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.

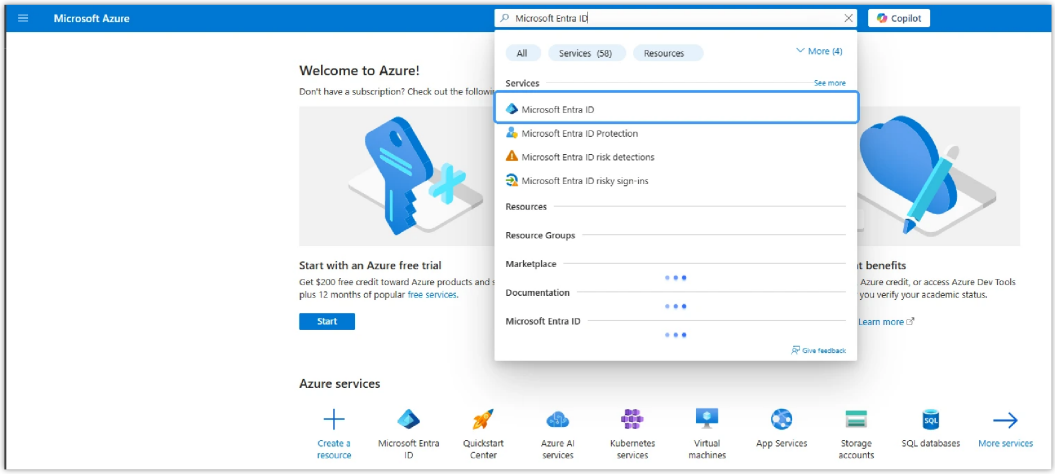
Usage Requirements

- 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

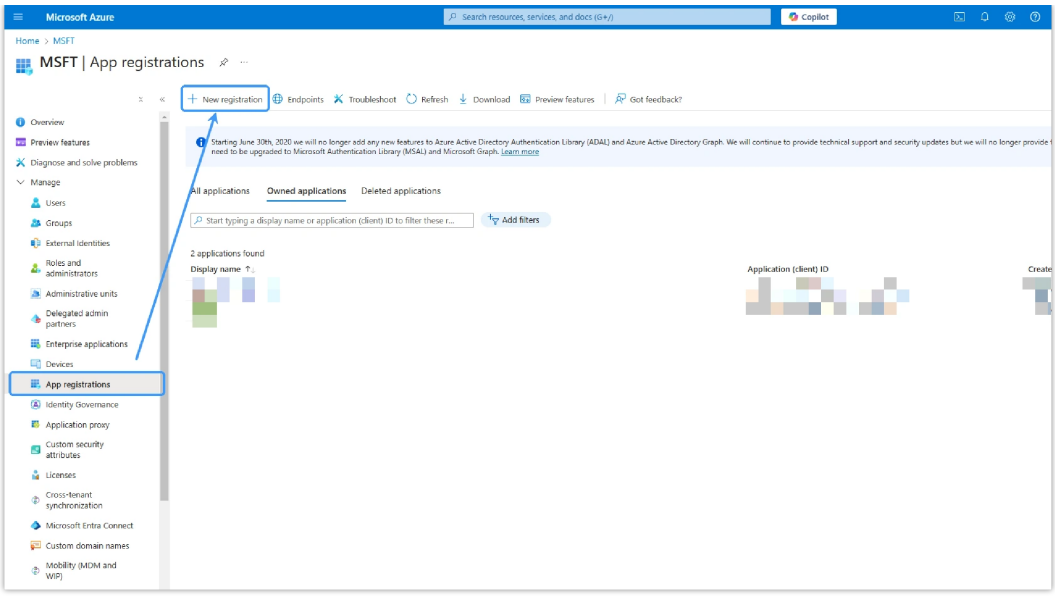
Registering the application with Microsoft Entra ID

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.



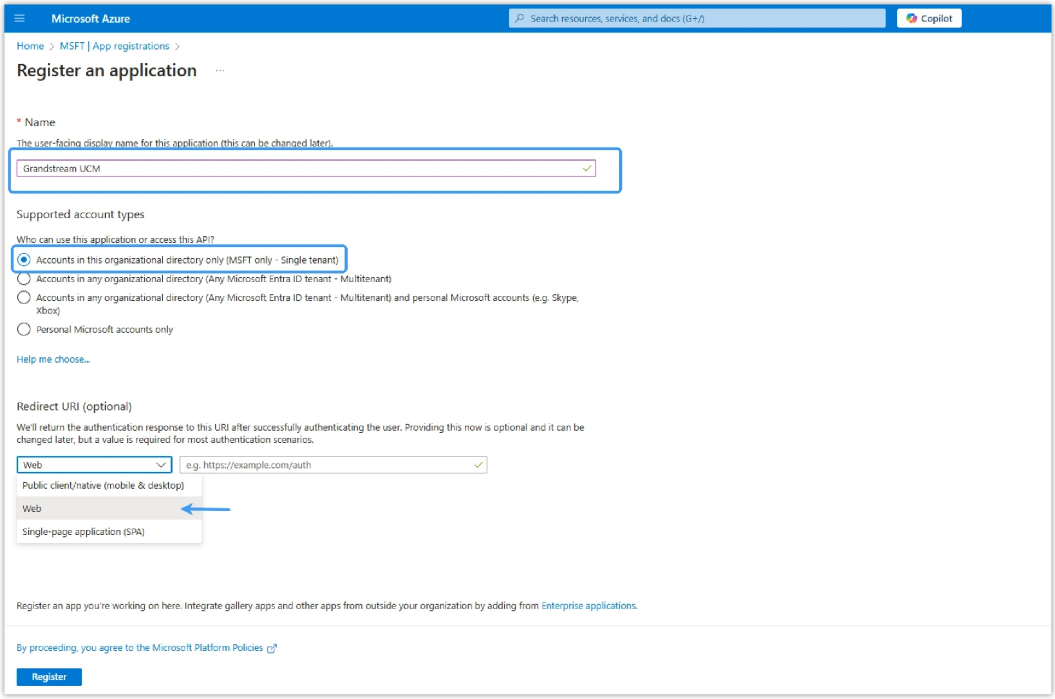
Azure Portal Search

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



Create New Registration

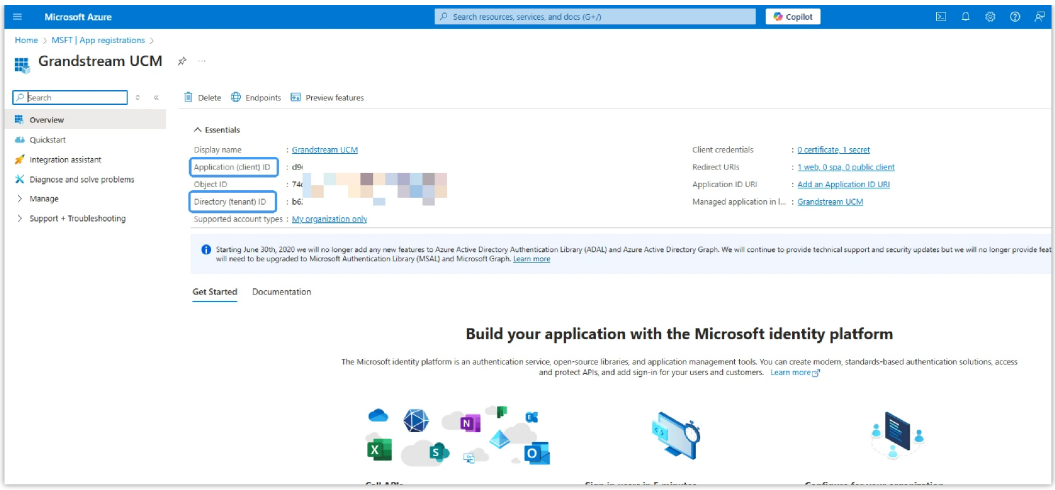
4. On the **App Registration** page, configure the application's registration information based on the table below, and then click **Register.**



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.

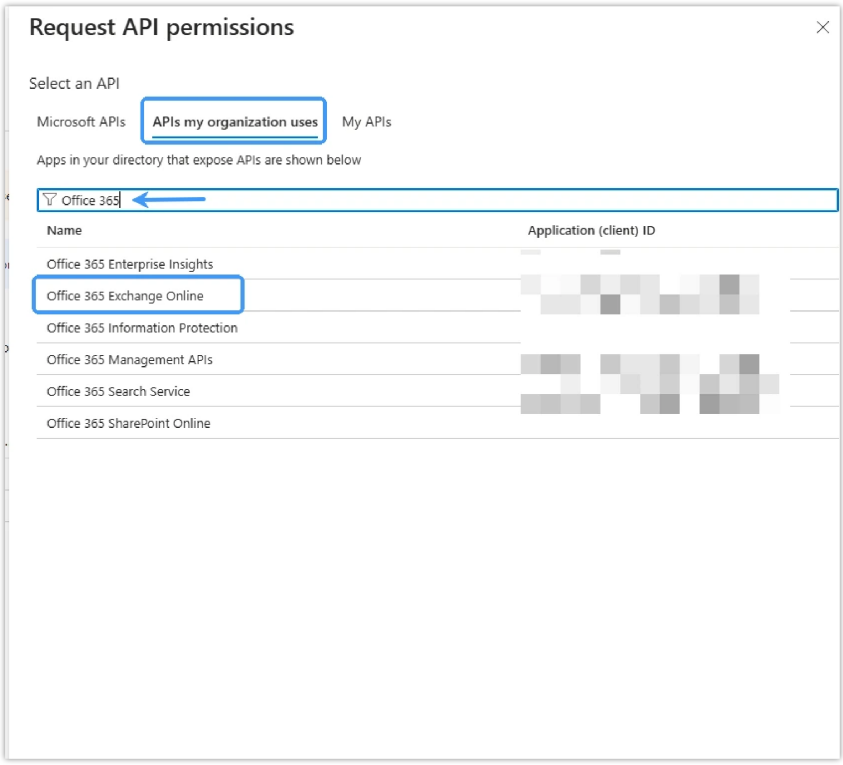
5. After completing the registration, the page will jump to the application's **overview** page. **The application (client) ID** and **directory (tenant) ID** of this application will be needed to fill in the relevant information on the PBX later.



Application Information

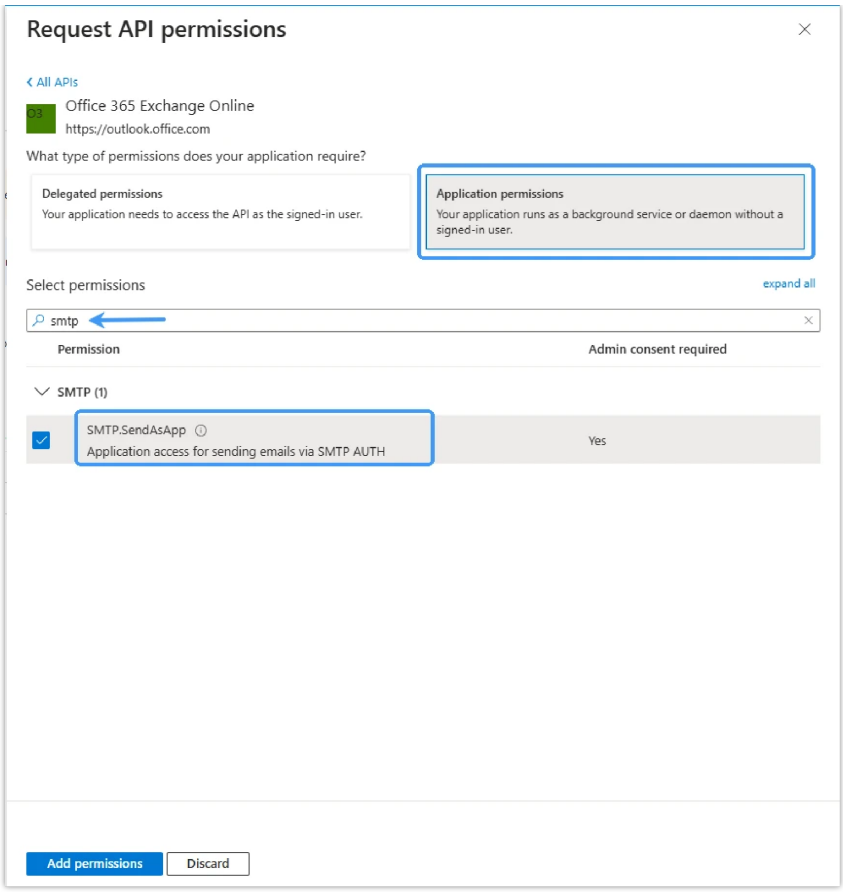
Assigning the Application API Permissions

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



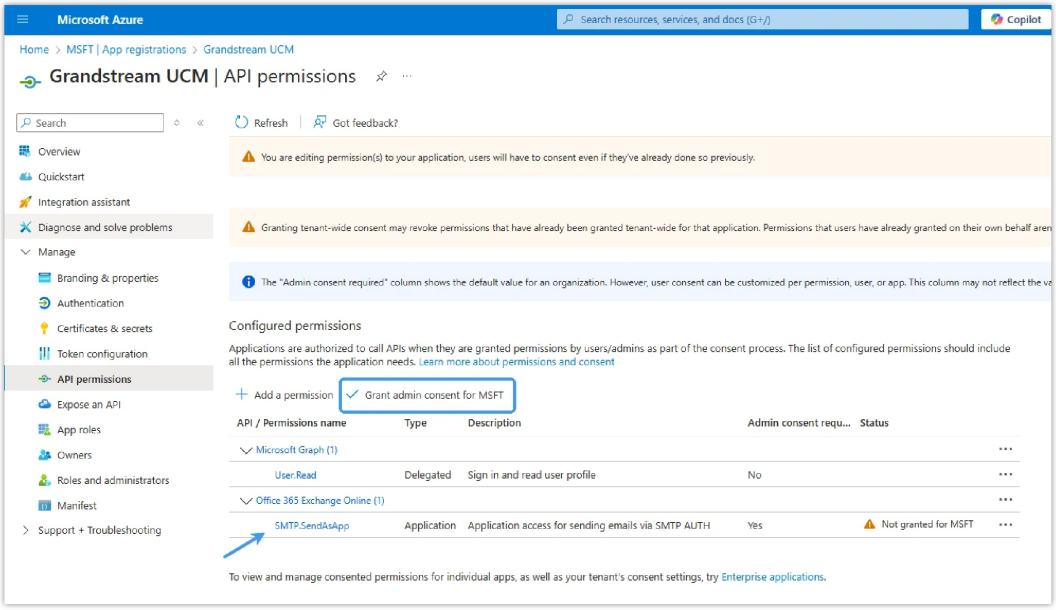
Requesting API Permissions

2. Click **Application Permissions** and search for “SMTP”. Check **SMTP.SendAsApp**.



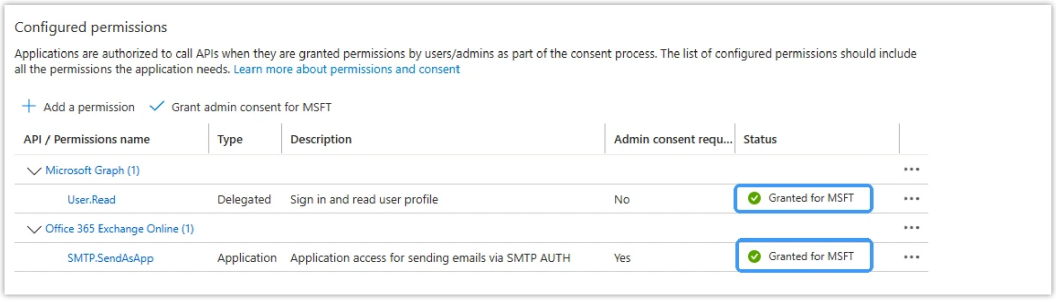
SMTP Permission

3. 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).



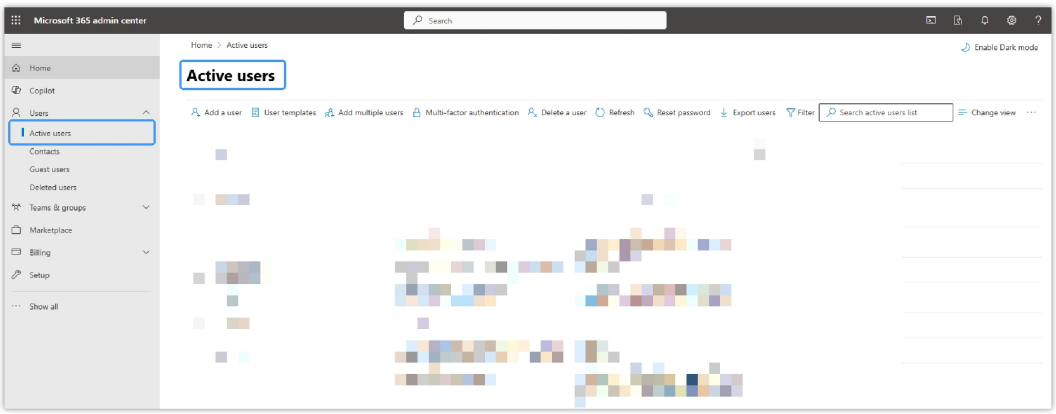
Grant Admin Consent

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



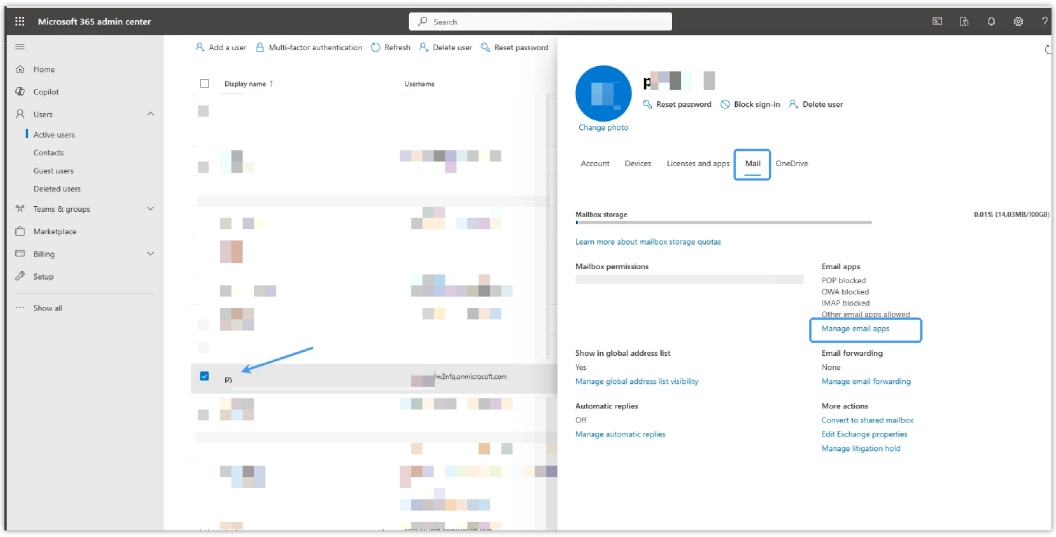
Admin Consent Granted

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.



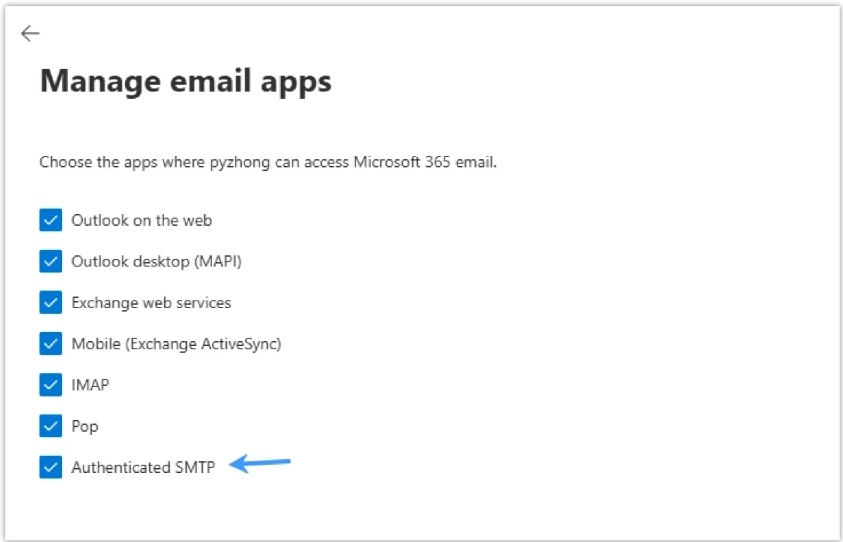
Active Users Page

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



Manage Email Apps

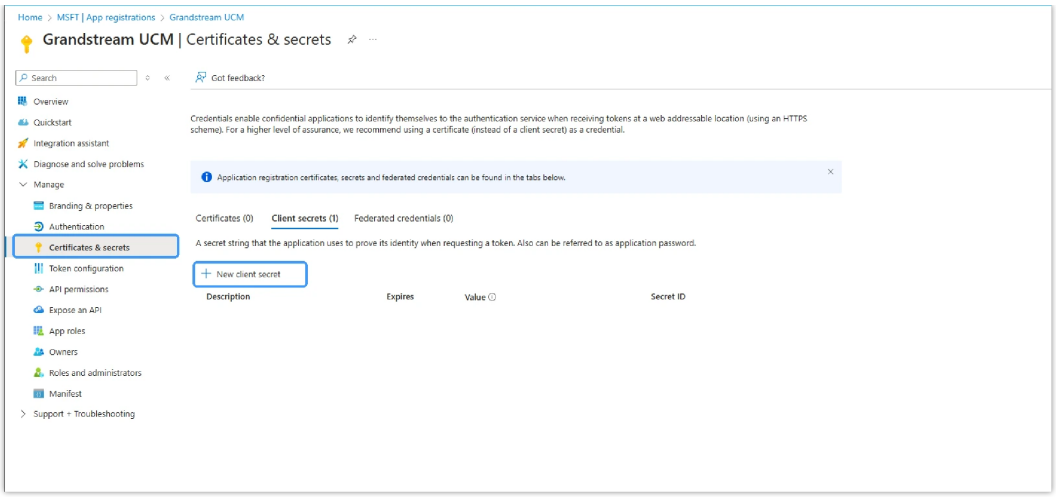
7. Check **Authenticated SMTP** and save to have the authority to log in to the SMTP server and send emails.



Authenticated SMTP

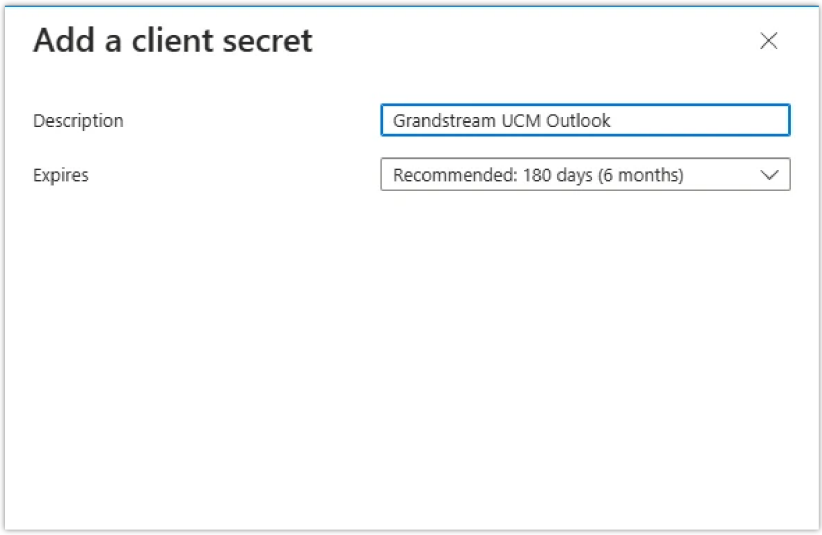
Creating a Client Secret for the Application

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



Certificates & Secrets Page

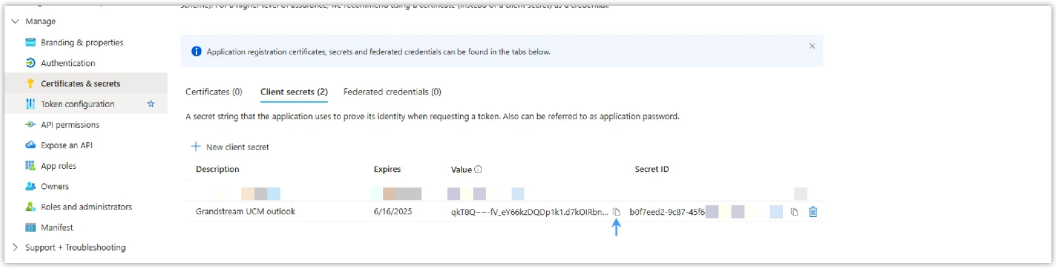
2. Complete the permission settings for the client key and add corresponding instructions.



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.

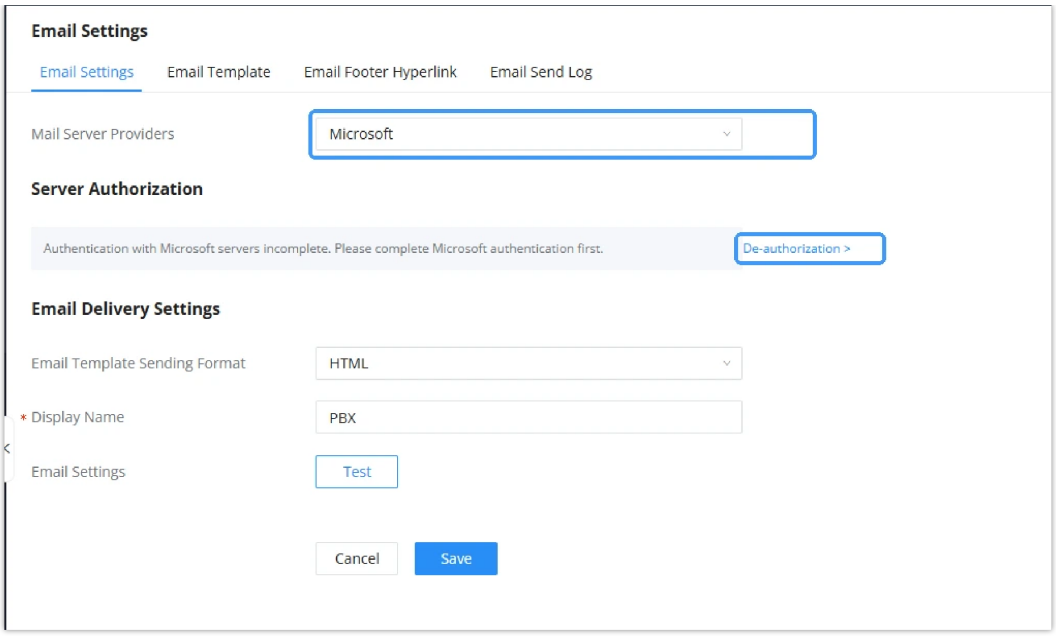
> **Note:**
>
> This information will only be displayed in full when it is created. Please ensure to record this value before leaving this page. Once the page is switched, this value will no longer be displayed publicly.



Client Secret Created

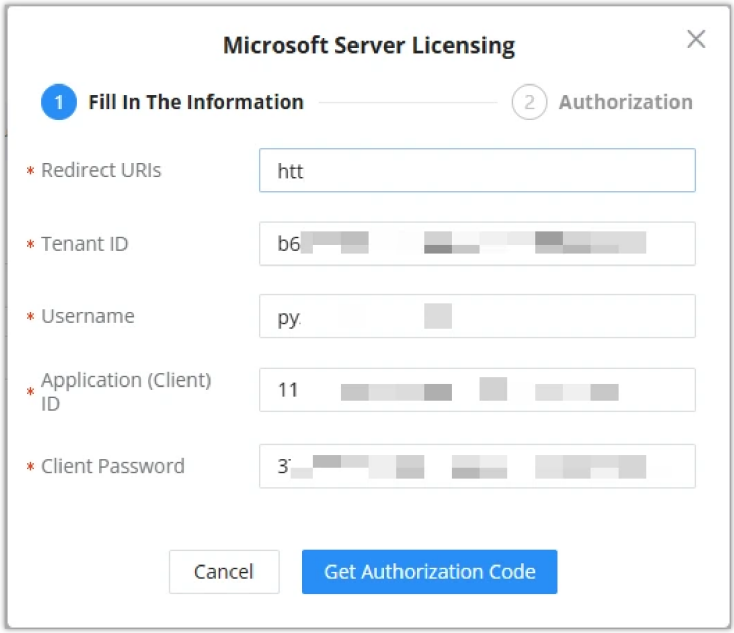
Configuring SMTP-related information on PBX

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**.



PBX Email Settings

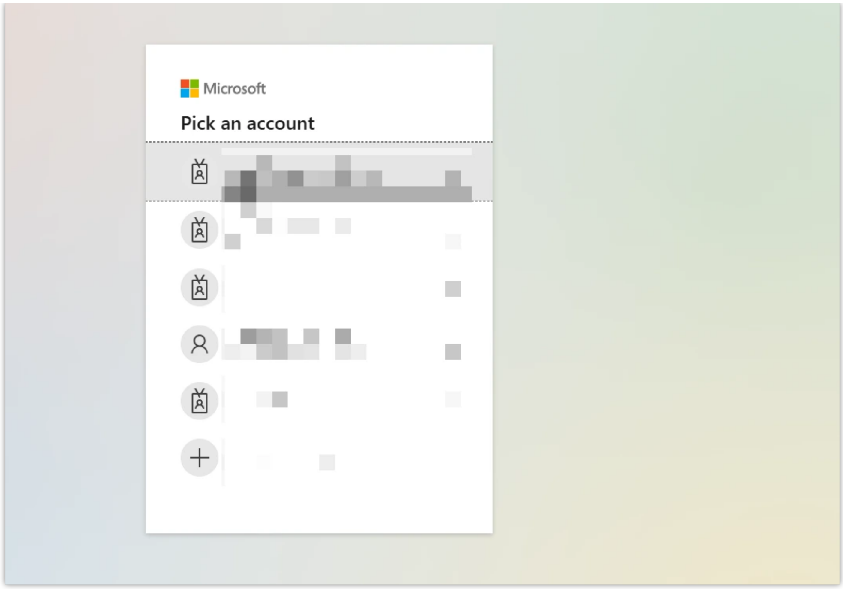
3. Fill in the relevant verification information based on the table below.



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.**



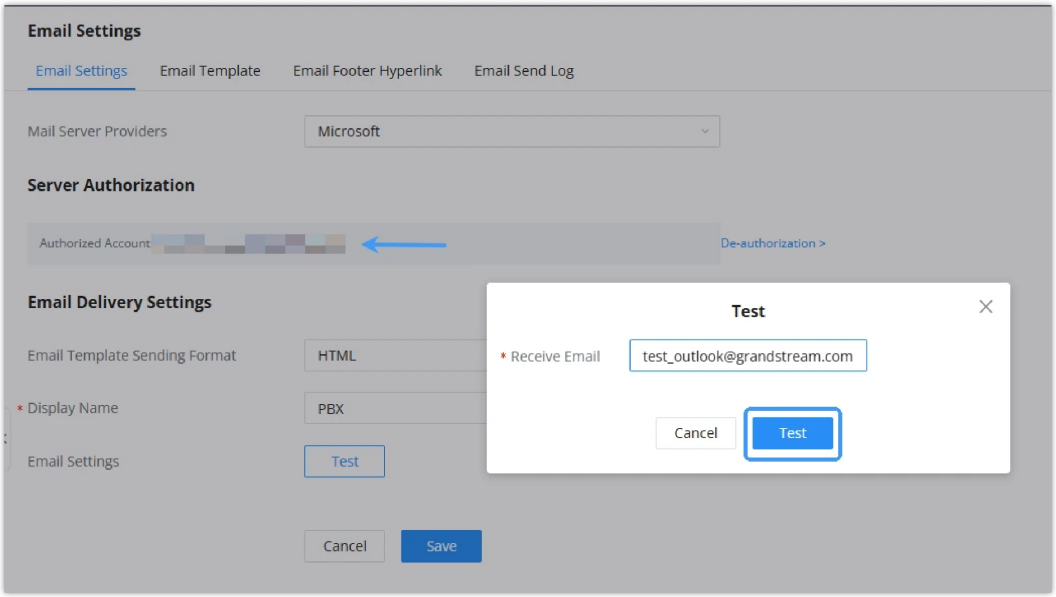
Redirection Login Page

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.

Authorization Code

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

PBX<{your Microsoft account username}>



Sending Test Email

Supported Devices

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