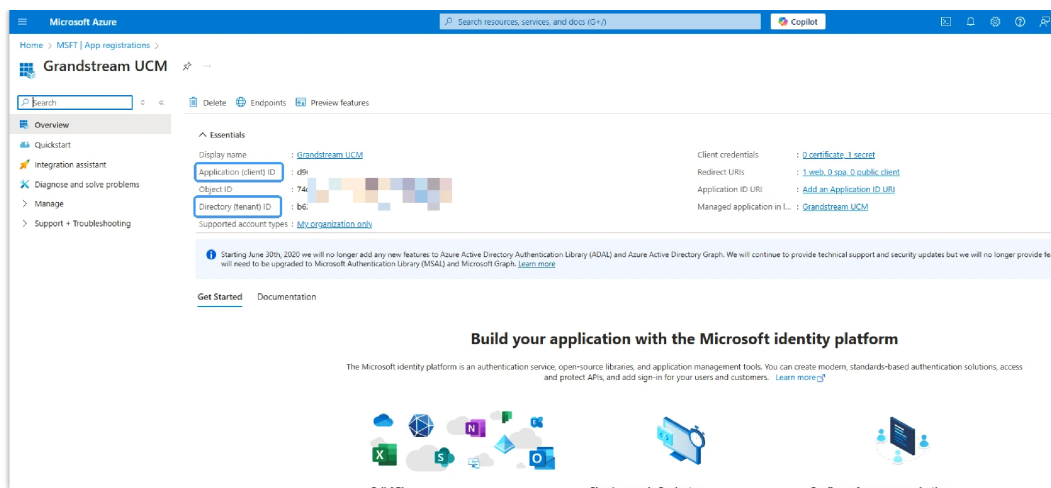
Create New Registration

4. On the **App Registration** page, configure the application's registration information based on the table below, and then click **Register**.

Registration Information

Name	Set the name that the application needs to display.
Supported account types	Select Accounts in this organization's directory only.
Redirect URI	In the Select Platform drop-down list, select Web , and then fill in the URI that needs to receive the token . Make sure this URI is secure and can be accessed normally.

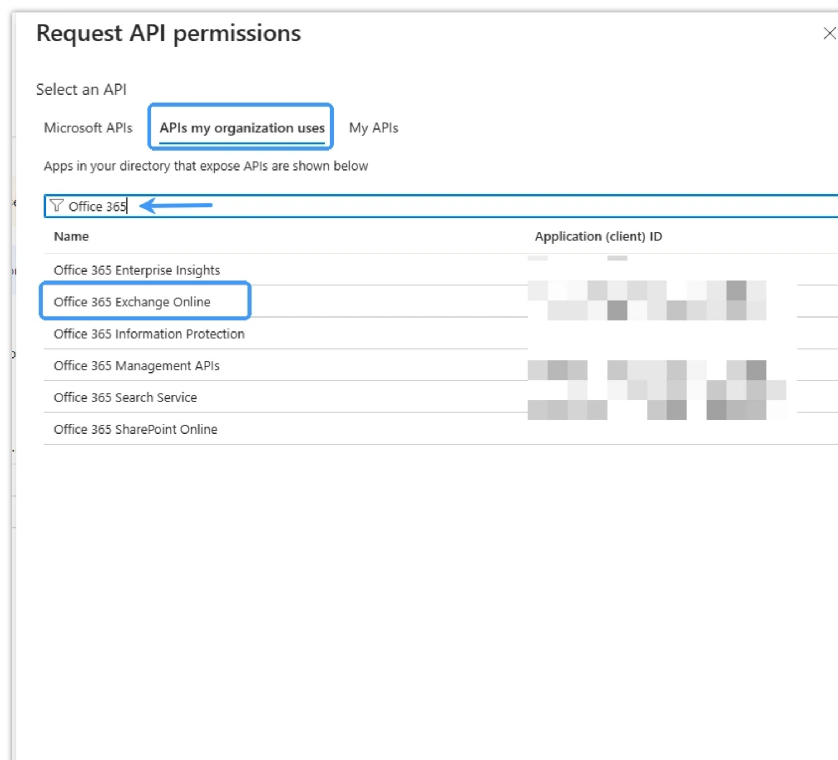
5. After completing the registration, the page will jump to the application's **overview** page. **The application (client) ID** and **directory (tenant) ID** of this application will be needed to fill in the relevant information on the PBX later.



Application Information

Assigning the Application API Permissions

1. In the left navigation bar of the application, go to **API Permissions—Add Permissions**.



Requesting API Permissions

2. Click **Application Permissions** and search for "SMTP". 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

Permission

Admin consent required

SMTP (1)

☒

SMTP.SendAsApp

Application access for sending emails via SMTP AUTH

Yes

Add permissions

Discard

SMTP Permission

- In **API Permissions**→**Agree on behalf of XX administrator**, click Agree to permission. (If this account is not the highest-authority administrator account, please contact the highest-authority administrator account to agree to the permission).

Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Home > MSFT | App registrations > Grandstream UCM

Grandstream UCM | API permissions

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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 are...

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 v...

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 MSFT

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...
Office 365 Exchange Online (1)				...
SMTP.SendAsApp	Application	Application access for sending emails via SMTP AUTH	Yes	Not granted for MSFT

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Grant Admin Consent

- After agreeing, the status of the corresponding API permissions will switch to normal.

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](#)

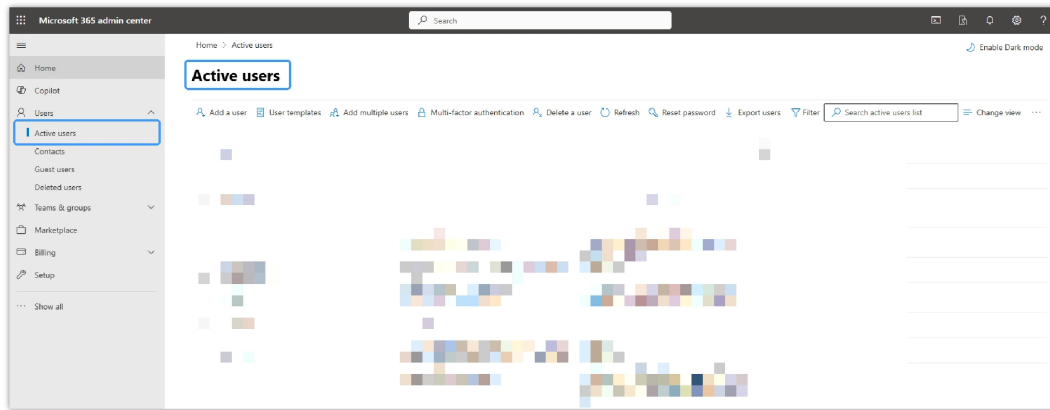
Add a permission

Grant admin consent for MSFT

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	Granted for MSFT
Office 365 Exchange Online (1)				...
SMTP.SendAsApp	Application	Application access for sending emails via SMTP AUTH	Yes	Granted for MSFT

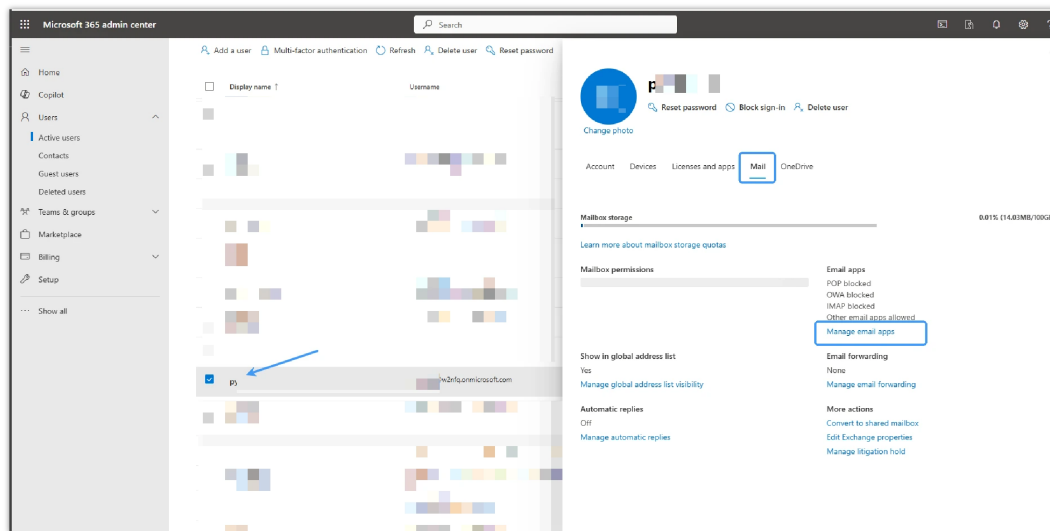
Admin Consent Granted

5. Use the highest privilege account to log in to [the Microsoft 365 admin center](#), find **User→Active users** in the left menu bar, and locate the corresponding user.



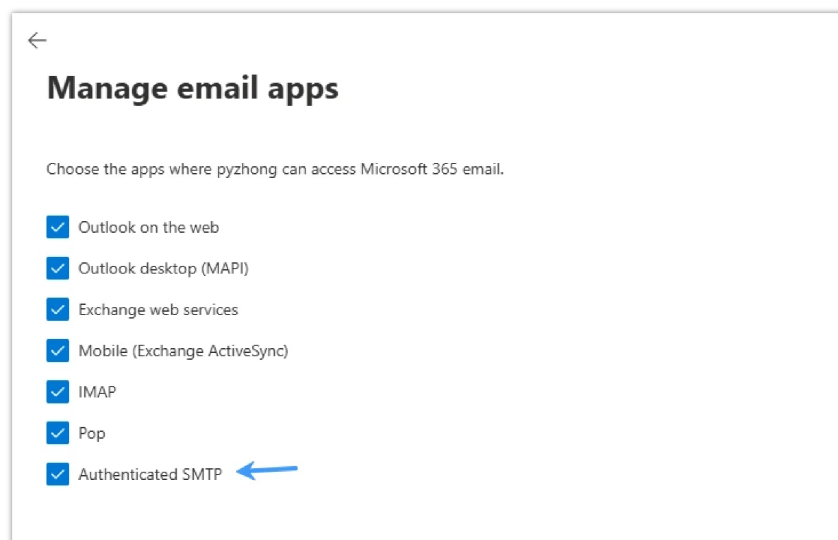
Active Users Page

6. Click on the target account and select **Mail→Manage email apps**.



Manage Email Apps

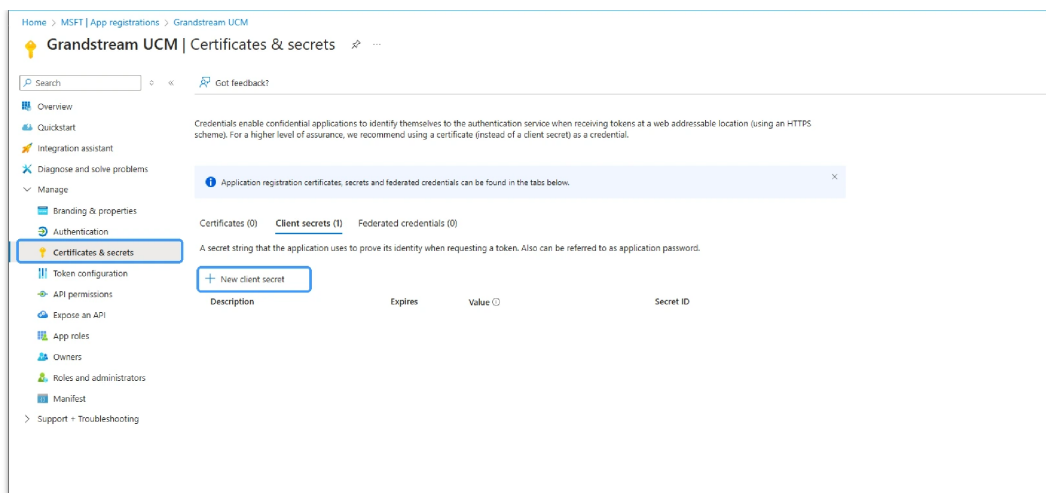
7. Check **Authenticated SMTP** and save to have the authority to log in to the SMTP server and send emails.



Authenticated SMTP

Creating a Client Secret for the Application

1. On the left navigation bar of the application, go to **Certificates & Passwords→Client Passwords** and click **New Client Secret**.



Certificates & Secrets Page

2. Complete the permission settings for the client key and add corresponding instructions.

Add a client secret

Description

Grandstream UCM Outlook

Expires

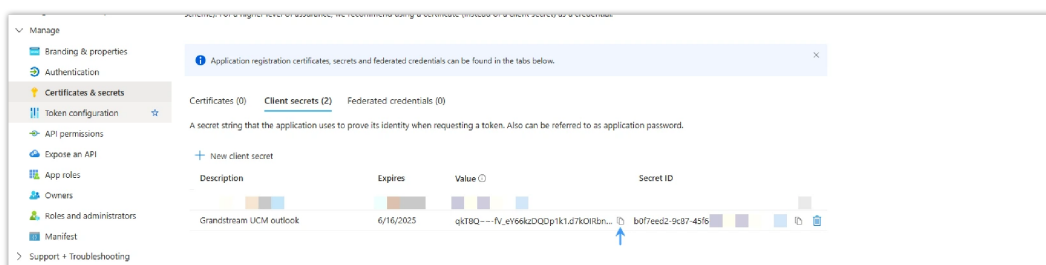
Recommended: 180 days (6 months)

Client Secret Information

3. After completing the secret creation, the corresponding client key can be seen on the **Certificate & Secrets page**. This information will be needed to fill in the relevant information on the PBX later.

Note:

This information will only be displayed in full when it is created. Please ensure to record this value before leaving this page. Once the page is switched, this value will no longer be displayed publicly.



Client Secret Created

Configuring SMTP-related information on PBX

1. Log in to the PBX Web UI and go to **System Settings**→**Email Settings**.
2. In the **Mail Server Providers** drop-down list, select **Microsoft** and click on **De-authorization**.

Email Settings

Email Settings | Email Template | Email Footer Hyperlink | Email Send Log

Mail Server Providers: Microsoft

Server Authorization

Authentication with Microsoft servers incomplete. Please complete Microsoft authentication first. [De-authorization >](#)

Email Delivery Settings

Email Template Sending Format: HTML

* Display Name: PBX

Test

Cancel Save

PBX Email Settings

3. Fill in the relevant verification information based on the table below.

Microsoft Server Licensing

1 Fill In The Information | 2 Authorization

* Redirect URIs: htt

* Tenant ID: b6...

* Username: py.

* Application (Client) ID: 11...

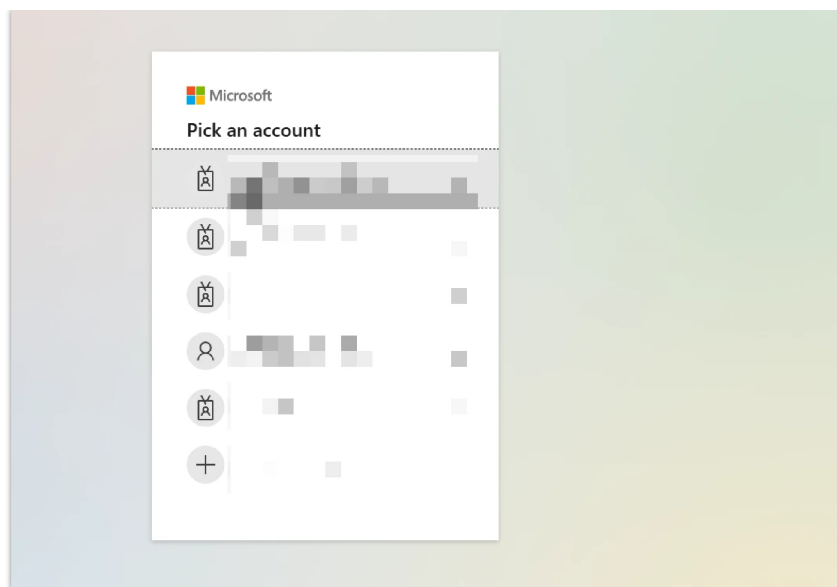
* Client Password: 3...

Cancel Get Authorization Code

Filling the Authorization Information

Redirect URIs	The redirect URI that needs to receive the token.
Tenant ID	The Directory (tenant) ID of the Microsoft Entra application
Username	Microsoft Entra login username.
The Application (Client) ID	The Application (Client) ID of the Microsoft Entra application.
The client password	The client secret of the Microsoft Entra application.

4. Click **GetAuthorization Code** to get redirected to the login page of the redirection URI. Select the **global permission account** to log in, and a token will be sent to **the redirection URI**.



Redirection Login Page

5. Copy the token obtained, fill it on the PBX, and select **Authorization**. Click the **Save** button and **Apply Changes** for the relevant email configuration to take effect.

A screenshot of the "Microsoft Server Licensing" window. The window has a white background with a blue header bar. The header bar contains the text "Microsoft Server Licensing" and a close button (X). Below the header bar, there are two tabs: "Fill In The Information" (selected) and "Authorization". The "Authorization" tab is active, showing instructions: "Enter the Microsoft account and password you want to authorize in the newly opened authorization window and click 'Accept' to get the authorization code string. If the authorization window does not pop up click [Get Authorization Code](#)". Below the instructions, there is a text input field labeled "Authorization Code" with a placeholder text "25...". At the bottom, there are two buttons: "Previous" and "Authorization" (highlighted with a blue border).

Authorization Code

After completing the authorization, a test email can be sent with the sender appearing as:

PBX<{your Microsoft account username}>

A screenshot of the "Email Settings" window. The window has a grey background with a white header bar. The header bar contains the text "Email Settings" and four tabs: "Email Settings" (selected), "Email Template", "Email Footer Hyperlink", and "Email Send Log". Below the header bar, there is a dropdown menu labeled "Mail Server Providers" with "Microsoft" selected. Below the dropdown menu, there is a section titled "Server Authorization" with a text input field labeled "Authorized Account" and a "De-authorization >" link. Below the "Server Authorization" section, there is a section titled "Email Delivery Settings" with a text input field labeled "Email Template Sending Format" set to "HTML", a text input field labeled "Display Name" set to "PBX", and a "Test" button. A "Test" dialog box is open in the foreground, showing a text input field labeled "Receive Email" with the value "test_outlook@grandstream.com" and two buttons: "Cancel" and "Test" (highlighted with a blue border).

Sending Test Email

Supported Devices

Supported Devices
UCM63xx
CloudUCM
SoftwareUCM
GCC (IP-PBX module)
