

Azure Active Directory Integration Guide

Yeastar P-Series Appliance Edition

Version: 1.0

Date: 2023-11-29



Contents

| | |
|--|-----------|
| Overview..... | 1 |
| Set up Azure Active Directory Integration..... | 3 |
| Integrate Yeastar P-Series PBX System with Azure Active Directory..... | 3 |
| Synchronize Azure AD Users to Yeastar P-Series PBX System..... | 15 |
| Synchronize Azure AD Groups to Yeastar P-Series PBX System..... | 20 |
| Synchronize Microsoft Outlook Contacts to Yeastar P-Series PBX System..... | 22 |
| Enable Microsoft Teams User Presence Synchronization..... | 29 |
| Allow Users to Log in to Linkus UC Clients with SSO..... | 30 |
| Manage Azure Active Directory Integration..... | 33 |
| Schedule Automatic Directory Synchronization..... | 33 |
| Manually Perform a Directory Synchronization..... | 34 |
| Update Client Secret for Azure Active Directory Integration..... | 34 |
| Pause Azure Active Directory Synchronization..... | 35 |
| Disable Azure Active Directory Integration..... | 38 |
| Disconnect Azure Active Directory Integration..... | 39 |

Azure Active Directory Integration Guide

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. By integrating Yeastar P-Series PBX System with Azure Active Directory, you can synchronize the Azure AD users and groups to PBX, and allow the synced Azure AD users to securely log in to Linkus UC Clients with Single Sign-on (SSO) by their Microsoft accounts.

Requirements

- **Azure Active Directory Edition:** Free, Office 365 apps, Premium P1, or Premium P2
- **PBX Server:**
 - **Firmware:** Version 37.8.0.25 or later



Important:

Outlook contacts synchronization and **Teams user presence synchronization** are only available for version 37.10.0.30 or later.

- **Plan:** Enterprise Plan (EP) or Ultimate Plan (UP)

Key features

The integration of Yeastar P-Series PBX System and Azure Active Directory provides the following key features:

User and group synchronization

The integration provides one-way synchronization, mapping your Azure AD users and groups to PBX's directory. Changes made on the synced users and groups within the Azure Active Directory will be automatically updated to PBX, thus implementing automated administration.

Auto extension assignment for Azure AD users

PBX automatically creates and assigns extensions for the synced Azure AD users, via which the users can utilize the unified communications features of the PBX.

Single Sign-on (SSO)

PBX supports a secure Single Sign-on (SSO) feature, allowing the synced Azure AD users to securely log in to Linkus Web Client and Mobile Client by their Microsoft accounts.

Outlook contacts synchronization

One-way Synchronization of Outlook contacts to PBX and Linkus clients, including personal Outlook contacts and shared contacts from Outlook shared mailboxes.

Teams user presence synchronization

Automatically synchronize Azure AD users' Teams user presence to their PBX extension presence.

Objectives

This integration guide provides detailed instructions on how to configure and manage Azure Active Directory integration.

Set up Azure Active Directory integration

- [Integrate Yeastar P-Series PBX System with Azure Active Directory](#)
- [Synchronize Azure AD Users to Yeastar P-Series PBX System](#)
- [Synchronize Azure AD Groups to Yeastar P-Series PBX System](#)
- [Synchronize Microsoft Outlook Contacts to Yeastar P-Series PBX System](#)
- [Enable Microsoft Teams User Presence Synchronization](#)
- [Allow Users to Log in to Linkus UC Clients with SSO](#)

Manage Azure Active Directory integration

- [Schedule Automatic Directory Synchronization](#)
- [Manually Perform a Directory Synchronization](#)
- [Update Client Secret for Azure Active Directory Integration](#)
- [Pause Azure Active Directory Synchronization](#)
- [Disable Azure Active Directory Integration](#)
- [Disconnect Azure Active Directory Integration](#)

Set up Azure Active Directory Integration

Integrate Yeastar P-Series PBX System with Azure Active Directory

This topic describes how to integrate Yeastar P-Series PBX System with Azure Active Directory (Azure AD).

Requirements

- **Azure Active Directory Edition:** Free, Office 365 apps, Premium P1, or Premium P2
- **PBX Server:**
 - **Firmware:** Version 37.8.0.25 or later
 - **Plan:** Enterprise Plan (EP) or Ultimate Plan (UP)

Prerequisites

Before you begin, make sure the followings are ready:

- Your organization already has an Azure Active Directory tenant.
- Use a Microsoft Azure account with **Global Administrator** privilege to implement the integration.
- You have [configured network for remote access by a Yeastar FQDN](#)

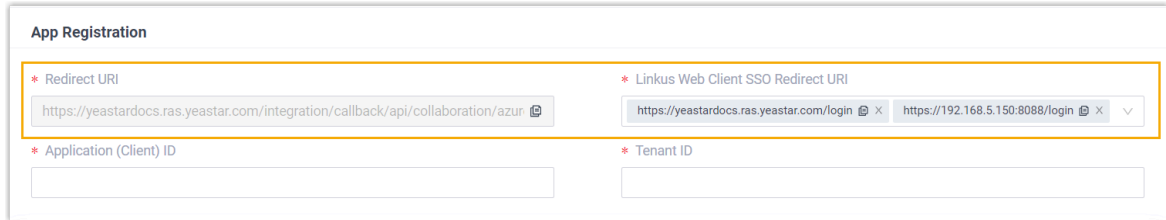
Procedure

- [Step1. Obtain redirect URIs from PBX](#)
- [Step2. Register an application in Azure AD tenant](#)
- [Step3. \(Optional\) Add SSO redirect URI to the Azure AD application](#)
- [Step4. Grant permissions to the Azure AD application](#)
- [Step5. Generate a client secret for the Azure AD application](#)
- [Step6. Connect PBX and Azure AD](#)

Step1. Obtain redirect URIs from PBX

Obtain redirect URIs from Yeastar P-Series PBX System, you will need the information when configuring an Azure AD application for the integration.

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. Click **Integrate** beside the **Microsoft 365**.
3. In the **App Registration** section, take note of the following redirect URIs.

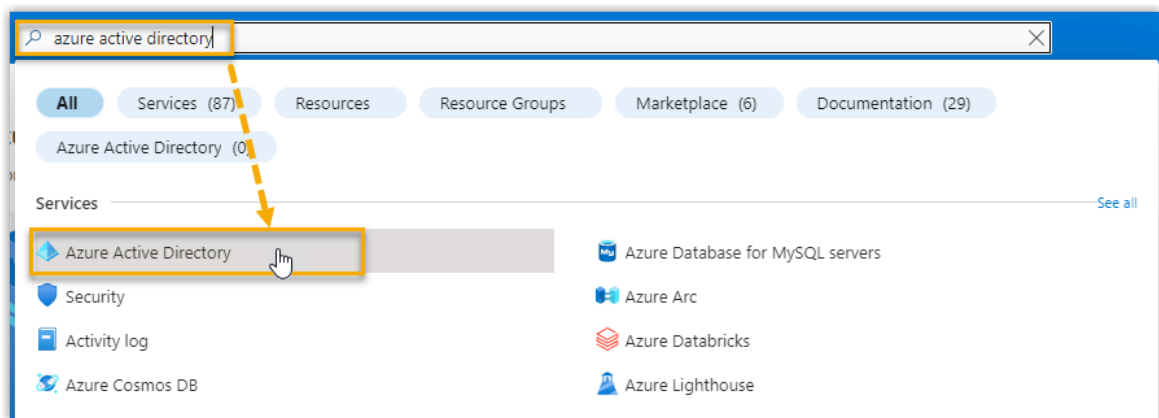


- **Redirect URI:** Used to specify the location to which you are redirected after the integration authentication is completed.
- **Linkus Web Client SSO Redirect URI:** Used to set up the Single Sign-on (SSO) feature of Linkus Web Client.

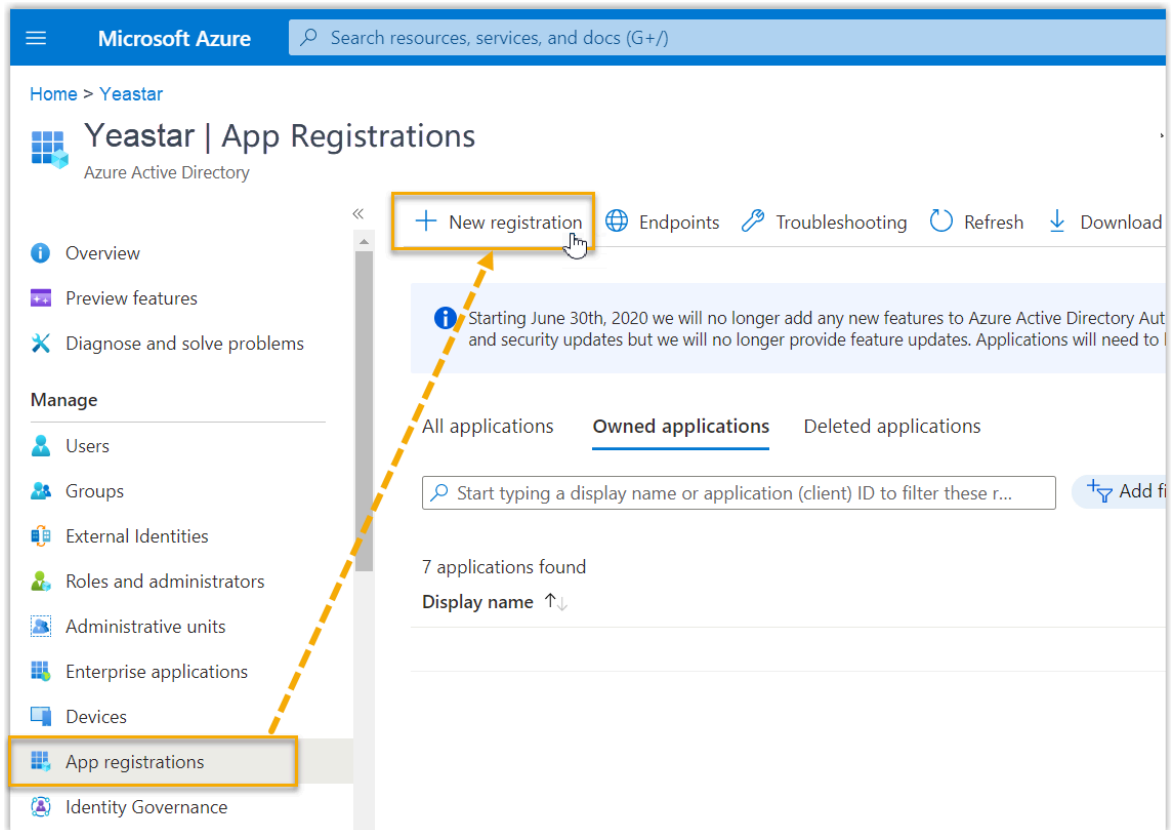
Step2. Register an application in Azure AD tenant

Register an Azure AD application that will be used to connect Yeastar P-Series PBX System and Azure AD.

1. Log in to [Microsoft Azure Portal](#) with the Microsoft Azure Global Administrator account.
2. In the search bar, search and select **Azure Active Directory** service to enter your organization's directory.



3. On the left navigation bar of organization's directory, go to **App registrations**, then click **New registration**.



4. In the **Register an application** page, do as follows:

Microsoft Azure

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

Home > Yeastar | App registrations

Register an application

*** Name**

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

Yeastar_P_series_PBX ✓

Supported account types

Who can use this application or access this API?

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

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - 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.

Select a platform ▼

Public client/native (mobile & desktop)

Web

Single-page application (SPA)

https://yeastardocs.ras.yeastar.com/integration/callback/api/collabor...

[Enterprise applications](#)

[Platform Policies](#)

Register

- a. Enter the registration information of the application.
 - **Name:** Specify a name to help you identify the application.
 - **Supported account types:** Select **Accounts in this organizational directory only**.
 - **Redirect URI:** In the **Select a platform** drop-down list, select **Web**, then paste the [Redirect URI](#) obtained from the PBX.
- b. Click **Register**.

An Azure AD application is registered successfully.

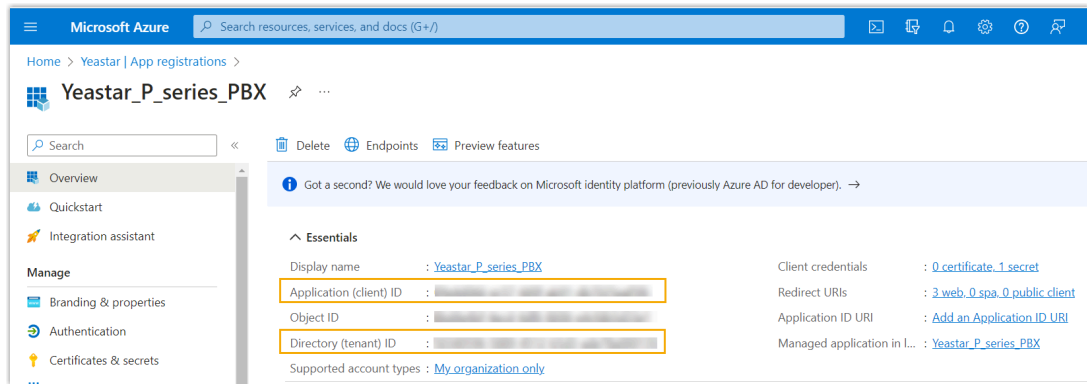
The **Application (client) ID** and **Directory (tenant) ID** of the application is displayed on the **Overview** page. Note them down as you will need to fill them into the PBX later.



Note:



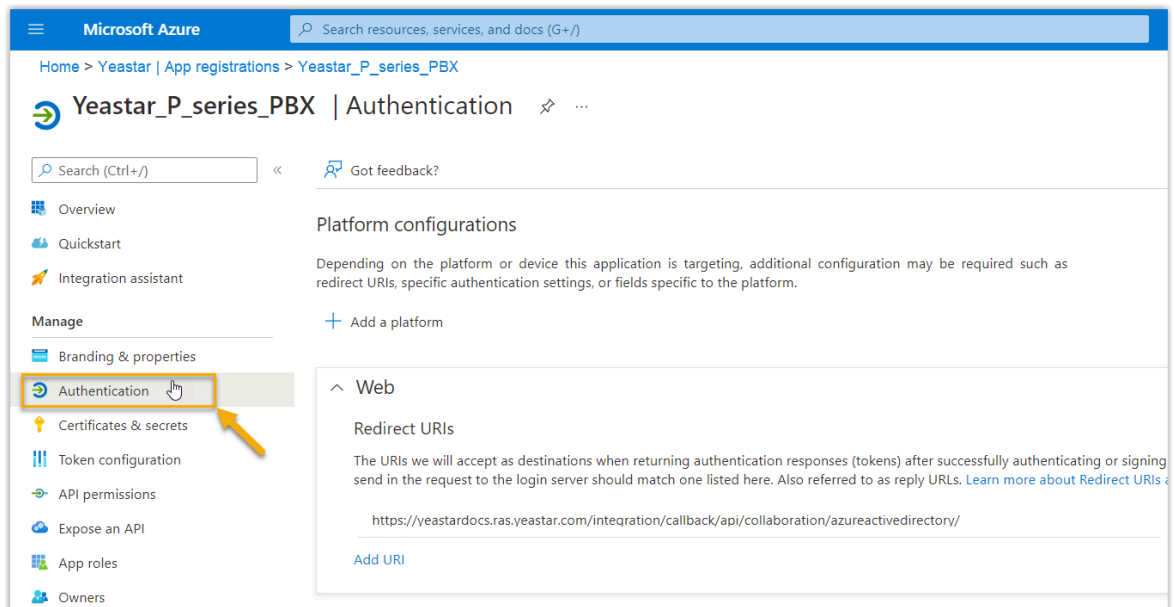
The **Directory (tenant) ID** is required if your PBX server is 37.10.0.30 or later.



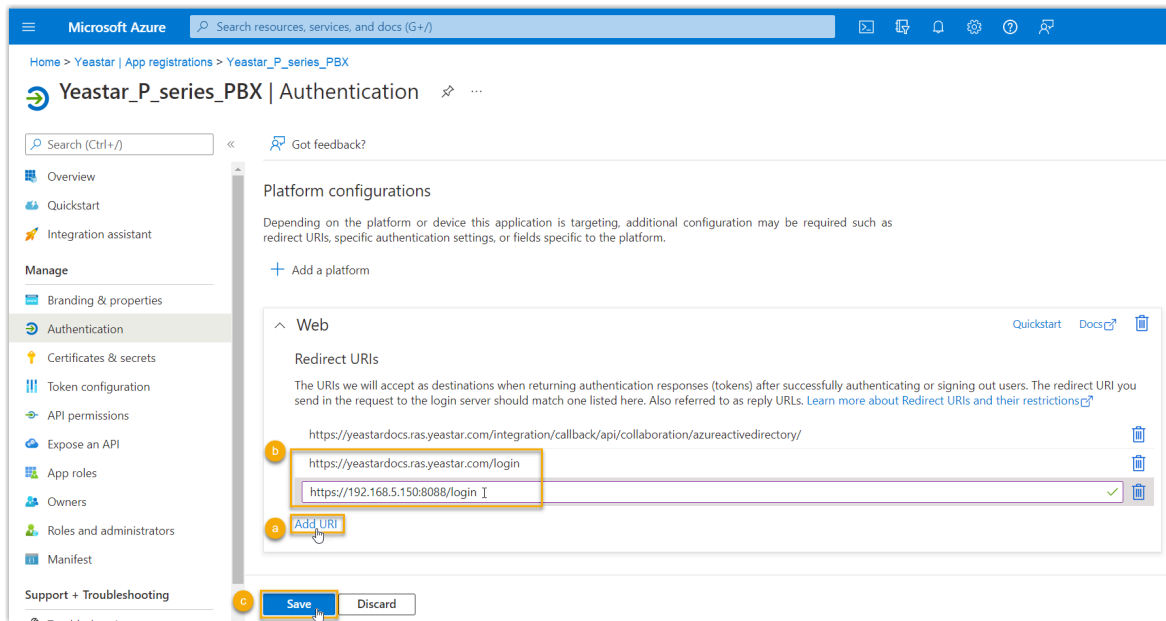
Step3. (Optional) Add SSO redirect URI to the Azure AD application

If you want to implement Single Sign-on (SSO) to allow the synced Azure AD users to log in to Linkus Web Client by their Microsoft accounts, you need to add the Linkus Web Client SSO Redirect URI to the Azure AD application.

1. On the left navigation bar of the Azure AD application, go to **Authentication**.



2. Add the SSO Redirect URI of Linkus Web Client.



- a. On the **Authentication** page, click **Add URI** in the **Web** section.
- b. Paste the [Linkus Web Client SSO Redirect URI](#) obtained from the PBX.
- c. Click **Save**.

Step4. Grant permissions to the Azure AD application

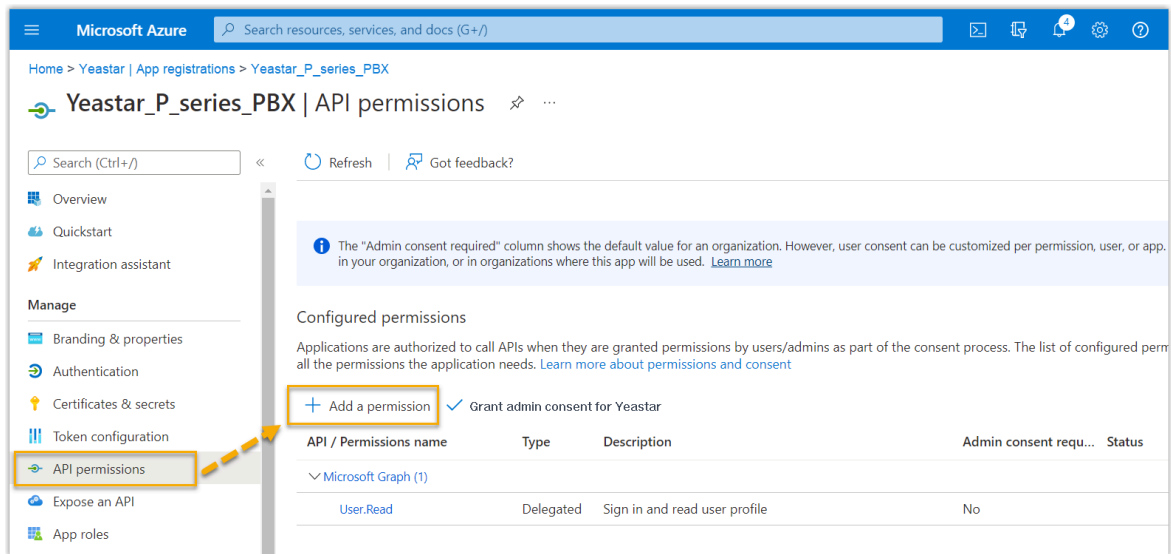


Important:

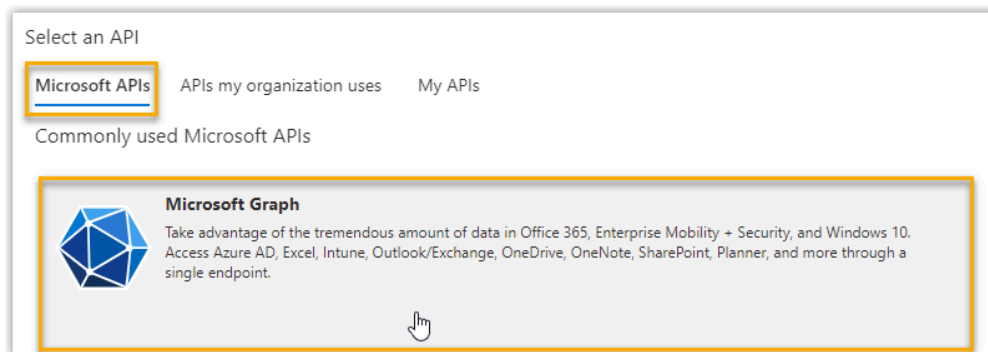
You DO NOT need to perform this step if your PBX server is 37.10.0.30 or later.

Grant the required API application permissions to the Azure AD application, allowing the application to access specified data within Azure Active Directory.

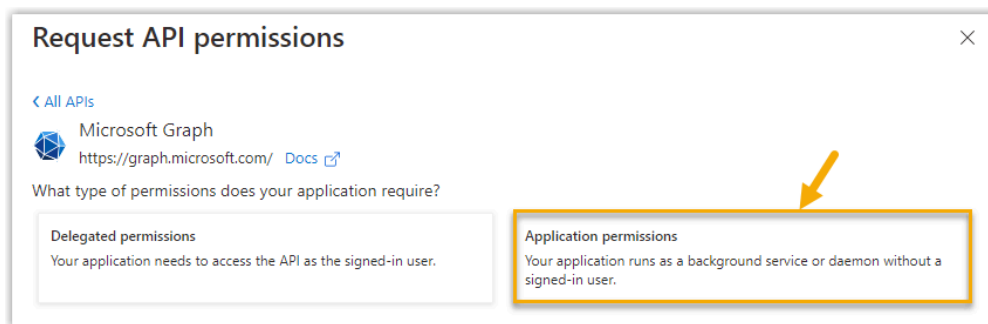
1. On the left navigation bar of the Azure AD application, go to **API permissions**, then click **Add a permission**.



2. In the **Select an API** page, go to **Microsoft APIs > Microsoft Graph**.



3. Click **Application permissions**.



4. Add the required application permissions:

- In the search bar, enter the keyword to search and select the following required permissions.

Select permissions expand all

| Permission | Admin consent required |
|--|------------------------|
| <div> <div>▼</div> <div>Directory (1)</div> </div> <div> <input checked="" type="checkbox"/> <div> Directory.Read.All ⓘ Read directory data </div> </div> | Yes |
| <input type="checkbox"/> <div> Directory.ReadWrite.All ⓘ Read and write directory data </div> | Yes |
| <input type="checkbox"/> <div> Directory.Write.Restricted ⓘ Manage restricted resources in the directory </div> | Yes |
| <div>> DirectoryRecommendations</div> | |
| <div>> RoleManagement</div> | |

| Permission | Description |
|--|--|
| Directory > Directory.Read.All | Allow the application to read data in your organization's directory, such as users and groups. |
| User > User.Read.All | Allow the application to read the profile properties of users in your organization. |
| Group > Group.Read.All | Allow the application to read group properties and memberships. |

b. Click **Add permissions**.

The selected permissions are added into the permissions list.

c. Click **Grant admin consent for...** to grant the permissions to the application.

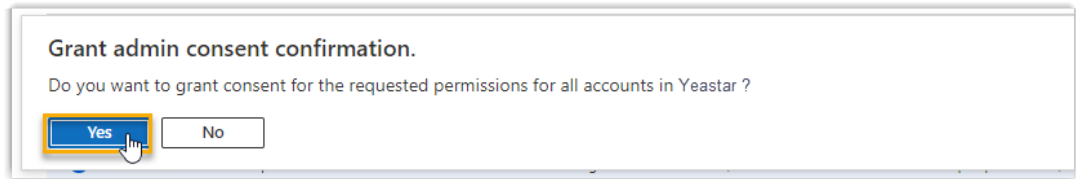
Configured permissions


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 Yeastar

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|------------------------|-------------|-------------------------------|-----------------------|-----------------------|
| ▼ Microsoft Graph (4) | | | | |
| Directory.Read.All | Application | Read directory data | Yes | ⚠ Not granted for ... |
| Group.Read.All | Application | Read all groups | Yes | ⚠ Not granted for ... |
| User.Read | Delegated | Sign in and read user profile | No | ... |
| User.Read.All | Application | Read all users' full profiles | Yes | ⚠ Not granted for ... |

d. In the pop-up dialog box, click **Yes** to proceed.

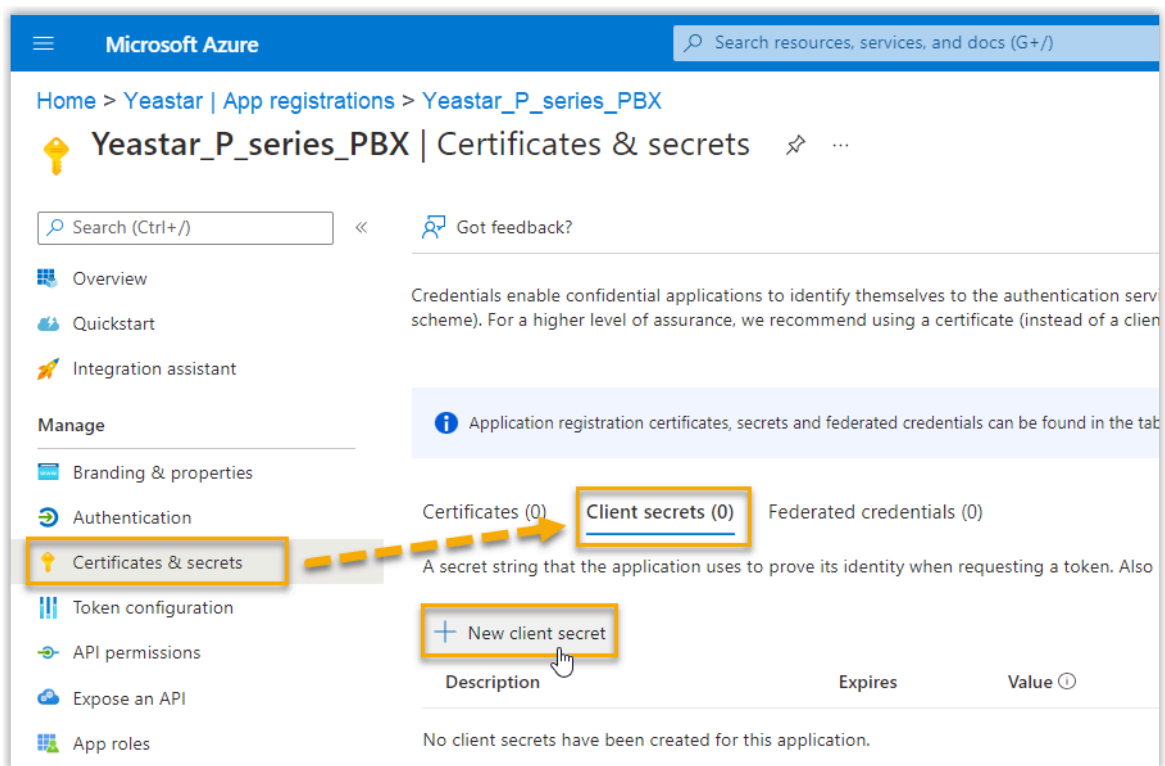


The **Status** of the permissions changes to , indicating that the API permissions have been granted to the application successfully.

Step5. Generate a client secret for the Azure AD application

Generate a client secret for the Azure AD application to authenticate the application in the integration.

1. On the left navigation bar of the Azure AD application, go to **Certificates & secrets > Client secrets**, then click **New client secret**.



2. In the **Add a client secret** page, do as follows:
 - a. Add a description and set an expiration date for the client secret.

b. On the bottom of the page, click **Add**.

A client secret is created and displayed in the **Client secrets** list.

3. Note down the client secret's **Value** as you will need to fill it into the PBX later.



Important:

Record the client secret's value before leaving the page, as the key is only shown once. Otherwise, you will have to create a new secret.

| Description | Expires | Value | Secret ID |
|---------------------|----------|----------|-----------------------|
| yeastar-pseries-pbx | 7/5/2024 | HoU8Q~Nm | Re~d... 977e... 78... |

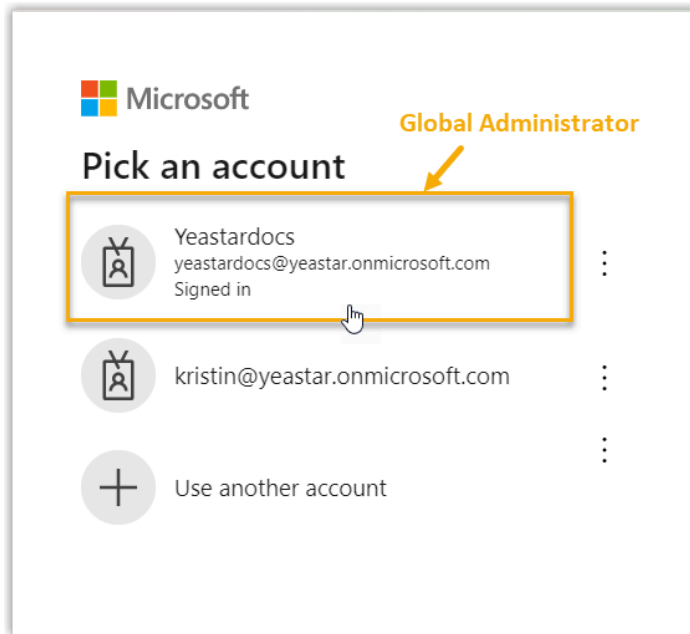
Step6. Connect PBX and Azure AD

Fill the application ID and client secret gathered from the Azure AD application into PBX to implement the integration between Yeastar P-Series PBX System and Azure Active Directory.

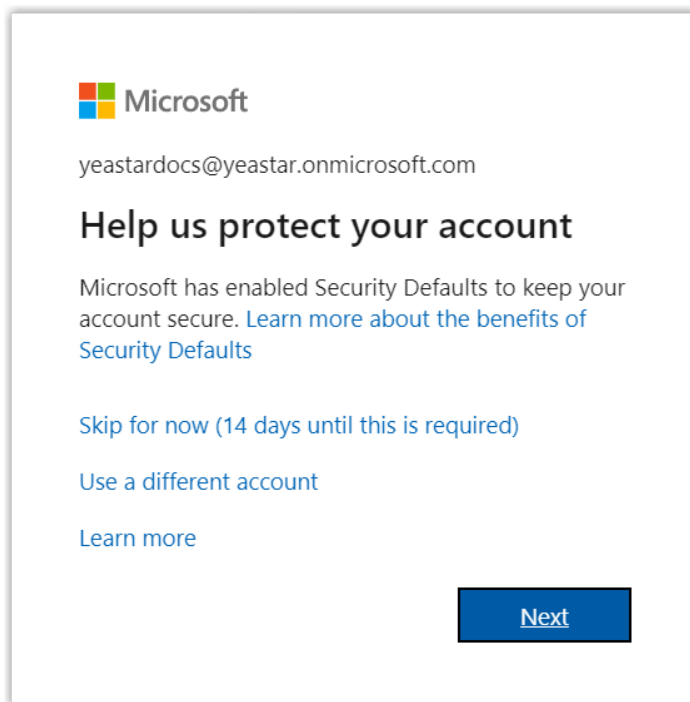
1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. Click **Integrate** beside the **Microsoft 365** service.
3. In the **App Registration** section, enter the following information:
 - **Application (Client) ID:** Paste the [application ID](#).
 - **Tenant ID:** Paste the [tenant ID](#).
4. In the **Certificates & Secrets** section, paste the [client secret](#) in the **Client Secret** field.
5. Click **Save**.

You are redirect to the Microsoft Sign-in page.

6. Sign in with the Microsoft Azure account that has **Global Administrator** privilege.



7. You might be asked to provide an additional security confirmation. Click **Next** to complete it or skip for now.




8. In the pop-up window, check the permissions and click **Accept** to confirm.



Note:



If your PBX server is 37.10.0.30 or later, you can grant consent on behalf of your organization in this page as needed.

 **Microsoft**

yeastardocs@yeastar.onmicrosoft.com

Permissions requested

Yeastar_P_series_PBX
[App info](#)

This application is not published by Microsoft.

This app would like to:

- ✓ Maintain access to data you have given it access to
- ✓ Have full access to user contacts
- ✓ Read and write user and shared contacts
- ✓ Read all users' full profiles
- ✓ Read all groups
- ✓ Read directory data
- ✓ Read user's presence information
- ✓ Read presence information of all users in your organization

☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

9. On the PBX configuration page, click **Yes** to close the dialog box.

Collaboration ×

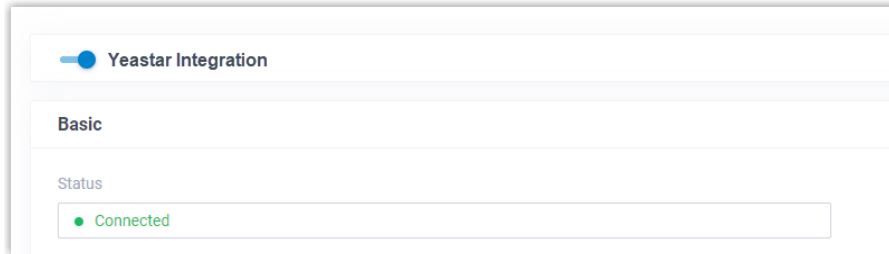
✓

Data initialization succeeded. You can configure synchronization rules and enjoy advanced features now.

✓ OK

Result

The status of the integration displays **Connected**, indicating that the PBX is successfully connected to your organization's Azure Active Directory.



What to do next

Set up synchronization rules to synchronize the desired Azure AD users and groups to PBX. For more information, see the following topics:

- [Synchronize Azure AD Users to Yeastar P-Series PBX System](#)
- [Synchronize Azure AD Groups to Yeastar P-Series PBX System](#)

Related information

- [Disable Azure Active Directory Integration](#)
- [Disconnect Azure Active Directory Integration](#)

Synchronize Azure AD Users to Yeastar P-Series PBX System

This topic describes how to customize synchronization rule based on Azure AD users, PBX will create extensions for the Azure AD users specified to be synced accordingly, and keep the extensions up-to-date with changes from the Azure AD users.

Limitation

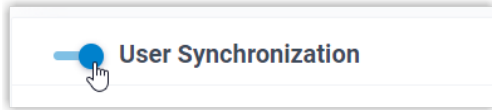
The number of Azure AD users that can be synced depends on the number of extensions that PBX system can create.

Prerequisites

You have [integrated Yeastar P-Series PBX System with Azure Active Directory](#).

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. In the **User Synchronization** section, turn on the switch.



3. Complete the following synchronization settings according to your need.
 - a. In the **User Range for Extension Auto Creation** drop-down list, specify the Azure AD users that you want to synchronize to PBX and create extensions for them.

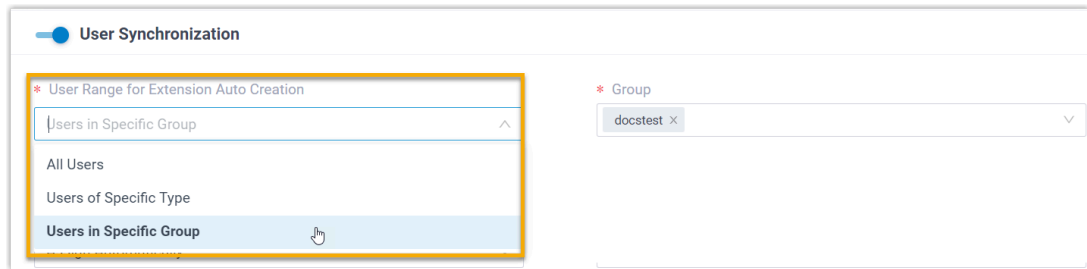


Table 1.

| Option | Description |
|-------------------------|---|
| All Users | Synchronize all Azure AD users to PBX and create extensions for them. |
| Users of Specific Type | <p>Synchronize the specified type(s) of Azure AD users to PBX and create extensions for them.</p> <p>You can select the desired user type(s) in the User Type drop-down list.</p> <ul style="list-style-type: none"> • Member: All member users in your organization's directory. • Guest: All guest users in your organization's directory. |
| Users in Specific Group | <p>Synchronize the Azure AD users within the specified group(s) to PBX and create extensions for them.</p> <p>You can select the desired group(s) in the Group drop-down list.</p> |



Note:

In future use, if you change the range of Azure AD users to be synced, you can decide how to deal with the extensions that are no longer



synced from the Azure AD users via the **Auto delete the Extensions no longer in sync** option.

* Extension Range for Auto Creation

Users in Specific Group

☒ Auto delete the Extensions no longer in sync

- If selected, the extensions will be deleted during the next synchronization.
- If unselected, the extensions will be retained and fully managed by the PBX.

b. In the **User's Extension Number** drop-down list, configure the extension number assignment rule.

* User's Extension Number

Assign Automatically


Assign Automatically

Read Specific Property Value

* Start Extension Number from

1000

Table 2.

| Option | Description |
|------------------------------|---|
| Assign Automatically | <p>Assign extension numbers from a specific starting number.</p> <p>You can specify the starting number in the Start Extension Number from field.</p> |
| Read Specific Property Value | <p>Assign extension numbers based on users' property value. This can be used in the scenario that Azure AD users already have phone extensions assigned, and you want to keep their extension numbers instead of assigning new ones.</p> <p>You can specify the property where the Azure AD users' extension numbers are stored (e.g. <code>businessPhones</code>) in the Property Name field.</p> <div>  Tip: Refer to Microsoft User Properties for the property name. </div> |

- c. In the **Delete the Extension when its associated user account is** drop-down list, select the Azure AD user account status(es) at which PBX will stop syncing from the Azure AD users, and delete the associated extensions.

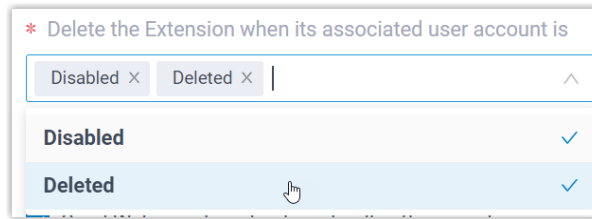


Table 3.

| Option | Description |
|----------|--|
| Disabled | If an Azure AD user account is disabled, PBX will stop syncing from the Azure AD user and delete the associated extension. |
| Deleted | If an Azure AD user account is deleted, PBX will stop syncing from the Azure AD user and delete the associated extension. |

- d. On the **Auto associate Extensions with the Users that share the same email address** option, decide whether to sync Azure AD users to PBX when the users have the same email addresses with existing extensions.
- If selected, the Azure AD users with same mailboxes will be synced to PBX and associated with the existing extensions, the extensions' user information will then be overwritten by that of the Azure AD users.
 - If unselected, the Azure AD users with same mailboxes will not be synced to PBX as the PBX system does not allow duplicated email addresses.
- e. If you want to send Linkus Welcome Email to the synced Azure AD users, select the checkbox of **Send Welcome Email automatically after an extension is created**.
4. Click **Save**.



Note:

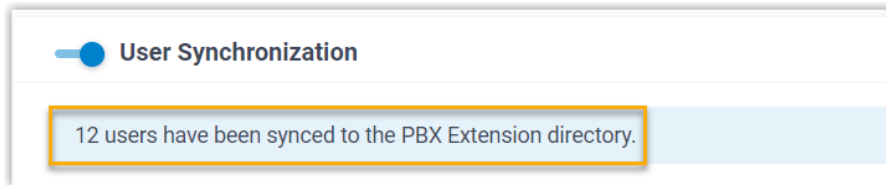
- If it is the FIRST time you save the synchronization-related settings, PBX will perform the initial synchronization immediately.
- Otherwise, you can [manually perform a directory synchronization](#) or wait for the [automatic directory synchronization](#).


Result

You have created your custom synchronization rule for Azure AD users.

During a synchronization process, PBX system performs queries within the Azure Active Directory based on the rule, and synchronize the desired Azure AD users as well as the updated information to PBX. After the synchronization, the followings can be implemented:

- You can check the synchronization result in the **User Synchronization** section.



- The PBX extensions associated with Azure AD users come with a label , and can not be manually deleted on PBX.
- You can NOT manually update the following information of the PBX extensions associated with Azure AD users.



Note:

The information can only be modified within the Azure Active Directory and updated to the PBX during a synchronization.

- Last name
- First name
- Email Address
- Mobile Number
- Job Title

What to do next

If you want to allow the synced Azure AD users to log in to Linkus Web Client and Mobile Client using their Microsoft accounts, you need to configure the Single Sign-on (SSO) feature. For more information, see [Allow Users to Log in to Linkus UC Clients with SSO](#).

Related information

[Synchronize Azure AD Groups to Yeastar P-Series PBX System](#)

[Synchronize Microsoft Outlook Contacts to Yeastar P-Series PBX System](#)

[Enable Microsoft Teams User Presence Synchronization](#)

[Pause Azure Active Directory Synchronization](#)

Synchronize Azure AD Groups to Yeastar P-Series PBX System

This topic describes how to customize synchronization rule based on Azure AD groups, so as to synchronize desired Azure AD groups to the PBX extension groups.

Limitation

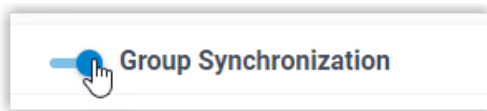
The number of Azure AD groups that can be synced depends on the extension groups that PBX system can create (up to 63 extension groups).

Prerequisites

You have [integrated Yeastar P-Series PBX System with Azure Active Directory](#).

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. Scroll down to the **Group Synchronization** section, turn on the switch.



3. In the **Synchronize for** drop-down list, specify the Azure AD groups that you want to synchronize to PBX.

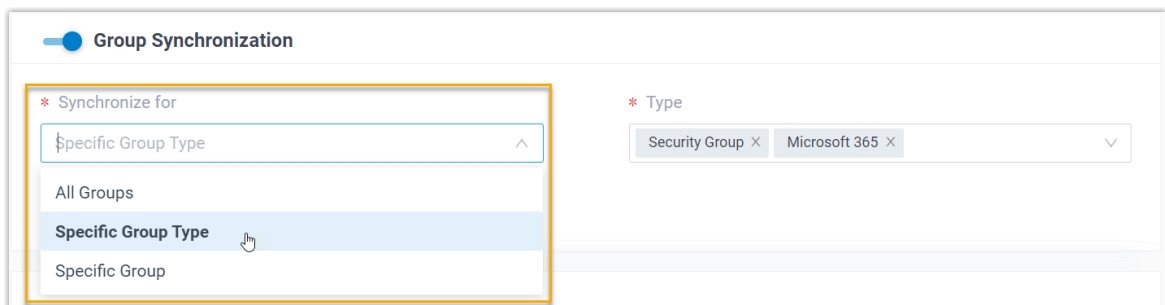



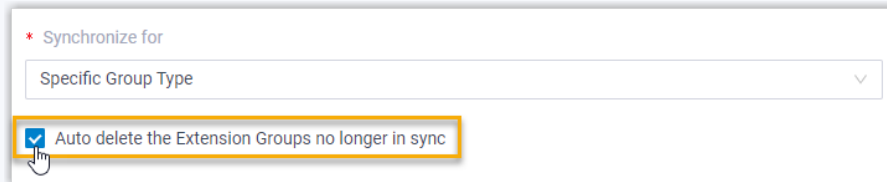
Table 4.

| Option | Description |
|---------------------|---|
| All Groups | Synchronize all Azure AD groups to PBX. |
| Specific Group Type | Synchronize the specified type(s) of Azure AD groups to PBX. You can select the desired group type(s) in the Type drop-down list. |

| Option | Description |
|----------------|--|
| | <ul style="list-style-type: none"> • Security Group: All security groups in your organization's directory. • Microsoft 365: All Microsoft 365 groups in your organization's directory. |
| Specific Group | <p>Synchronize specific Azure AD groups to PBX. You can directly search and select the desired groups in the Group drop-down list.</p> <div>  Note: By default, the Group drop-down list displays 200 records of Azure AD groups. If you need the system to display more records, contact Yeastar. </div> |

**Note:**

In future use, if you change the range of Azure AD groups to be synced, you can decide how to deal with the extension groups that are no longer synced from the Azure AD groups via the **Auto delete the Extension Groups no longer in sync** option.



- If selected, the extension groups will be deleted during the next synchronization.
- If unselected, the extension groups will be retained and fully managed by the PBX.

4. Click **Save**.

**Note:**

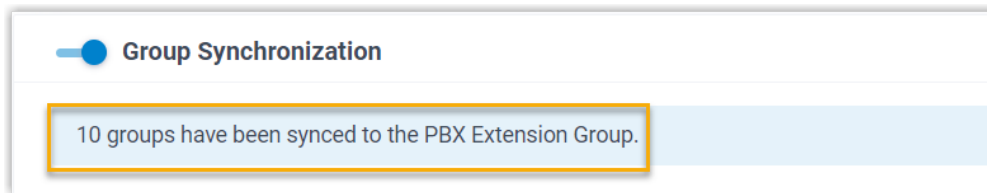
- If it is the **FIRST** time you save the synchronization-related settings, PBX will perform the initial synchronization immediately.
- Otherwise, you can [manually perform a directory synchronization](#) or wait for the [automatic directory synchronization](#).


Result

You have created your custom synchronization rule for Azure AD groups.

During a synchronization process, PBX system performs queries within your organization's Azure Active Directory based on the rule, and synchronize the desired Azure AD groups as well as the updated information to PBX. After the synchronization, the followings can be implemented:

- You can check the synchronization result in the **Group Synchronization** section.



- The PBX extension groups associated with Azure AD groups come with a label , and can NOT be deleted.
- You can NOT manually update the name and group member of the PBX extension groups associated with Azure AD groups on PBX.



Note:

The information can only be modified within the Azure Active Directory and updated to the PBX during a synchronization.

Related information

[Synchronize Azure AD Users to Yeastar P-Series PBX System](#)

[Pause Azure Active Directory Synchronization](#)

Synchronize Microsoft Outlook Contacts to Yeastar P-Series PBX System

Azure Active Directory integration provides one-way synchronization of Outlook contacts (personal Outlook contacts and contacts from Outlook shared mailboxes) to PBX and Linkus clients. After synchronization, Azure AD users can access and make calls to their Outlook contacts through Linkus clients.

Requirement

PBX server: Version 37.10.0.30 or later.

Prerequisites

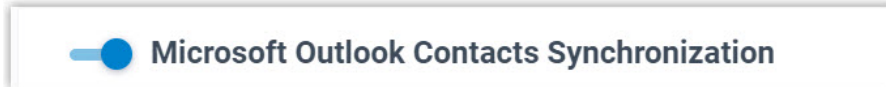
- You have [integrated Yeastar PBX with Azure Active Directory](#).
- You have [synchronized Azure AD users to Yeastar PBX](#).

Synchronize personal Outlook contacts to Linkus Contacts directory

To synchronize Azure AD users' personal Outlook contacts, you need to select the user range for syncing personal contacts on PBX, and the selected Azure AD users need to share their personal contacts folder with the authorization account ([the account that is used to authorize the Azure AD integration with the PBX](#)), so that PBX can access the contacts.

Step 1. Select user range for syncing personal contacts on PBX

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. Scroll down to the **Microsoft Outlook Contacts Synchronization** section, and turn on the switch.



3. Select the checkbox of **Contacts Synchronization**.
4. In the **User Range for Contacts Synchronization** drop-down list, select the range.



Important:

Ensure that the user range you select here is covered by the [user range you selected when syncing Azure AD users to PBX](#), as this feature is only available for synced Azure AD users.


| Option | Description |
|-------------------------|--|
| All Users | Synchronize all Azure AD users' personal contacts to their Linkus Contacts directory. |
| Users in Specific Group | Synchronize personal contacts of the Azure AD users within specified Azure AD group(s) to their Linkus Contacts directory. |

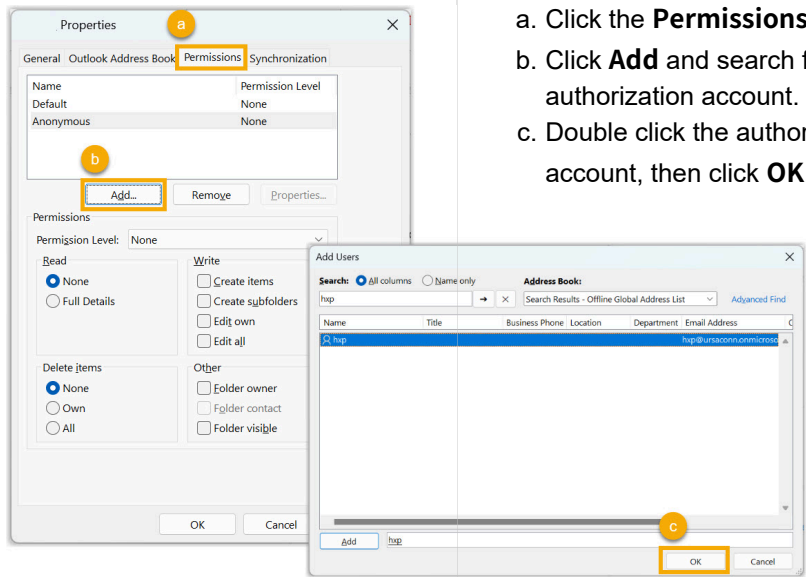
| Option | Description |
|--------|---|
| | You can select the desired groups in the Group drop-down list. |

5. Click **Save**.

Step 2. Share personal Outlook contacts folder on Outlook Desktop Client

We provide an example on how an individual Azure AD user can share his or her personal Outlook contacts folder on Outlook Desktop Client.

1. Log in to Outlook Desktop Client, go to  (**People**).
2. In **My Contacts** section, right click the personal contacts folder, then select **Properties...**
3. In the pop-up window, search for and add the authorization account (the account that is used to authorize the Azure AD integration with PBX).

| Screenshot | Instruction |
|---|--|
|  | <p>a. Click the Permissions tab.</p> <p>b. Click Add and search for the authorization account.</p> <p>c. Double click the authorization account, then click OK.</p> |

4. Grant the authorization account access to contacts in the folder.

| Screenshot | Instruction |
|------------|--|
| | <p>a. In the upper user section, select the authorization account.</p> <p>b. In the Read section, select Full Details.</p> <p>c. In the Other section, select Folder contact.</p> <p>d. Click OK.</p> |

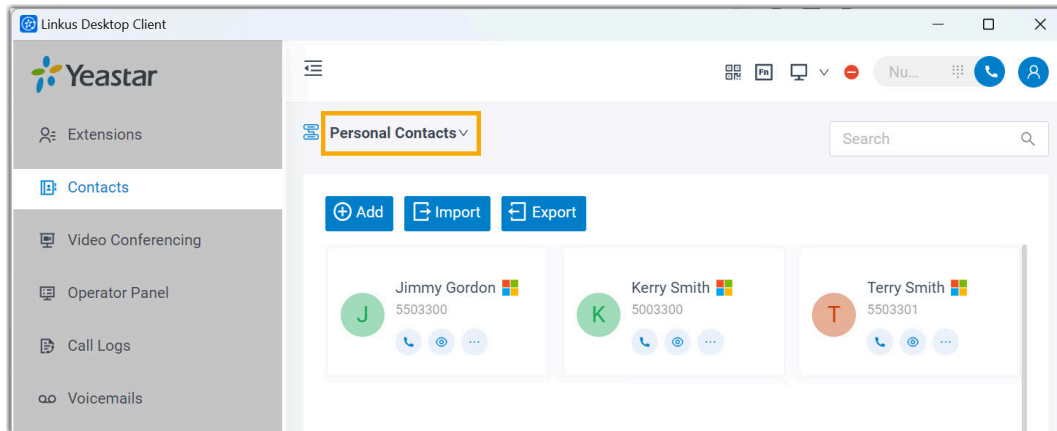


Note:

The system will perform the synchronization at the preset time for [automatic directory synchronization](#), you can also [manually perform a directory synchronization](#) to sync Outlook contacts.

Result

After the synchronization, Azure AD users' personal Outlook contacts are synced to their Linkus Contacts directory with a label . And the synced contacts can NOT be edited or deleted on Linkus client.



Troubleshooting:

Unable to synchronize specific Outlook contacts?

Incomplete information of Outlook contacts can lead to synchronization failure. Make sure the following fields are filled in for Outlook contacts, then perform the directory synchronization again:

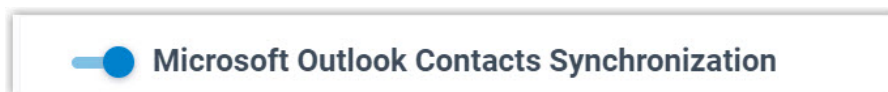
- **First name** or **Last name**: At least one field is required.
- **Mobile phone number**, **Home phone**, or **Business phone**: At least one field is required.

Synchronize contacts from Outlook shared mailboxes to PBX phone-books

To synchronize contacts from shared mailboxes, you need to set up shared contacts synchronization on PBX, and add the authorization account ([the account that is used to authorize the Azure AD integration with the PBX](#)) as a member of the desired shared mailboxes on Microsoft 365 admin center, so that PBX can access the contacts within the shared mailboxes.

Step 1. Set up shared contacts synchronization on PBX

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. Scroll down to **Microsoft Outlook Contacts Synchronization** section, turn on the switch.



3. Select the checkbox of **Shared Mailbox Contacts Synchronization**.
4. In the **Shared Mailbox Contacts Synchronization** drop-down list, select the range.

| Option | Description |
|---------------------------------------|---|
| Contacts in All Shared Mailboxes | Synchronize contacts from all the Outlook shared mailboxes to PBX phonebooks. |
| Contacts in Specific Shared Mailboxes | <p>Synchronize contacts from specific Outlook shared mailbox(es) to PBX phonebooks.</p> <p>You can select the desired shared mailbox(es) in the Shared Mailboxes drop-down list.</p> |

5. Define the phonebook name for the shared contacts to be synced.

6. Click **Save**.

Step 2. Add the authorization account to the shared mailboxes on Microsoft 365 admin center

1. Log in to [Microsoft 365 admin center](#).
2. On the left navigation bar, click **Teams & groups** and select **Shared mailboxes**.
3. Click the desired shared mailbox and configure the following settings.
 - a. In the **Members** section, click **Edit**.
 - b. Click **Add members** and search for the authorization account (the account that is used to authorize the Azure AD integration with PBX).
 - c. Select the authorization account and click **Add**.
4. Repeat **step 3** for all the shared mailboxes that needs to be synced.




Note:

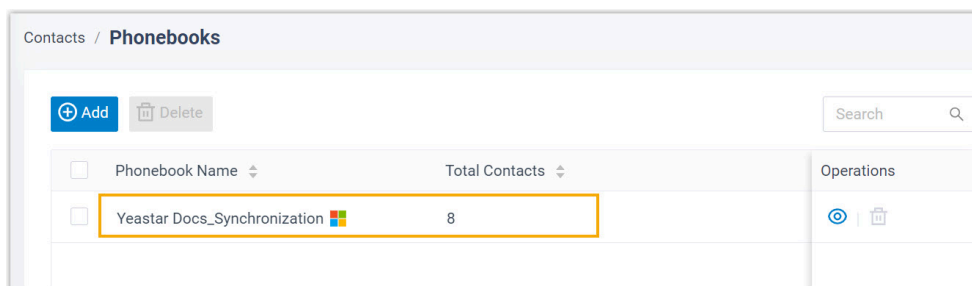


The system will perform the synchronization at the preset time for [automatic directory synchronization](#), you can also [manually perform a directory synchronization](#) to sync Outlook contacts.

Result

After the synchronization, the followings can be implemented:

- The shared mailboxes and their contacts are synchronized to PBX phonebook, which comes with a label  and can NOT be edited or deleted on PBX.



Troubleshooting:

Unable to synchronize specific Outlook contacts?

Incomplete information of Outlook contacts can lead to synchronization failure. Make sure the following fields are filled in for Outlook contacts, then perform the directory synchronization again:

- **First name** or **Last name**: At least one field is required.
- **Mobile phone number**, **Home phone**, or **Business phone**: At least one field is required.

- By default, the synced phonebook is NOT visible to users. To allow users to view the phonebook and its contacts, go to **Extension and Trunk > Client Permission > Contact Visibility Permission**.



Note:

Users with permission can log in to Linkus clients, go to **Contacts** and select the phonebook to view its contacts.

Enable Microsoft Teams User Presence Synchronization

Azure Active Directory integration provides one-way synchronization of Teams user presence to PBX extensions. To achieve the Teams user presence synchronization, you need to enable this feature on PBX, and Azure AD users need to set up presence synchronization on their Linkus clients. After the setup, Azure AD users' extension presence can follow their Teams user presence.

Requirement

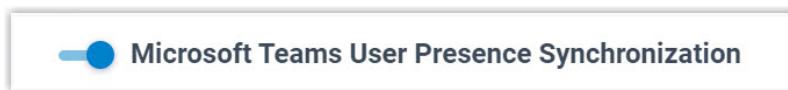
PBX server: Version 37.10.0.30 or later.

Prerequisites

- You have [integrated Yeastar PBX with Azure Active Directory](#).
- You have [synchronized Azure AD users to Yeastar PBX](#).

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. Scroll down to the bottom, and turn on the switch of **Microsoft Teams User Presence Synchronization**.




3. Click **Save**.

Result

- Teams user presence synchronization is enabled.
- Azure AD users need to log in to **Linkus Web Client** or **Linkus Desktop Client** to enable this feature and set the corresponding extension presence for each Teams user presence (Path: **Preferences > Features > Microsoft Teams User Presence Synchronization**).

 **Tip:**



You can also click  of an Azure AD user's extension to enable and set up Teams presence synchronization for this user (Path: **Features > Microsoft Teams User Presence Synchronization**).

| Teams User Presence | Extension Presence |
|---------------------|--------------------|
| Available | Available |
| Busy | Away |
| Do not disturb | Do Not Disturb |
| Be right back | Away |
| Appear away | Off Work |
| Appear offline | Off Work |

After the setup, when Azure AD users' Teams presence changes, their extension presence will be switched to the corresponding one automatically.



Note:

Since it's one-way synchronization, when users switch their extension presence, the result will NOT update to their Teams user presence.

Allow Users to Log in to Linkus UC Clients with SSO

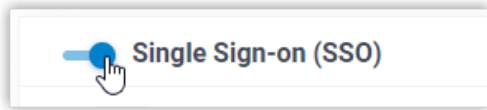
This topic describes how to configure the Single Sign-on (SSO) feature, so that synced Azure AD users can securely log in to Linkus Web Client and Mobile Client by their Microsoft accounts.

Prerequisites

You have [integrated Yeastar P-Series PBX System with Azure Active Directory](#).

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. In the **Single Sign-on (SSO)** section, turn on the switch.

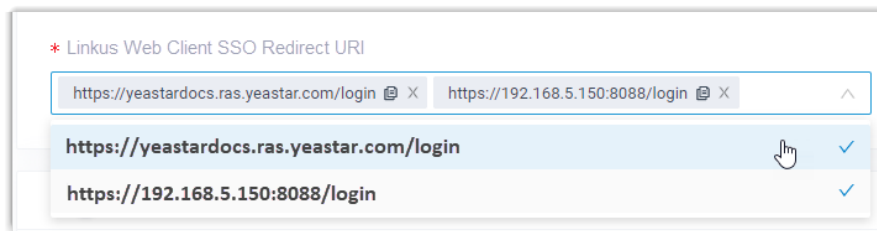


3. In the **Linkus Web Client SSO Redirect URI** drop-down list, select the desired Linkus Web Client login address.



Note:

To implement SSO on Linkus Web Client, make sure you have [added the selected Linkus Web Client SSO Redirect URI to the Azure AD application](#).



4. Click **Save**.

Result

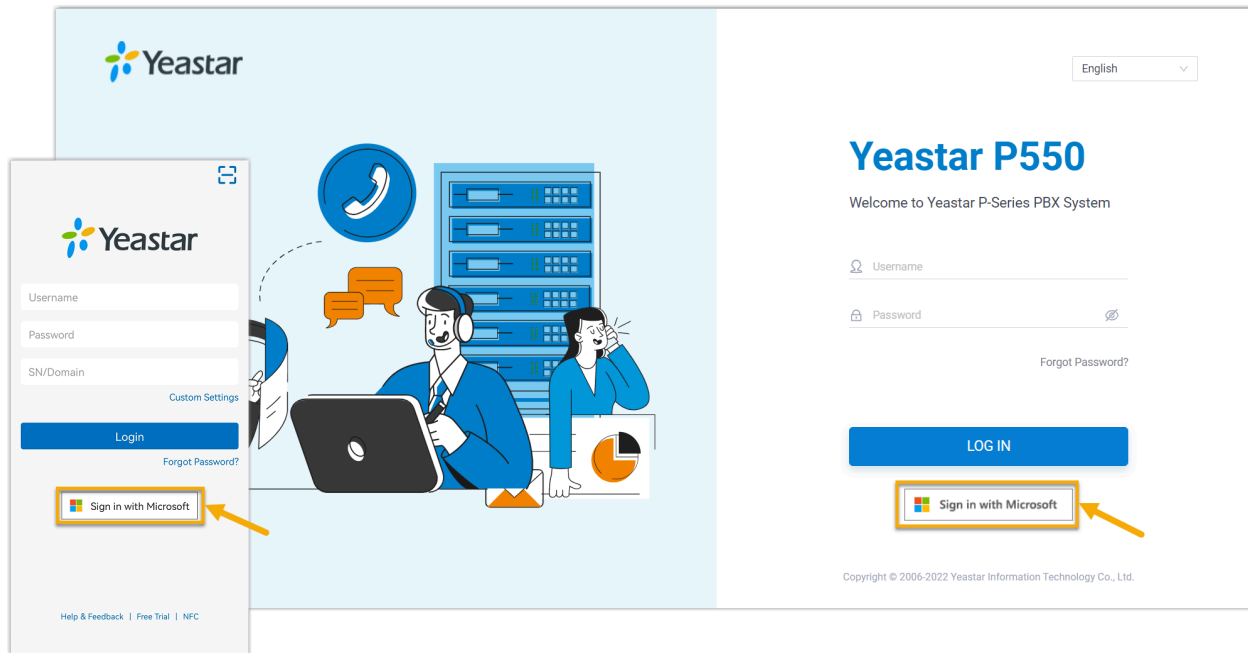
The synced Azure AD users can directly log in to Linkus Web Client and Mobile Client by their Microsoft accounts.



Note:

To use the SSO feature on Linkus Mobile Client, the App version should be updated.

- Linkus Android Client: 4.9.6 or later
- Linkus iOS Client: 4.9.5 or later



Related information

[Synchronize Azure AD Users to Yeastar P-Series PBX System](#)

Manage Azure Active Directory Integration

Schedule Automatic Directory Synchronization

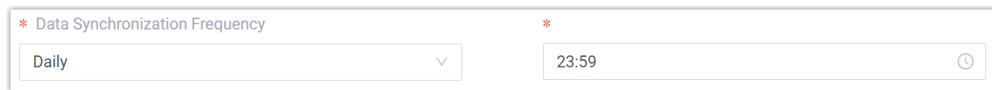
By default, PBX system automatically performs a directory synchronization at 00:30 every-day. You can also customize the automatic synchronization schedule to synchronize data from Azure Active Directory to Yeastar P-Series PBX System at a specified time.

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. In the **Basic** section, select the data synchronization frequency and set a specific time (non-office hours or weekends is recommended).

- **Daily:** The system synchronizes data daily at a preset local time.

For example, set up to synchronize data at 23:59 everyday.

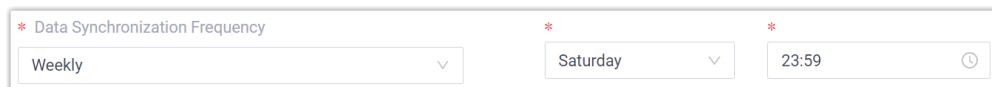


* Data Synchronization Frequency

Daily 23:59

- **Weekly:** The system synchronizes data on the selected days at a preset local time.

For example, set up to synchronize data at 23:59 on every Saturday.



* Data Synchronization Frequency

Weekly Saturday 23:59

3. Click **Save**.

Result

The PBX system performs periodic synchronizations automatically based on the schedule.



Note:

In addition to the scheduled automatic synchronization, the integration also implements another automatic synchronization, which will be triggered when either of the following conditions is met:



- If there are data changes (synced users have been modified or removed, name or group member of synced groups have been changed) occur in Azure Active Directory, PBX will perform an automatic directory sync in 10 minutes.
- If there are data changes (synced users have been modified or removed, member of synced groups have been changed) occur in Azure Active Directory, and the number of change events reaches 10, PBX will immediately perform an automatic directory sync.

Related information

[Manually Perform a Directory Synchronization](#)

Manually Perform a Directory Synchronization

In case you want to immediately apply a new synchronization rule, or update the data changes from the Azure Active Directory to PBX, you can manually start a synchronization.

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. In the **Basic** section, click **Update Now**.

Result

The PBX system performs directory synchronization once.

Related information

[Schedule Automatic Directory Synchronization](#)

Update Client Secret for Azure Active Directory Integration

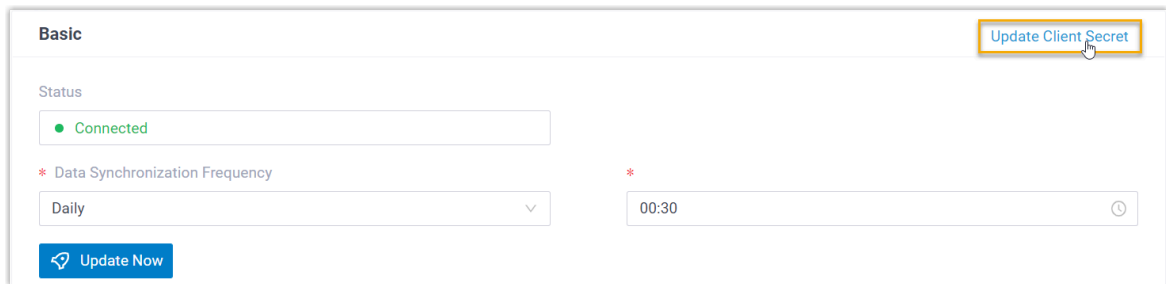
The client secret of the Azure AD application has an expiration date, which is set when you creating one. You will need to update the client secret for the integration prior to the expiration date to avoid the directory synchronization interruption.

Prerequisites

You have [generated a new client secret for the Azure AD application](#).

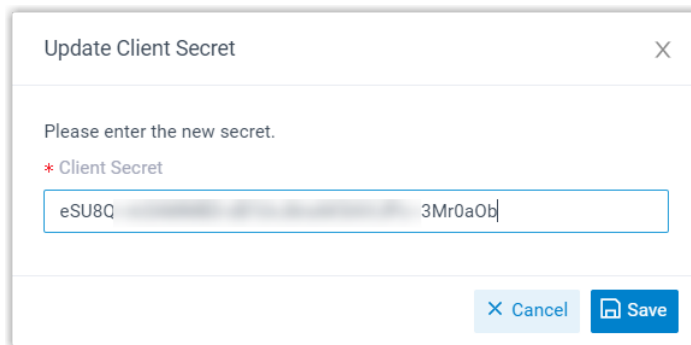
Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. At the top-right of the **Basic** section, click **Update Client Secret**.



The screenshot shows the 'Basic' configuration tab. In the top right corner, there is a button labeled 'Update Client Secret' which is highlighted with a yellow box. Below this, the 'Status' is shown as 'Connected'. There is a section for 'Data Synchronization Frequency' with a dropdown set to 'Daily' and a time field set to '00:30'. An 'Update Now' button is located at the bottom left of this section.

3. In the pop-up window, do as follows:



The screenshot shows a pop-up window titled 'Update Client Secret'. It contains the text 'Please enter the new secret.' followed by a label '* Client Secret'. Below this is a text input field containing the characters 'eSU8Q' and '3Mr0a0b'. At the bottom right of the window are two buttons: 'Cancel' and 'Save'.

- a. In the **Client Secret** field, paste the new client secret.
- b. Click **Save**.

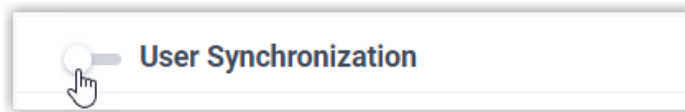
Pause Azure Active Directory Synchronization

If you want to prevent the synced data from being overwritten by the updates from Azure Active Directory, you can temporarily put the sync on hold. This topic describes how to pause the synchronization of Azure AD users and groups.

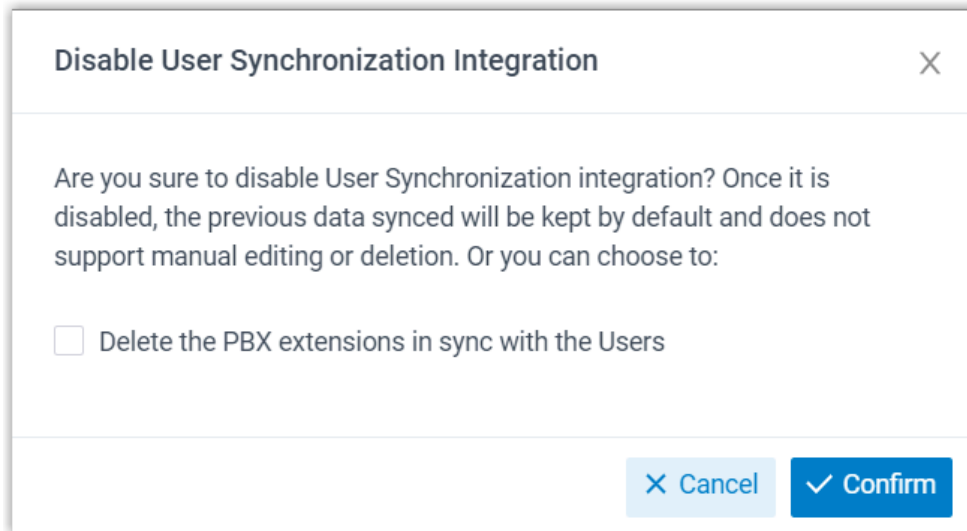
Pause synchronization of Azure AD users

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. In the **User Synchronization** section, turn off the switch.



3. Click **Save**.
4. In the pop-up window, do as follows:



- a. If you want to delete the PBX extensions associated with the synced Azure AD users, select the checkbox of **Delete the PBX extensions in sync with the Users**.
- b. Click **Confirm** to proceed.

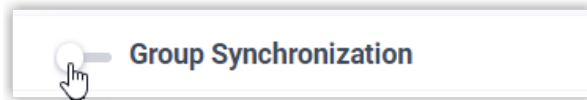
Result

- The user synchronization is paused.
- The settings of **User Synchronization** remain and can not be edited.
- If you choose to retain the associated PBX extensions, you can NOT update the user information of the extensions, or delete the extensions.

Pause synchronization of Azure AD groups

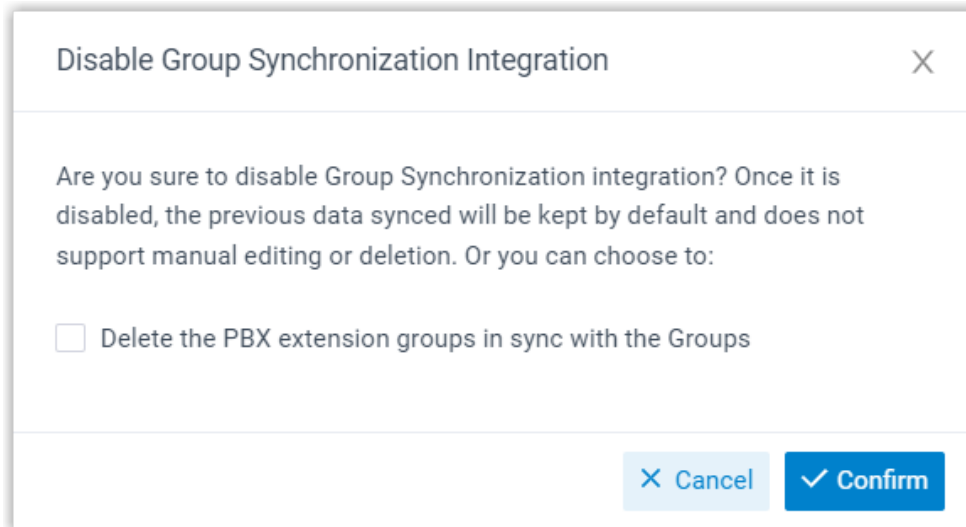
Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. In the **Group Synchronization** section, turn off the switch.



3. Click **Save**.

4. In the pop-up window, do as follows:



- a. If you want to delete the PBX extension groups associated with the synced Azure AD groups, select the checkbox of **Delete the PBX extension groups in sync with the Groups**.
- b. Click **Confirm** to proceed.

Result

- The group synchronization is paused.
- The settings of **Group Synchronization** remain and can not be edited.
- If you choose to retain the associated extension groups, you can NOT update the name and group member of the extension groups, or delete the extension groups.

Related information

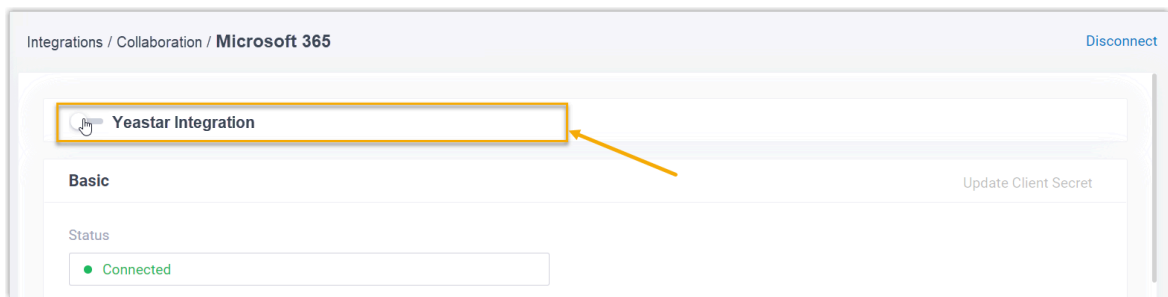
[Disable Azure Active Directory Integration](#)

Disable Azure Active Directory Integration

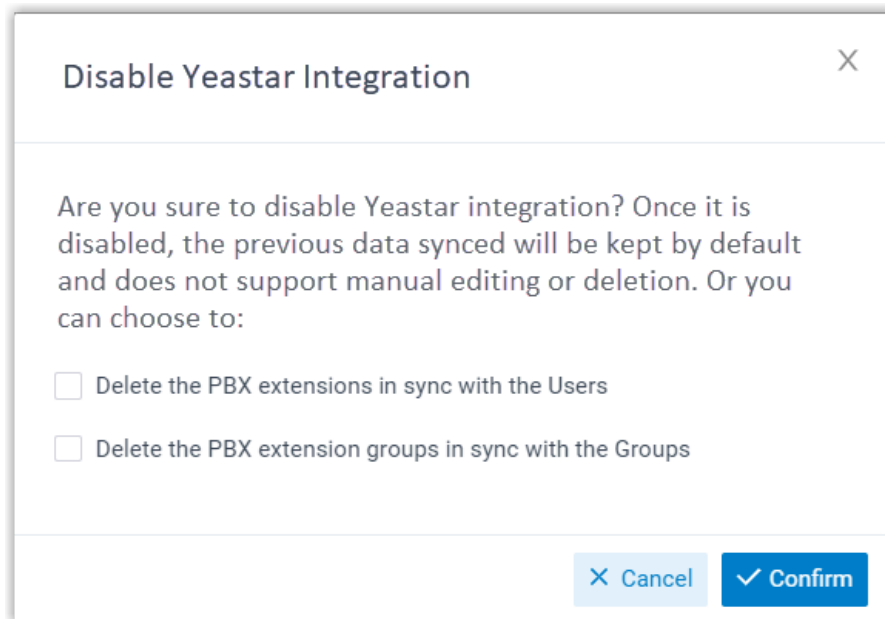
If there is a fix ongoing, and you might need to turn off the integration for troubleshooting, you can suspend the Azure Active Directory integration instead of disconnecting it. This topic describes how to disable the Azure Active Directory integration temporarily without losing the existing configurations.

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. On the top of the integration page, turn off the switch.



3. Click **Save**.
4. In the pop-up window, do as follows:



- a. Decide whether to clean up the PBX data that are associated with the synced Azure AD users and groups.

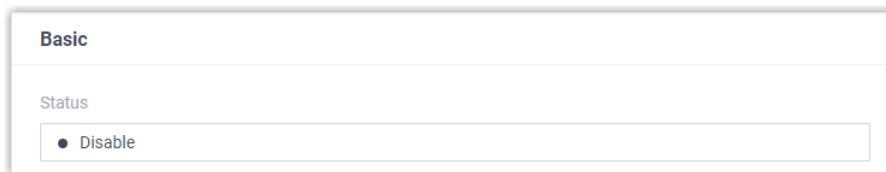
Table 5.

| Option | Description |
|---|---|
| Delete the PBX extensions in sync with the Users | <ul style="list-style-type: none"> • If selected, the extensions will be deleted. • If unselected, the extensions will be retained, and you can NOT update the user information of the extensions, or delete the extensions. |
| Delete the PBX extension groups in sync with the Groups | <ul style="list-style-type: none"> • If selected, the extension groups will be deleted. • If unselected, the extension groups will be retained, and you can NOT update the name and group member of the extension groups, or delete the extension groups. |

b. Click **Confirm** to proceed.

Result

- The **Status** displays "Disable", indicating that the entire integration is suspended.



- The integration configurations remain and can not be edited.
- The synced Azure AD users can NOT log in to Linkus Web Client and Mobile Client by their Microsoft accounts now.

Related information

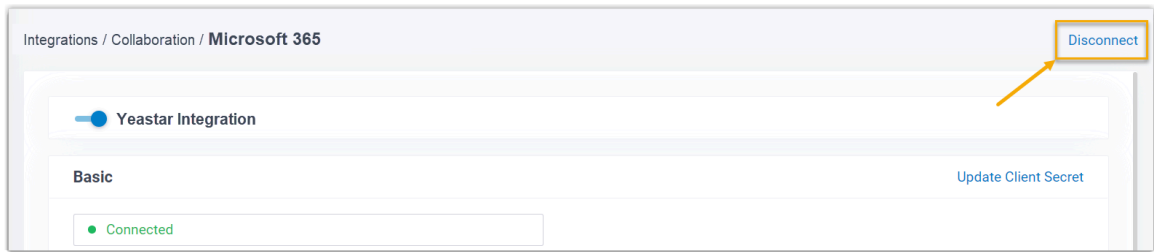
[Disconnect Azure Active Directory Integration](#)

Disconnect Azure Active Directory Integration

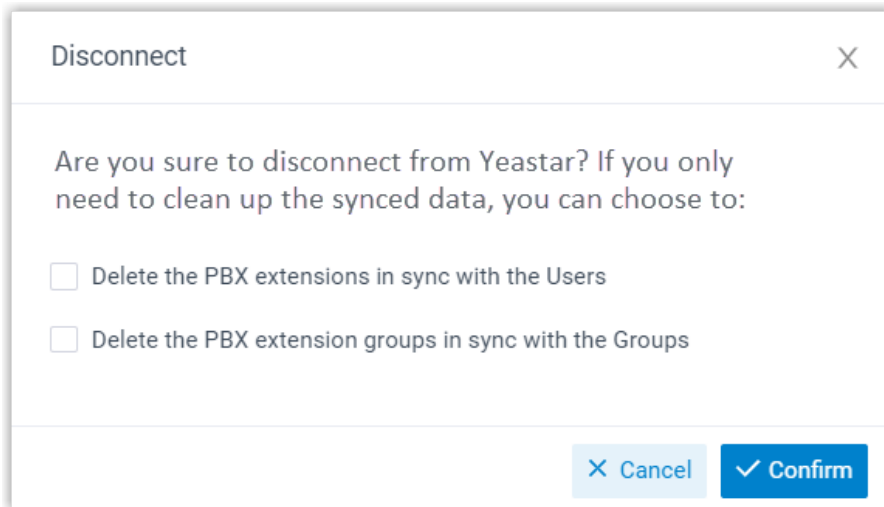
If you want to integrate with another directory, you need to remove the current integration first. This topic describes how to disconnect the integration between Yeastar P-Series PBX System and Azure Active Directory.

Procedure

1. Log in to PBX web portal, go to **Integrations > Collaboration**.
2. At the top-right of the integration page, click **Disconnect**.



3. In the pop-up window, do as follows:



- a. Decide whether to clean up the PBX data that are associated with the synced Azure AD users and groups.

Table 6.

| Option | Description |
|---|--|
| Delete the PBX extensions in sync with the Users | <ul style="list-style-type: none"> • If selected, the extensions will be deleted. • If unselected, the extensions will be retained and fully managed by the PBX. |
| Delete the PBX extension groups in sync with the Groups | <ul style="list-style-type: none"> • If selected, the extension groups will be deleted. • If unselected, the extension groups will be retained and fully managed by the PBX. |

- b. Click **Confirm**.

Result

The Azure Active Directory integration is disconnected.