

Akixi CXA & CXI Teams required M365 permissions

Authorising Akixi CXI application with M365/Entra

Document Revision v1_20250617

Table of Contents

Table of Contents.....	2
Copyright & Confidentiality Notice.....	3
Warranty.....	3
Trademarks.....	3
Akixi CX MSFT Teams required M365 permissions.....	4
<i>Overview.....</i>	4
<i>M365 administrator consent and authorisation process and permissions necessary for each step.....</i>	4
Administrator consent.....	4
Authorisation.....	4
Admin Consent and Authorization process visualised (using different user accounts with different permission levels for each step).....	5
Authorising Akixi CX application with M365/Entra.....	6
<i>ACXMT update to requested M365 permissions set.....</i>	6
Akixi CX v3.1.0 upgrade (R-T Presence events), new permissions and re-consent process.....	6
Akixi CX v3.2.0 upgrade (R-T CQ monitoring, shared voicemail), new permissions and re-consent process.....	6
<i>M365 permissions and Akixi CX reason to use</i>	7
<i>Example M365 request prompt for Akixi CX authorisation</i>	10
Entra/Azure Tenant ID, key TelSys identifier	11
<i>Overview</i>	11
<i>Where to find the Azure Tenant ID</i>	11
Microsoft Entra admin center.....	11
Azure portal.....	11
<i>Entra/Azure TenantID correct format when configuring Akixi CX Telephony Server</i>	12

Copyright & Confidentiality Notice

Copyright © Akixi. All Rights Reserved.

Any technical documentation that is made available by Akixi Limited is proprietary and strictly confidential and is considered the copyrighted work of Akixi Limited.

This publication is for distribution under either the Akixi Non-Disclosure Agreement, the Akixi Reseller Agreement, or the Reseller Distribution Agreement only.

No part of this publication may be duplicated without the express written permission of Akixi Limited.

Akixi Limited reserves the right to make changes without prior notice.

Warranty

The Akixi Service reporting functionality, supported call flow scenarios, Akixi Service configuration and provisioning functionality and workflow examples, recommended telephony platform configuration, suggested product billing strategies, and/or any provided data examples is/are provided “as is”, without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement.

In no event shall Akixi Limited be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the Akixi Service reporting functionality, supported call flow scenarios, Akixi Service configuration and provisioning functionality and workflow examples, recommended telephony platform configuration, suggested product billing strategies, and/or any provided data examples, or the use or other dealings of the Akixi Service, its APIs, or any associated documentation.

Trademarks

Cisco® BroadWorks® and BroadSoft M6 are trademarks of Cisco System, Inc.

MICROSOFT TEAMS is a trademark of Microsoft Corporation.

All other trademarks identified herein are the property of their respective owners.

Akixi CXA & CXI Teams required M365 permissions

Overview

The Akixi CXA & CXI Teams platform requires access to the Customer's Microsoft Teams instance to deliver its functionality.

Up to Akixi CX release v3.1.1, the customer's SysAdmin account holding "Global Admin" permission was required to authorise the Akixi CX platform with the customer's MSFT Teams instance. Some customers, predominantly larger accounts with defined IT security policies, have been objecting to indefinitely assigning Global Admin permissions to users. After the initial authorisation and consent process was completed, the customers sought a solution to remove the Global Admin permission from the authorising user.

There are multiple methods of assigning temporary Global Admin permissions to an authorising SysAdmin user

- using PIM (Privileged Identity Management) - time-capped temporarily elevated Global Admin permissions for the Akixi CX authorisation process, which automatically falls back to a lower level of access rights when expired
- manually modify the SysAdmin user permission group and replace the Global Admin permissions with lower administrator rights after the Akixi CX access is authorised
- service account - using an authorisation account with Global Admin permissions that can't be used to log into the M365 administration tools

M365 administrator consent and authorisation process and permissions necessary for each step

Every MSFT Teams add-on application requiring read and write access to an MSFT Teams instance needs to go through a 2-step authorisation process

Administrator consent

1. This process, better known as the "Requested Permissions" splash screen, lists all the permissions a particular application requests, allowing the SysAdmin to review and approve them.
2. **A SysAdmin user account with Global Admin privileges can only perform the Administrator consent process.**
3. The process needs to be performed one time only during the application's first deployment (each incremental permission requested by the application in its lifecycle needs to follow the Administrator consent process and requires Global Admin permission as well)
4. Given the one-time nature, the Administrator consent process **CAN** be served by a SysAdmin user account granted temporary Global Admin permission using the PIM method.

Authorisation

1. This part of the process assigns a user account that will be used to authorised subsequent application requests to read and write data from customer MSFT Teams instance
2. **A Sysadmin user account can perform the Authorisation process with one of the following privilege sets:**
 - a. **Teams Administrator + User Administrator**
 - b. **Teams Communications Administrator + User Administrator**
3. The process will be repeated throughout the application's lifetime. Hence, necessary permissions need to be permanently assigned to the SysAdmin user account.
4. Given the permanent nature of the Authorisation process, SysAdmin user account permissions **CANNOT** be granted using the PIM method.



Please note that the User Administrator permission level requested by Akixi CX is based solely on MSFT Teams Resource Account management requirements, which are based on changes to the M365 permissions structure.

[Manage resource accounts for service numbers - Microsoft Teams](#) | [Microsoft Learn](#)

! Note

Currently, Teams administrators can create and manage resource accounts without requiring any user management permissions in Microsoft 365. As part of our commitment to deliver secure solutions that meet the highest standards, we are implementing changes to the management of resource accounts. Going forward, Teams administrators will need to have user management permissions in Microsoft 365 to create and manage resource accounts. This change will take effect in the 3rd quarter of 2024.

Permissions level	Consent (Day 0)	Authorisation (Day 0)	User / Queue R-T	Presence	Historic Reporting
Global Admin	✓	✓	✓	✓	✓
Teams Admin + User Admin	✗	✓	✓	✓	✓
Teams Comms Admin + User Admin	✗	✓	✓	✓	✓

Admin Consent and Authorization process visualised (using different user accounts with different permission levels for each step)





APD-7980 is a requirement scheduled for v3.x Q2 2025 release. It will decouple the Admin consent and Authorisation procedures, offering a better user experience than the current single-flow model. The decoupled process will allow performing Admin consent and Authorisation at different times, given obtaining certain permission levels might be a time-consuming process

Authorising Akixi CX application with M365/Entra

The authorisation consent will enable the following capabilities:

- Data-feed
 - access to MSFT Graph API
 - provisioning of bots using MSFT SDK
 - bot placement in call flows
- Subscribing to MSFT Teams Presence API
- Reading M365 license store data
- Synchronising the MSFT Teams user directory
- Reading and monitoring changes to the MSFT Teams configuration
- Submitting changes to the MSFT Teams configuration (e.g. "R-T CQ monitoring")

ACXMT update to requested M365 permissions set

Akixi CX v3.1.0 upgrade (R-T Presence events), new permissions and re-consent process

Akixi CX v3.1 introduces Presence monitoring capabilities for MS Teams Telephony Server types. To receive the presence events from the customer's MSFT Teams instance, Akixi CX product will request additional permissions during the authorization and consent provisioning phase.

These new permissions include:

- Reading presence information for all users (Presence.Read.All)
- Reading and writing presence information for all users (Presence.ReadWrite.All)



These permissions will be automatically requested when creating new Telephony Servers. Existing Telephony **Servers from the v3.0 release will need to undergo a re-consent process to access the new v3.1 functionality, which includes Presence monitoring.**

Telephony Servers created in the v3.0 Akixi CX release will not be able to utilize the new v3.1 functionality until the re-consent process is completed. However, the v3.0 functionality covered by the existing consent will continue to function as expected.

Akixi CX v3.2.0 upgrade (R-T CQ monitoring, shared voicemail), new permissions and re-consent process

Akixi CX v3.2.0 introduces improvements for the coverage of the R-T CQ monitoring routing methods and exception handling cases. Starting with this release, all Microsoft Teams Call Queues configured with new supported parameters will change their designation to "compatible", and the Administrator user will be able to set the CQ into "monitored" mode, whereas previously, only the "monitored forced" was available. For the described capability to be available, the Akixi CX product will request additional permissions during the authorization and consent provisioning phase.

These new permissions include:

- Manage Exchange configuration (Delegated) (M365 Exchange Online permission)
- Sign in and read user profile (User.Read)



These permissions will be automatically requested when creating new Telephony Servers. **Existing Telephony Servers from the v3.1 release will need to undergo a re-consent process to access the new v3.2 functionality.** The “Akixi Release 3.2 Full Release Document - For Administrators” describes the process.

Telephony Servers created in the v3.1 Akixi CX release will not utilize the new v3.2 functionality until the re-consent process is completed. This includes:

- a CQ can't be placed into “R-T monitored” mode when shared voicemail exception handling is used (CQ will be placed into “R-T monitored forced” instead)
- if a CQ is already in “R-T monitored” mode and shared voicemail exception handling is enabled (CQ will be downgraded into “R-T monitored forced”)

However, the v3.1 R-T CQ monitoring functionality covered by the already consented permissions set will continue functioning as expected.

M365 permissions and Akixi CX reason to use

Permission type	Description	Akixi CX reason to use
Manage Exchange configuration (Delegated)	Allows the app to manage the organisation's Exchange environment, such as mailboxes, groups and other configuration objects. To enable management actions, an admin must assign the appropriate roles to the app user.	M365 Exchange Online permission. R-T CQ monitoring, shared voicemail CQ exception handling, allowing reading the shared voicemail address associated with destination selected in TAC.
Maintain access to data you have given it access to	Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.	Retain data access when the user session is inactive through web UI or Teams client.
Read presence information of all users in your organization	Allows the app to read presence information of all users in the directory on behalf of the signed-in user. Presence information includes activity, availability, status note, calendar out-of-office message, time zone and location.	Subscribe to the MSFT Teams Presence API, which is necessary to feed events into the Presence Dashboard and the Akixi BLF.
Sign in and read user profile	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	Support for SSO between Akixi CX App and Akixi CX web portal, using M365 authentication provider.
Read all users' full profiles (Application)	Allows the app to read user profiles without a signed in user.	Part of the MSFT Teams user directory sync process, enhanced user data, like group participation and effective call recording policy

Read PSTN and direct routing call log data	Allows the app to read all PSTN and direct routing call log data without a signed-in user.	Historic data feed
Read all call records	Allows the app to read call records for all calls and online meetings without a signed-in user.	Historic data feed
Access media streams in a call as an app	Allows the app to get direct access to media streams in a call, without a signed-in user.	Real-time data feed, deploying Akixi CX Bot
Initiate outgoing 1 to 1 calls from the app	Allows the app to place outbound calls to a single user and transfer calls to users in your organization's directory, without a signed-in user.	Real-time data feed, deploying Akixi CX Bot
Initiate outgoing group calls from the app	Allows the app to place outbound calls to multiple users and add participants to meetings in your organization, without a signed-in user.	Real-time data feed, deploying Akixi CX Bot
Join group calls and meetings as an app	Allows the app to join group calls and scheduled meetings in your organization, without a signed-in user. The app will be joined with the privileges of a directory user to meetings in your organization.	Real-time data feed, deploying Akixi CX Bot
Join group calls and meetings as a guest	Allows the app to anonymously join group calls and scheduled meetings in your organization, without a signed-in user. The app will be joined as a guest to meetings in your organization.	Real-time data feed, deploying Akixi CX Bot
Read all groups	Allows the app to read group properties and memberships, and read conversations for all groups, without a signed-in user.	R-T CQ monitoring sync, shared voicemail group information
Send mail as any user	Allows the app to send mail as any user without a signed-in user.	R-T CQ monitoring sync, send shared voicemail messages (CQ exception handling)
Read organization information	Allows the app to read the organization and related resources, without a signed-in user. Related resources include things like subscribed SKUs and tenant branding information.	Part of the MSFT Teams user directory sync process, organization data, including available licenses
Read presence information for all users	Allows the app to read presence information of all users in the directory without a signed-in user. Presence information includes activity, availability, status note, calendar out-of-office message, time zone and location.	Subscribe to the MSFT Teams Presence API, which is necessary to feed events into the Presence Dashboard and the Akixi BLF.
Read and write presence information for all users	Allows the app to read all presence information and write activity and availability of all users in the directory without a signed-in user. Presence information includes	Future capability. Subscribe to MSFT Teams Presence API, setting agent status from dashboard/report.

	activity, availability, status note, calendar out-of-office message, time zone and location.	
Read all users' full profiles (Delegated)	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.	Part of the MSFT Teams user directory sync process, enhanced user data, like group participation and effective call recording policy
Read and write all users' full profiles	Allows the app to read and update user profiles without a signed in user.	R-T CQ monitoring sync, designed to update Resource Account licenses. Since MSFT requires RAL for each voice app, this requirement will be removed from future Akixi CX releases.
Access Microsoft Teams and Skype for Business data as the signed in user	Allows the app to have the same access to information in the directory as the signed-in user.	Legacy permissions; compatibility reasons until obsoleted by MSFT. Part of the MSFT Teams user directory sync process, enhanced user data.

Example M365 request prompt for Akixi CX authorisation



markwatson@akixi.net

Permissions requested

Review for your organisation

Akixi Staging



This app would like to:

- ✓ Manage Exchange configuration
- ✓ Maintain access to data you have given it access to
- ✓ Read presence information of all users in your organization
- ✓ Sign in and read user profile
- ✓ Read all users' full profiles
- ✓ Read PSTN and direct routing call log data
- ✓ Read all call records
- ✓ Access media streams in a call as an app
- ✓ Initiate outgoing 1 to 1 calls from the app
- ✓ Initiate outgoing group calls from the app
- ✓ Join group calls and meetings as an app
- ✓ Join group calls and meetings as a guest
- ✓ Read all groups
- ✓ Send mail as any user
- ✓ Read organization information
- ✓ Read presence information for all users
- ✓ Read and write presence information for all users
- ✓ Read all users' full profiles
- ✓ Read and write all users' full profiles
- ✓ Access Microsoft Teams and Skype for Business data as the signed in user

If you accept, this app will get access to the specified resources for all users in your organisation. 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. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

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

Cancel

Accept

Entra/Azure Tenant ID, key TelSys identifier

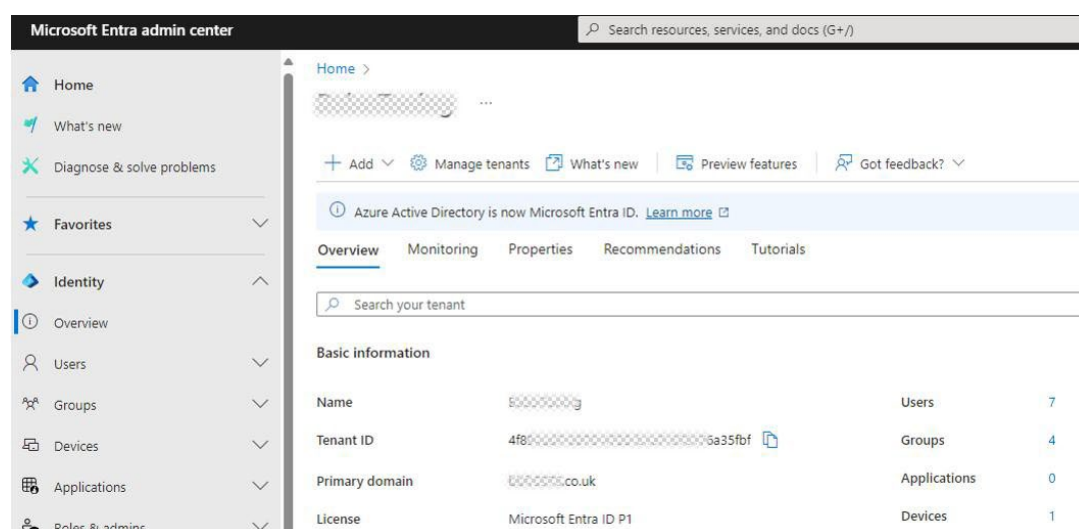
Overview

The Akixi CX MSFT Teams service relies on M365 Azure/Entra tenant ID. This tenant ID is utilized to recognize the Telephony Server throughout the entire Akixi CX platform and serves to locate the Telephony Server within the Akixi CX GSL. It is also used to request the monitoring of users and CQ bots. Finally, the tenant ID facilitates the assignment of users to Telephony Servers when the Akixi CX App (Teams desktop) is in use. The Service Provider will request the tenant ID during the Telephony Server provisioning process.

Where to find the Azure Tenant ID

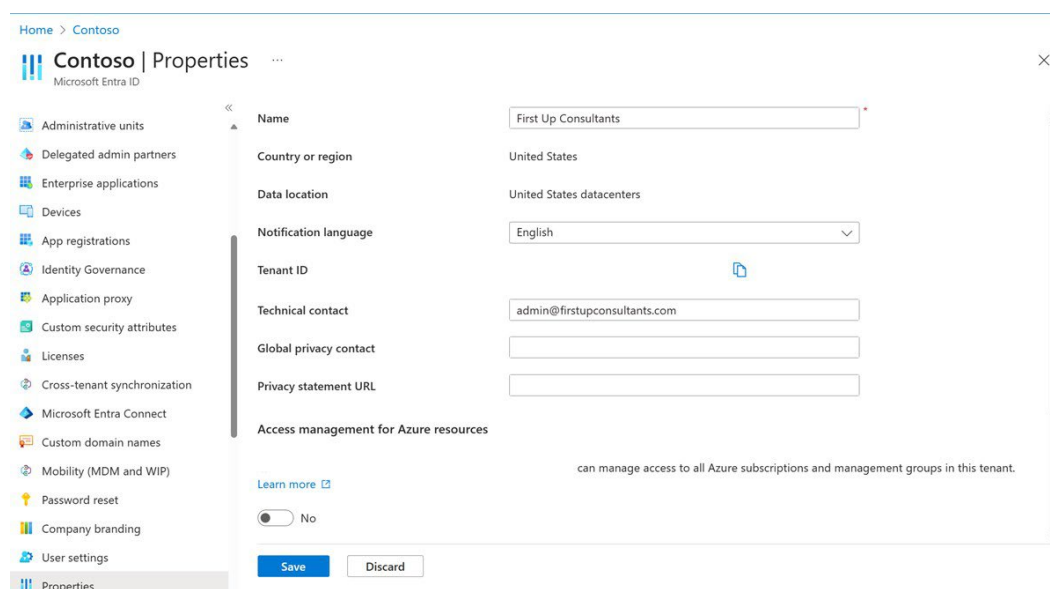
Microsoft Entra admin center

The customer M365 tenant ID can be easily found on the overview page with the Microsoft Entra admin center. Sign into the Microsoft Entra admin center with a user granted at least Global Reader permission. Browse to Identity > Overview. Scroll to the Tenant ID section.



Azure portal

The customer M365 tenant ID can also be found in the Azure portal. Sign into the Azure portal. Browse to Microsoft Entra ID > Properties. Scroll down to the Tenant ID section.



Entra/Azure TenantID correct format when configuring Akixi CX Telephony Server

The Entra tenant ID is a valid GUID; it should be returned in lowercase format and without brackets or parentheses (as per RFC 4122, Section 3), such as "1111aaaa-bbbb-2222-cccc-3333dddd4444".

Using uppercase Tenant IDs in TelSys configuration leads to an issue where the Akixi CX GSL is unable to register the new TelSys properly, preventing user/queue capture. The same principles apply to feeding the TenantID parameter through the Akixi CX provisioning API.

Functionality that enforces lowercase on the TenantID parameter, regardless of the use or API input, is a Akixi CX roadmap item.

Modify Telephony Server

Details

Communication

Default Site Settings

Licence Management

Advanced

Telephony Server Type: Microsoft Teams

Integration Mode: Real-Time

Auth Email: adminEmail@emailaddress

User Authenticated with: adminEmail@emailaddress

Tenant ID:

CORRECT: 1111aaaa-bbbb-2222-cccc-3333dddd4444

INCORRECT: 1111AAAA-BBBB-2222-CCCC-3333DDDD4444

Grant Admin Consent

✓ This Telephony Server has already been authorised.

✓ Communication Enabled

□ In-Service

Native app setup **Help** **Save** **Cancel**