

Grandstream Networks, Inc.

**Microsoft Entra ID (Azure AD) Integration Guide**



This guide provides a comprehensive, step-by-step walkthrough for integrating **Microsoft Entra ID (formerly Azure Active Directory)** with Grandstream's IP PBXs. By enabling this integration, administrators can synchronize Microsoft 365 contacts, configure Single Sign-On (SSO), and streamline user account binding.

This setup is ideal for organizations using Microsoft 365 that want to centralize identity and access control across their communication infrastructure.

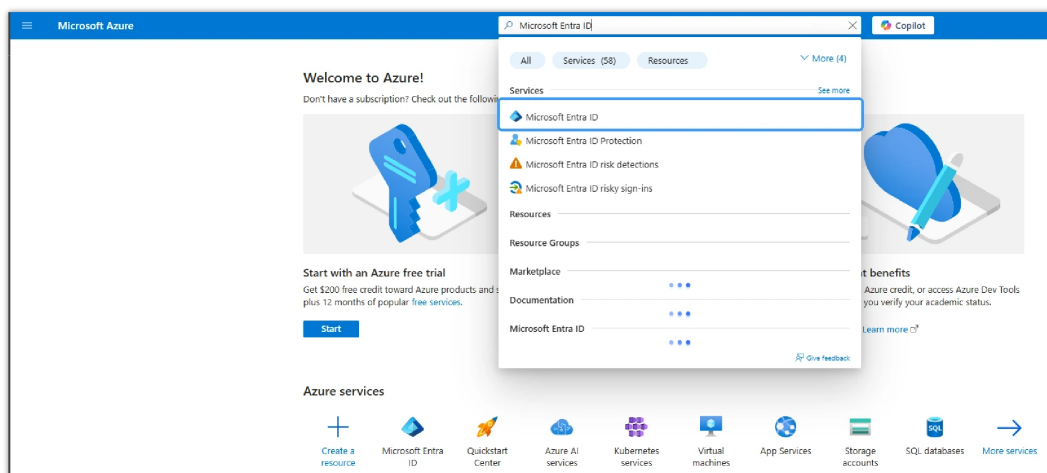
## PREREQUISITES

- Microsoft account with **global administrator permissions**.
- Modern authentication has been enabled in [the Microsoft 365 admin center](#).
- Grandstream PBX running a compatible firmware version (*Refer to the [Supported Models](#)*).

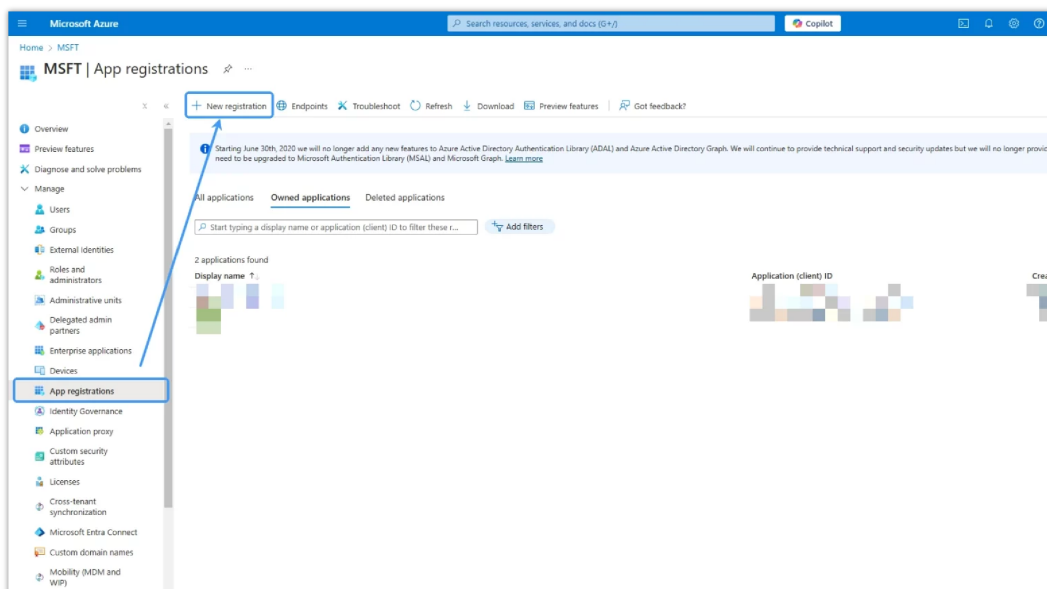
## ENTRA ID CONFIGURATION

### 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.



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



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

Microsoft Azure

Home > MSFT | App registrations >

### Register an application

\* Name

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

Grandstream UCM

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (MSFT only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

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

Public client/native (mobile & desktop)

Web

Single-page application (SPA)

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

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

|                         |                                                                                                                                                                           |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 required to complete the relevant information on the PBX later.

Microsoft Azure

Home > MSFT | App registrations >

### Grandstream UCM

Search resources, services, and docs (G+)

Copilot

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Essentials

Display name : Grandstream UCM

Application (client) ID : d9...

Object ID : 74...

Directory (tenant) ID : b6...

Supported account types : My organization only

Client credentials : 0:certificate:1:secret

Redirect URIs : 1:web:0:spa:0:public:client

Application ID URI : Add an Application ID URI

Managed application in L. : Grandstream UCM

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. You will need to upgrade to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started

Documentation

### Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Get Started

Documentation

## Assigning API Permissions

To enable Microsoft Entra ID user and contact synchronization, the application must be granted both Application permissions and Delegated permissions in Microsoft Graph.

Microsoft Graph uses two permission models:

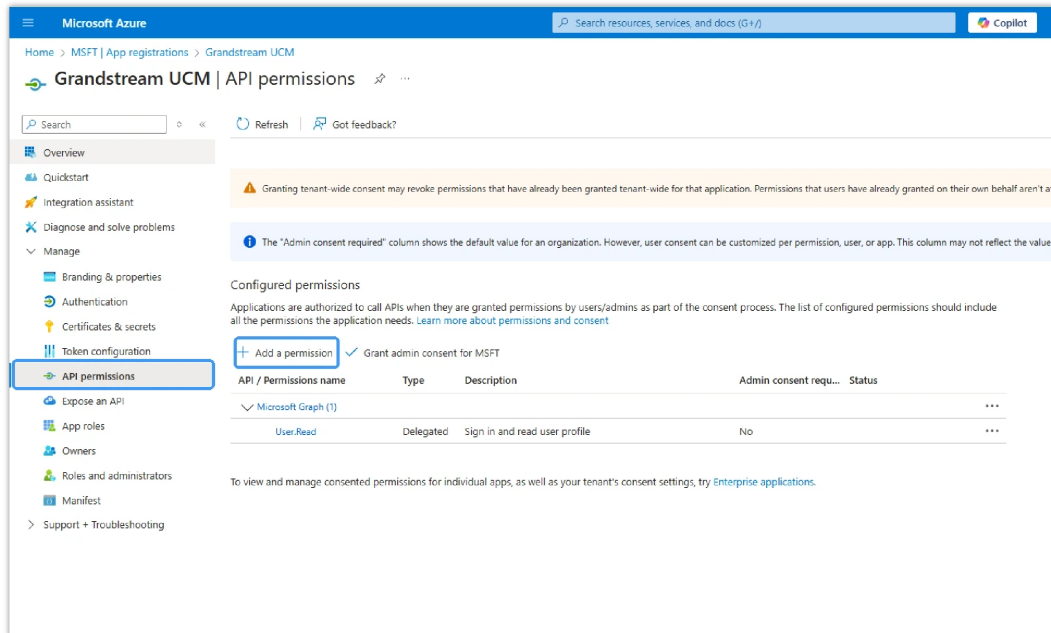
- **Delegated permissions (scopes):** used when the PBX accesses Microsoft Graph on behalf of a signed-in administrator during authorization.

- **Application permissions (app-only / app roles):** used when the PBX accesses Microsoft Graph as a background service, without a signed-in user.

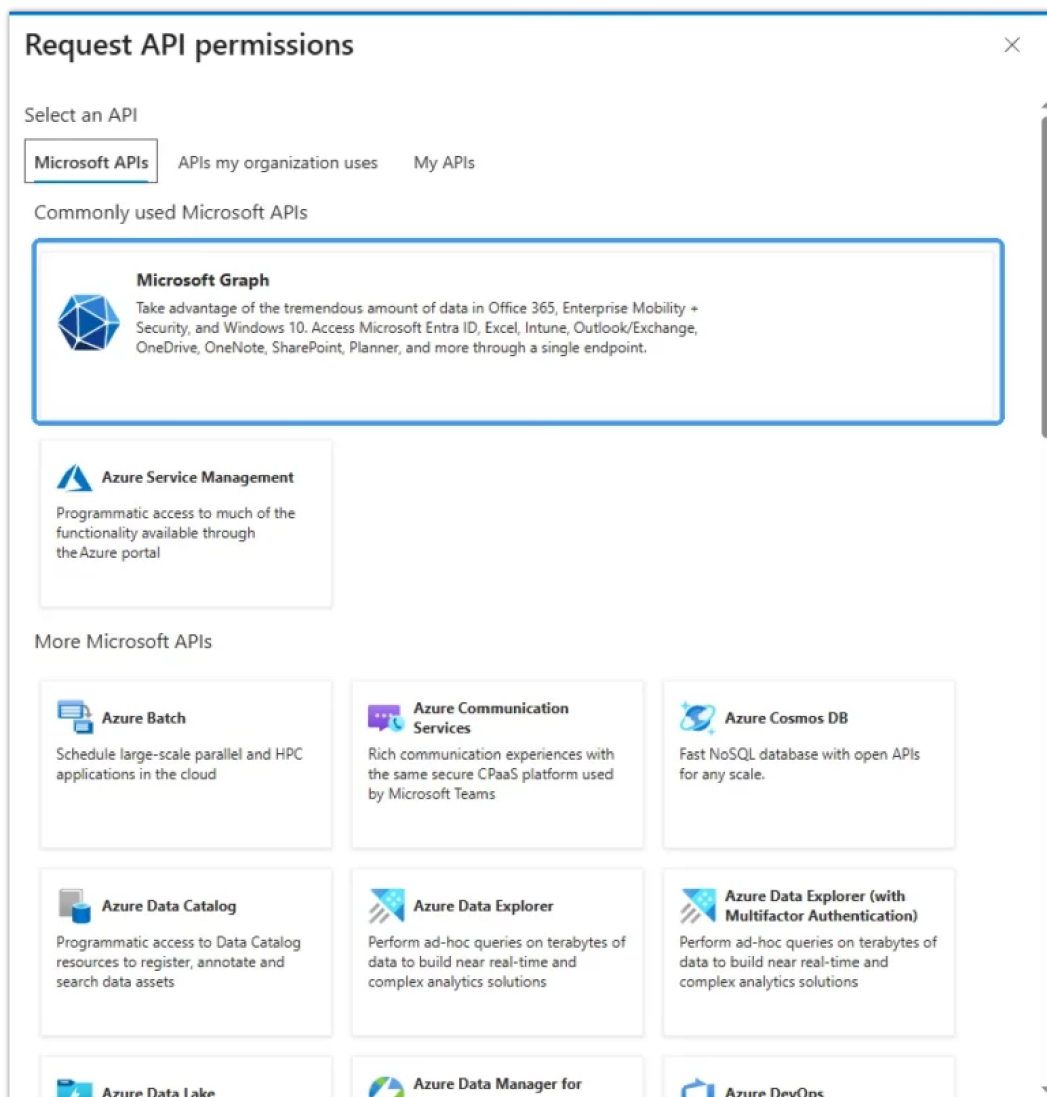
Both permission types are required for this integration because the PBX performs operations that occur during user-authorized access and operations that occur as the service itself during synchronization.

To configure the required permissions, please refer to the steps below:

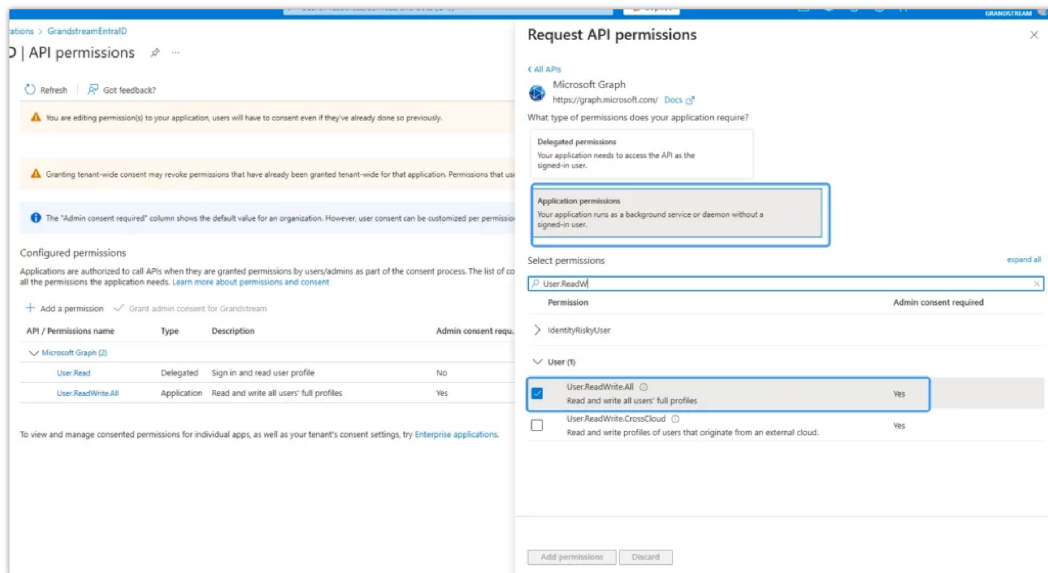
1. In the app's menu, go to **API permissions** → Click **Add a permission**.



2. Select **Microsoft Graph** → Choose **Application permissions**.



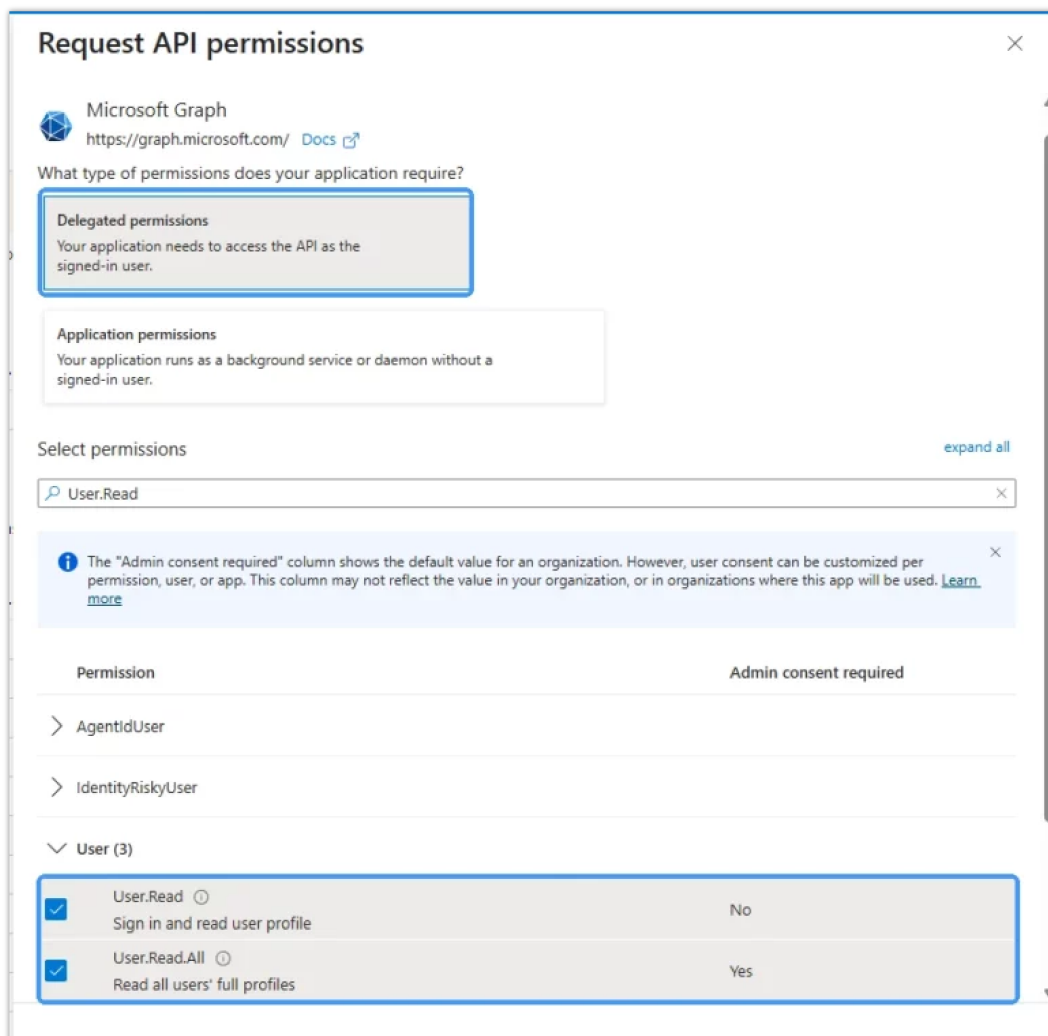
3. Under the application permissions, search for and add: **User.ReadWrite.All**.



4. Choose **Delegated permissions**, and select **"User.Read"** and **"User.Read.All"** under **User**.

**Note:**

Both delegated permissions are required. If either permission is missing or not granted, Microsoft Entra ID contacts cannot be synchronized to the PBX.



5. After adding the permissions, click **Grant admin consent** for the organization (if you're not the **Global Admin**, request approval from one).

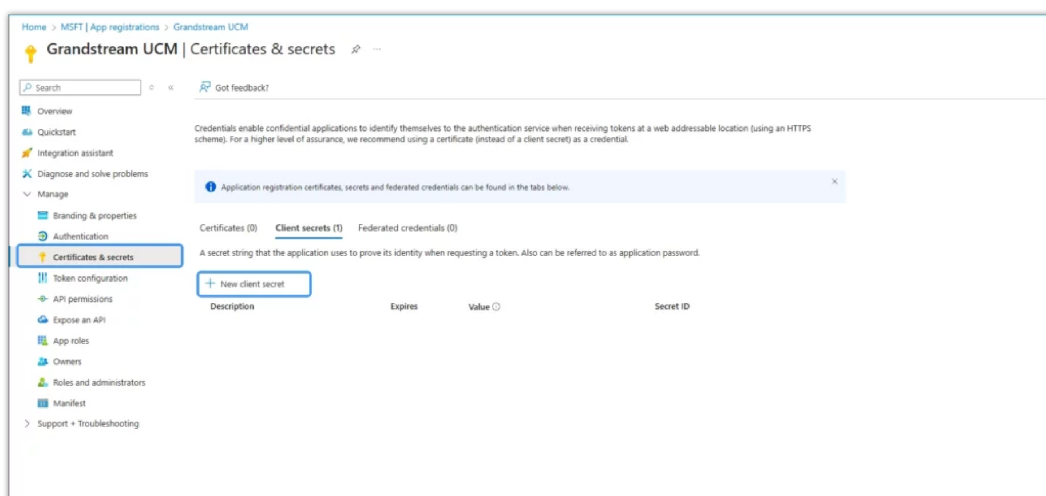
| + Add a permission     |           | ✓ Grant admin consent for abvc          |                       |                        |     |
|------------------------|-----------|-----------------------------------------|-----------------------|------------------------|-----|
| API / Permissions name | Type      | Description                             | Admin consent requ... | Status                 |     |
| Microsoft Graph (3)    |           |                                         |                       |                        |     |
| User.Read              | Delegated | Sign in and read user profile           | No                    | ✓ Granted for abvc     | ... |
| User.Read.All          | Delegated | Read all users' full profiles           | Yes                   | ⚠ Not granted for abvc | ... |
| User.ReadWrite.All     | Delegated | Read and write all users' full profiles | Yes                   | ⚠ Not granted for abvc | ... |

6. Confirm that the permission has been granted for your organization. The status should be **"Granted for [Org]"**.

| + Add a permission     |           | ✓ Grant admin consent for abvc |                       |                    |     |
|------------------------|-----------|--------------------------------|-----------------------|--------------------|-----|
| API / Permissions name | Type      | Description                    | Admin consent requ... | Status             |     |
| Microsoft Graph (2)    |           |                                |                       |                    |     |
| User.Read              | Delegated | Sign in and read user profile  | No                    | ✓ Granted for abvc | ... |
| User.Read.All          | Delegated | Read all users' full profiles  | Yes                   | ✓ Granted for abvc | ... |

## Creating a Client Secret

1. Go to **Certificates & secrets** → Under **Client secrets**, click **New client secret**.



2. Add a **description** and choose the desired expiration time.

Add a client secret

Description

Grandstream UCM

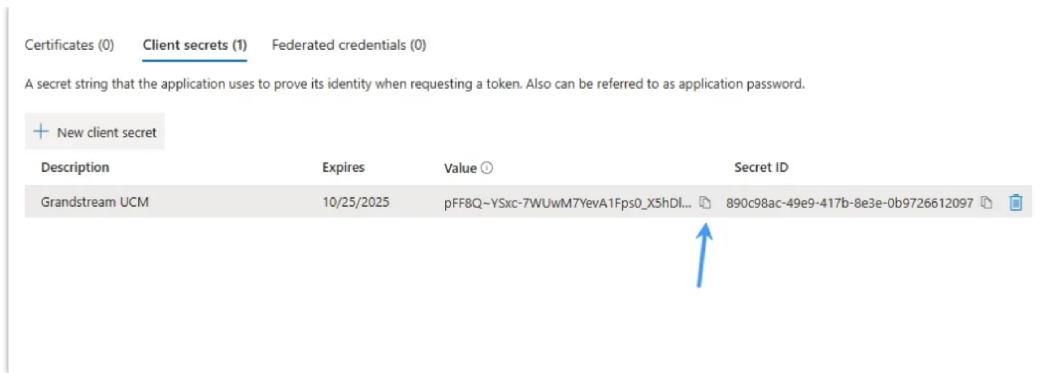
Expires

Recommended: 180 days (6 months)

3. Click **Add** and **copy** the generated **client secret value**.

### Important!

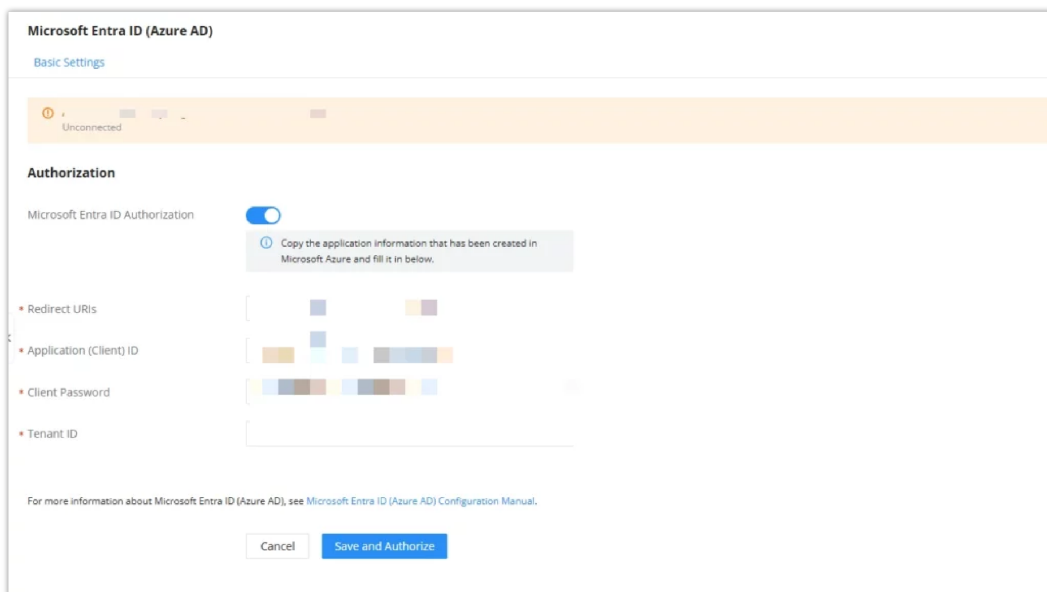
Save the client secret value now, as it will not be visible again once you leave the page.



## IP PBX CONFIGURATION

After creating and configuring your app in Azure, log in to your PBX system to input the required data.

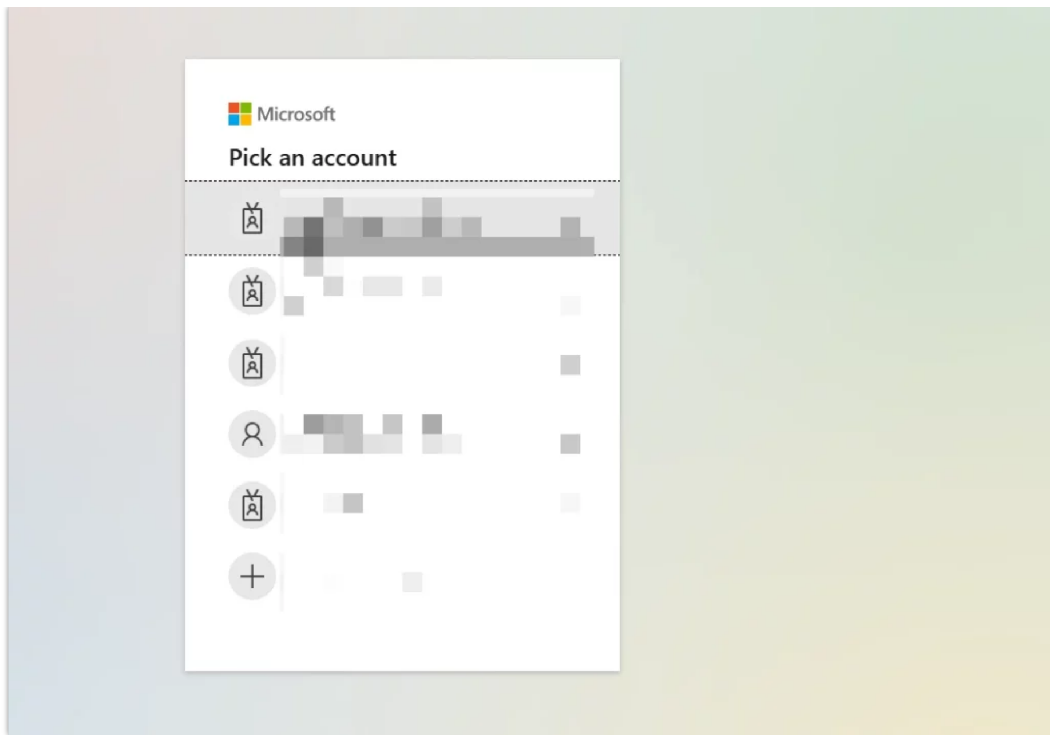
1. Log into the Web UI and navigate to **Integrations** → **Microsoft Entra ID (Azure AD)**.



2. Fill in the following fields:

|                                |                                                                            |
|--------------------------------|----------------------------------------------------------------------------|
| <b>Redirect URI</b>            | This should be the same redirect URI as the one used in Azure registration |
| <b>Tenant ID</b>               | Paste your <b>Directory (Tenant) ID</b>                                    |
| <b>Application (Client) ID</b> | Paste your <b>Client ID</b>                                                |
| <b>Client Password</b>         | Paste the saved <b>Client Secret</b> .                                     |

3. Click **"Save and Authorize"**. A new browser window will open, prompting you to sign in with your Microsoft Global Administrator account. Upon successful authentication, an authorization token will be sent to the configured redirect URI.



4. Copy the **token** received, paste it into the window prompt, and click **Authorization**.

A screenshot of the "Microsoft Server Licensing" window. The window has a title bar with a close button. Below the title bar, there are two steps: "1 Fill In The Information" and "2 Authorization". The "2 Authorization" step is currently active. Below the steps, there is a text box with 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 text box, there is a label "\* Authorization Code" and a text input field containing a blurred authorization code. At the bottom, there are two buttons: "Previous" and "Authorization". The "Authorization" button is highlighted with a blue border.

5. Once authorized, click **Save** to apply changes.

**Note:**

Any change to API permissions in Microsoft Entra ID **requires the application to be re-authorized** in the PBX Web UI. The authorization process must be completed again before synchronization can succeed.

## INTEGRATION FEATURES

This section describes the key features available after successful integration of Microsoft Entra ID with the Grandstream PBX systems.

### Synchronizing Microsoft Users/Extensions

Enables the PBX to retrieve and display Entra ID user information in the local contact list.

- **Get Microsoft Users:** Enables the PBX to retrieve contacts from Microsoft Entra ID, store them locally, and display them in the list.
- **User Range:** Controls whether to retrieve all Microsoft users or specify a user type.

- **User Type:** Defines which Entra user types (e.g., Members, Guest) will be retrieved. Only selected types are synchronized.
- **Add Users to LDAP:** Adds the synchronized Entra ID users to the PBX LDAP phonebooks, making them available to LDAP-enabled devices.

The screenshot shows the 'User Settings' tab for 'Microsoft User'. It includes a toggle for 'Get Microsoft User' which is turned on. Below it is an informational note: 'When enabled, Microsoft users can be associated one-to-one with system users/extensions in UCM.' There is a 'User Range' dropdown set to 'Specify Type User'. The 'User Type' section shows 'Guest' and 'Members' selected. At the bottom, the 'Add User to LDAP' toggle is also turned on.

Once LDAP synchronization is enabled, the synchronized Microsoft Entra ID contacts will be accessible via the PBX LDAP directory path: **ou=microsoft,dc=pbx,dc=com**.

The screenshot shows the 'LDAP Phonebook' configuration page. It contains a table of phonebook entries. The entry 'ou=microsoft,dc=pbx,dc=com' is highlighted with a red box. The table has columns for 'Phonebook DN' and 'Options'. At the bottom right, there is a pagination control showing 'Total: 3' and '10 / page'.

## Associated User Settings

The screenshot shows the 'Associated User Settings' configuration page for 'Microsoft Entra ID (Azure AD)'. It includes a toggle for 'Associated UCM' which is turned on, with a note: 'After enabled, the associated UCM user's information (first name, last name, email address, mobile phone, job title) will be overwritten by Microsoft user information.' The 'Association Mode' is set to 'Automatic Association'. The 'Associated User Range' dropdown is set to 'Specify Type User'. The 'Associated User Type' section shows 'Guest' and 'Members' selected. The 'Association Policy' dropdown is set to 'Automatic Allocation'. The 'Starting Extension' is set to '4000'. At the bottom, there are 'Cancel' and 'Save' buttons.

- **Associated UCM** (Field may vary by PBX model): After checking this option, you can bind Microsoft users to PBX extensions/users to form an alternative management method.
- **Association Mode:** allows choosing automatic association or manual association.

- **Manual association** requires users to bind users/extensions themselves by clicking **Bind** in the user list.

×

Edit Associated User

Microsoft User

Username: gstest@grandstr... Display Name: gstest

FirstName: Last Name:

Associate UCM User ☒

\* UCM User

4003

▼

Cancel

Save

- **Automatic association** involves many configuration items:
  1. **Associated user range:** refers to the scope of binding, specifying which Microsoft Entra ID users are eligible for binding. This can include all users, guests, or members.
  2. **Association Policy:** Defines how the PBX assigns extensions to Microsoft Entra ID users during automatic association.
    - **Auto Allocation** assigns extensions sequentially, starting from a specified base number.
    - **Read the Specified Property Value** uses a chosen Entra ID attribute (e.g., *mobilePhone* or *businessPhone*) to determine the extension or match it to an existing PBX user, enabling precise user binding based on existing directory data.

Extensions and users that are successfully bound to Microsoft Entra ID accounts will be marked with a Microsoft logo icon in the PBX interface, making them easily identifiable.

| User Management                         |                                             |                                            |                                                                                                                                                                             |
|-----------------------------------------|---------------------------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">System User Information</a> | <a href="#">User Portal/Wave Privileges</a> | <a href="#">Extension Login Management</a> | <a href="#">User Endpoint Access History</a>                                                                                                                                |
| Username                                | Privilege                                   | Last Operation Time                        | Options                                                                                                                                                                     |
| John                                    | Administrator                               | 2025-05-20 11:12:09                        |   |

## Microsoft User List

Displays the list of synchronized Entra ID users and allows manual or automatic association management.

- o The **Sync Now** button means that a synchronization will be performed immediately. If binding information is set, rebinding will also be performed.

| Sync Now            |                | Sync Settings |             |             |         |                 |                  |             |                      |                   |
|---------------------|----------------|---------------|-------------|-------------|---------|-----------------|------------------|-------------|----------------------|-------------------|
| Username ↕          | Display Name ↕ | FirstName ↕   | Last Name ↕ | Job Title ↕ | Email ↕ | Mobile Number ↕ | Business Phone ↕ | User Type ↕ | Associate UCM User ↕ | Options           |
| user1@grandstrea... | User1          |               |             |             |         | 3024            |                  | Members     | 1001                 | <a href="#">↗</a> |
| user2@grandstrea... | User2          |               |             |             |         | 3021            |                  | Members     |                      | <a href="#">↗</a> |
| user3@grandstrea... | User3          |               |             |             |         | 3022            |                  | Members     |                      | <a href="#">↗</a> |
| user4@grandstrea... | User4          |               |             |             |         | 1001            |                  | Members     | 4000                 | <a href="#">↗</a> |
| user5@grandstrea... | User5          |               |             |             |         | 111111          |                  | Members     | 4001                 | <a href="#">↗</a> |
| user6@grandstrea... | User6          |               |             |             |         |                 |                  | Members     | 4002                 | <a href="#">↗</a> |
| user7@grandstrea... | User7          |               |             |             |         |                 |                  | Members     | John                 | <a href="#">↗</a> |
| user8@grandstrea... | User8          |               |             |             |         |                 |                  | Members     | 4003                 | <a href="#">↗</a> |
| user9@grandstrea... | User9          |               |             |             |         |                 |                  | Guest       |                      | <a href="#">↗</a> |
| user10@grandstre... | User10         |               |             |             |         |                 |                  | Guest       | 4004                 | <a href="#">↗</a> |

- **Sync Settings:** allows the configuration of the following synchronization settings:
  - **Automatically delete extensions:** When the selected scenarios occur during synchronization, the bound extensions will be automatically deleted.
  - **Automatic Sync:** Allows administrators to set a schedule for recurring user synchronization.

**Microsoft Entra ID (Azure AD) > Sync Settings**

**Extensions**

Automatically Delete Extensions ☒ When The Associated User Is disabled In The Microsoft Entra ID

☒ When The Associated User Is delete In The Microsoft Entra ID

☒ When the user is no longer associated with the UCM extension

**Microsoft User Data Synchronization**

*Data synchronization includes obtaining the latest Microsoft users and updating the association between Microsoft users and UCM extension/system users. The synchronization process may affect the efficiency of equipment usage. It is recommended to carry it out during non-office hours.*

Timed automatic synchronization ☒

Sync Time By Day 3

Cancel Save

- **Synchronous Record:** Keeps a log of all synchronization activities for auditing and troubleshooting purposes.

| Synchronous Record  |                        |         |         |
|---------------------|------------------------|---------|---------|
| Sync Time           | Synchronization Mode   | Results | Options |
| 2025-05-09 15:23:11 | Manual synchronization | Success | ⓘ       |
| 2025-05-09 15:17:27 | Manual synchronization | Success | ⓘ       |
| 2025-05-09 15:07:50 | Manual synchronization | Failed  | ⓘ       |

## Single Sign-On (SSO)

Allows users to log in to the PBX system using their Microsoft Entra ID credentials.

**Microsoft Entra ID (Azure AD)**

Basic Settings User Settings Single Sign-on (SSO)

Single Sign-on (SSO) ☒

*When enabled, extensions/users can log in to Wave/UCM using the associated Microsoft account.*

SSO Redirect Address Intranet Address: <https://192.168.129.109:8089/login>

*Add the above address to the Microsoft Entra ID application before using SSO.*

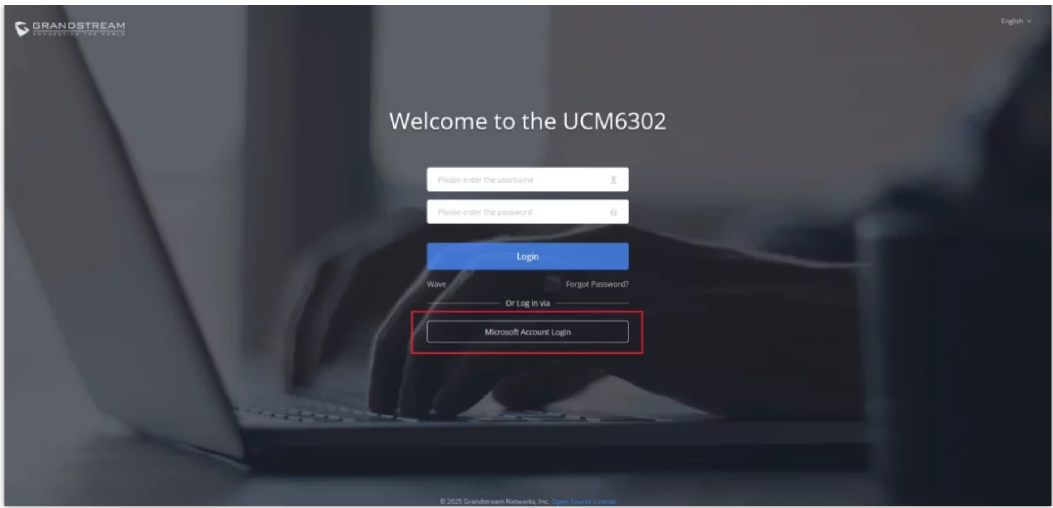
Cancel Save

After enabling SSO (Single Sign-On), users must add the PBX SSO redirect URI to the list of redirect URIs in the Microsoft Entra ID application settings to complete the configuration.

### Note:

SSO cannot be activated unless at least one Microsoft Entra ID user is successfully bound to a PBX user account.

Once SSO is successfully configured, a Microsoft login option will appear on the PBX login page, allowing users to authenticate using their Microsoft Entra ID credentials.



# SUPPORTED MODELS

| Supported Devices | Firmware Version |
|-------------------|------------------|
| UCM6300/A Series  | 1.0.29.6+        |
| CloudUCM          | 1.0.29.7+        |
| SoftwareUCM       | 1.0.33.7+        |