CXA

Teams + Call Reporting

Teams Tenant/Global Admin

Initial Setup 101

Quick Start Guide

MOMENTUM

powered by: akixi

Teams + CXA Service Implementation Requirements

The following must be in place and (when requested) the account information must be provided to the Service Provider prior to the implementation of the Teams CXA Call Reporting service to allow stable synchronization with the customer's Teams account:

1. A dedicated Teams Global Admin account to be used for initial and continuous consent/authorization/sync with CXA Call Reporting.
   Preferably a Teams Global Admin service account used exclusively to manage the sync for the CXA service hosted at momentumakixi@domain.com

2. Teams Global Admin account should be set to have a non-expiring complex password with MFA disabled.
   This is to reduce the potential for disconnection and data loss.
   Note: *If the password expires or is erroneously altered, it breaks the connection with CXA and can result in negative service impacts. If not corrected and restored quickly, visibility and retention of call data can be impacted and data loss can occur as Microsoft does not retain historical call data past 28 days.*

3. If granularity of permission for the Teams Global Admin account is needed, the following should be set up on that Teams Global Admin service account:

   a. Azure AD Admin, Teams Administrator, and Graph API consent permissions.

   b. The ability to access all call data (should be covered if item **a.** above is complete)

   c. The ability to receive email sent to the UPN for the Global Teams Admin service account. *Email is used for onboarding, access, instructions, ongoing service alerts, and system newsletters for upcoming features, maintenance, and scheduled downtime.*

Per Akixi

- For Admin **Consent:** the Global Administrator role is required (even if temp permissions given through PIM).
- For **Authorization:** the Global Admin account must have one of the following combinations through the life of the CXA integration going forward:
  - **Global Admin**
  or
  - Teams Admin + User Admin + Exchange Admin
  - Teams Comms Admin + User Admin + Exchange Admin
  - Teams Admin + User Admin + Exchange Recipient Admin
  - Teams Comms Admin + User Admin + Exchange Recipient Admin - *Note: This basic set of permissions is the bare minimum permission set that the Teams Admin can have to authorize.*

Important Note:
It is the responsibility of the Customer to decide how to accomplish the above within the framework of their M365, Business/Security practices, and financial structure prior to integration/implementation.

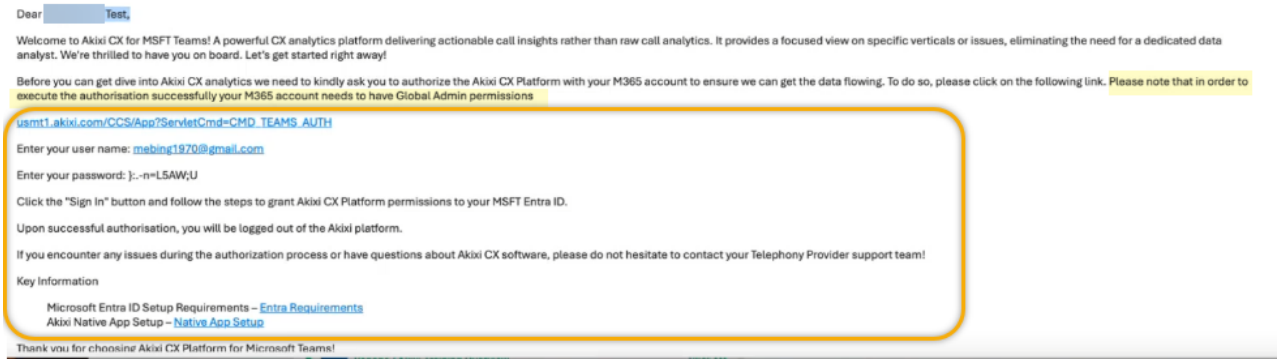
The requirements outlined above are in addition to the primary preparation requirements to have purchased the appropriate licenses for Teams CXA from the service provider and to have the correct/compatible Teams telephony licensing that is necessary to accomplish implementation with full functionality.

Contact your service provider Implementation Project Manager with questions about the steps outlined below.

1. Teams Sync and Set In Service

Service Provider CXA Telephony Server Creation

Upon successful MS Teams Telephony Server CXA account creation based on CXA licenses ordered to initiate the Call Reporting implementation, the customer's authorized Teams Tenant/Global administrator will receive an email containing the information needed to consent to allow sync and setup within their Teams tenant. Here is an example:



Dear [redacted] Test,

Welcome to Akixi CX for MSFT Teams! A powerful CX analytics platform delivering actionable call insights rather than raw call analytics. It provides a focused view on specific verticals or issues, eliminating the need for a dedicated data analyst. We're thrilled to have you on board. Let's get started right away!

Before you can get dive into Akixi CX analytics we need to kindly ask you to authorize the Akixi CX Platform with your M365 account to ensure we can get the data flowing. To do so, please click on the following link. Please note that in order to execute the authorisation successfully your M365 account needs to have Global Admin permissions

usmt1.akixi.com/CCS/App?ServletCmd=CMD_TEAMS_AUTH

Enter your user name: mebing1970@gmail.com

Enter your password: }:.-n=L5AW;U

Click the "Sign In" button and follow the steps to grant Akixi CX Platform permissions to your MSFT Entra ID.

Upon successful authorisation, you will be logged out of the Akixi platform.

If you encounter any issues during the authorization process or have questions about Akixi CX software, please do not hesitate to contact your Telephony Provider support team!

Key Information

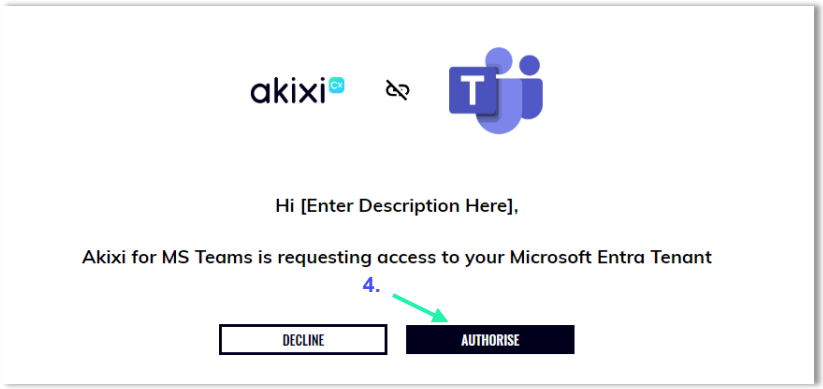
Microsoft Entra ID Setup Requirements – Entra Requirements
Akixi Native App Setup – Native App Setup

Thank you for choosing Akixi CX Platform for Microsoft Teams!

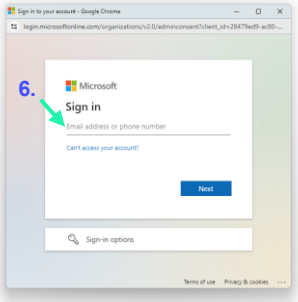
1.a. Grant Authentication and Consent

REQUIRED Once the Teams Global Admin (defined by the customer in the UIF) has received the 'Consent Email', they will need to click the URL in that email to begin. This action will open a browser to the correct CXA instance. Contact the Service Provider to verify the URL and to work through the process with your Implementation Project Manager and Implementation Engineer. The customer administrator will be required to:

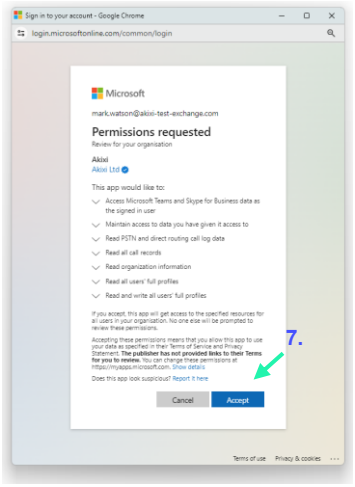
1. Enter the username and password credentials provided in the email
2. Accept the terms and conditions
3. Change the password when prompted.
4. Click **Authorise** when prompted.



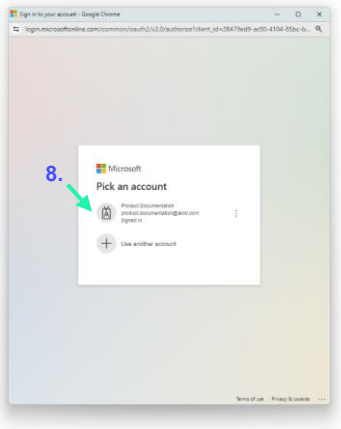
5. A Microsoft Authentication screen will pop up
6. Enter your username and the password here and click **Next** to continue...



7. Click ‘Accept’ Consenting to the requested permissions
   Required Permissions
   I. Access Microsoft Teams & Skype for Business data as the signed in User
      Access Microsoft Teams and Skype for Business data based on the user's role membership
   II. Maintain access to the data 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.
   III. 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.
   IV. Read all call records
      Allows the app to read call records for all calls and online meetings without a signed-in user.
   V. 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.
   VI. Read all users’ full profiles
      Allows the app to read user profiles without a signed in user.
   VII. Read and write all users’ full profiles
      Allows the app to read and update user profiles without a signed in user.



8. Enter the username and password when prompted and Click on the correct User Name in the dialog presented
9. Click Authorise when prompted.



Once these steps are completed and CXA is ready to synchronize with the Teams Tenant, the dialog closes and the Teams Global Admin is automatically logged out.

The sync process begins.
While the sync is in process, the Teams Admin may complete step 1.b. (optional) if they wish to utilize the Teams App for CXA

Please give the sync process a day to fully complete before moving on to step 1.c.

First Synchronization

Upon successful completion of the Consent and Authorization steps noted above, Akixi CXA will perform its first synchronization with the customer's Teams tenant, where it will pull the data for:

1. All MS Teams Users in the environment with OR without TPS/EV (telephony) licensing
2. All Voice Apps/Devices (resource accounts like Momentum Teams Fax, Auto Attendants, Hunt Groups, & Call Queues)

During the sync, the MS Teams accounts are added to CXA in a Monitoring Deactivated (unlicensed) state. This means that Post-Sync, call reporting monitoring is NOT active for any user or device until an Administrator assigns an available license to them (as appropriate) in CXA > Administration > User Management and then sets CXA to IN SERVICE.

1.b. (Optional) 3rd Party Analytics Teams App Integration

During the initial Teams + CXA implementation and sync process (your Service Provider's Implementation PM can walk through the process with you), the Teams Tenant/Global Admin can also install and set up the optional native CX **Analytics** app for use by Call Reporting eligible users in their Teams environment.

- You will need sufficient Teams Admin access to perform the installation/consent tasks for your org (Global Admin is necessary) during the Teams + CXA implementation and sync process.
  Your Service Provider's PM/Implementation Engineer will assist.
- Basic Instructions to install and allow users to find, install, and use the Analytics app for Teams can also be found in ***CXA > Administration > Telephony Servers > Communications*** as you and the Service Provider PM work through this process.
- **Obtain and download the Teams Analytics native app zip file from the Service Provider.**

Install the CX Analytics App in Teams Admin Center

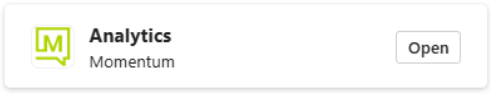
- Log into the **Teams Admin Center** with sufficient global access to the tenant.
- In the left navigation menu, choose **Teams apps > Manage apps**
- In the top right, dropdown '**Actions**' and select '**Upload new app'**
- Click '**Upload'**
- Browse and select the **Native App Zip File**
- Confirmation of the app added is displayed as expected

Manage the App in Teams Admin Center

- Log in to **Teams Admin Center**
- In the left navigation menu go to **Teams apps** and select **Manage apps**
- **Search** for the app and click on the app **name**
- **Management Options**
  1. **Assignment** – Admin may assign to the whole Org – or (highly recommended) only to individual users they wish to allow to add or use the Analytics app in their Teams .
  2. **Permissions** – Recommended that the Global Administrator review and consent to the permissions presented, so the admin does not have to grant consent each time an authorized user attempts to add the App from their Teams Apps section.

Authorized Users Can Add the Application to Teams

While working in the Teams Application (logged in):

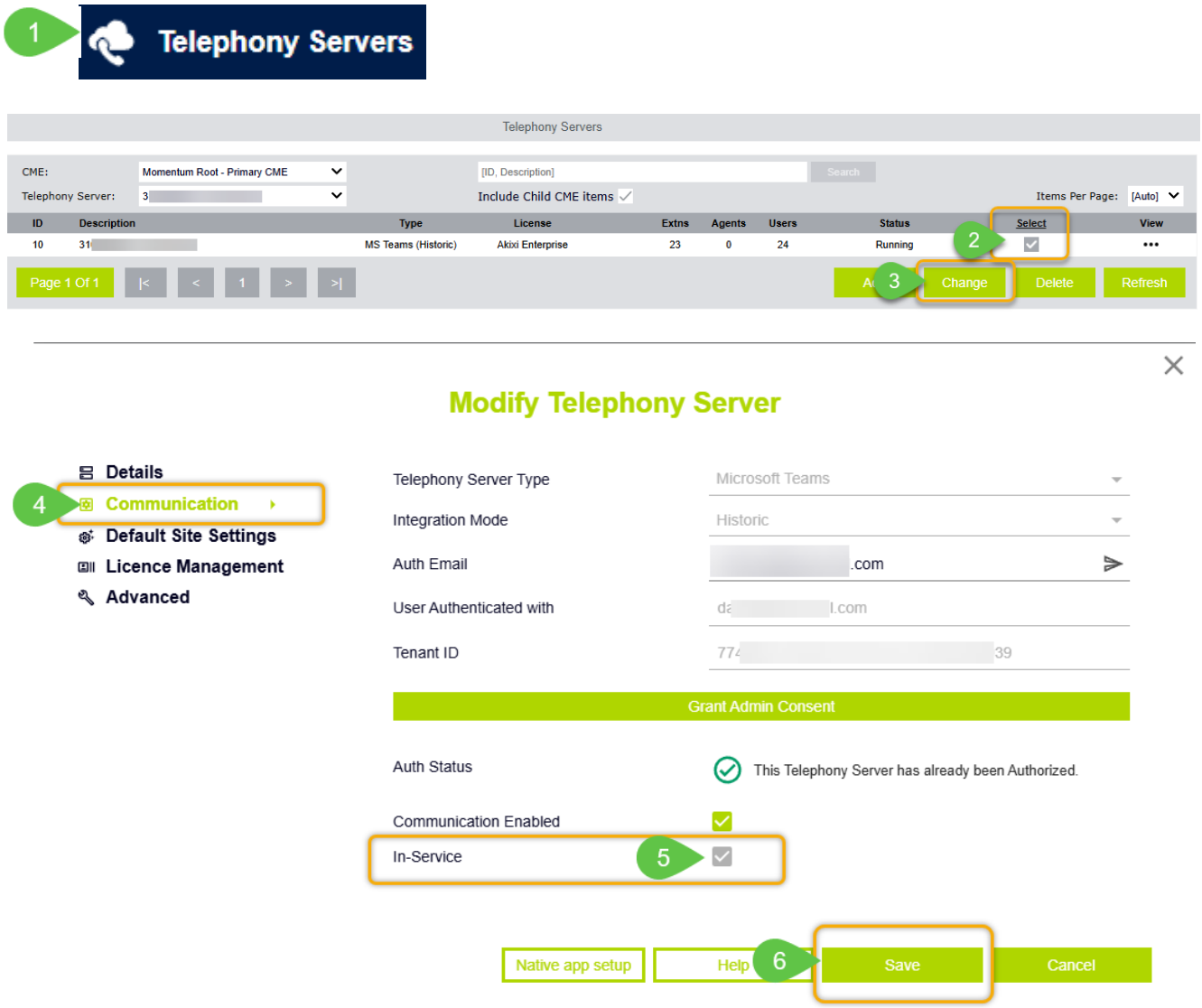


1. In the left navigation menu, select **Apps – Built for your org**
2. Search for **Momentum Analytics**.
3. Click **Open** and then click on the App's **Add** button and follow any steps to set up or get consent, if prompted.
4. Once done, the **Analytics** app will then appear in the Left navigation menu and can be **Pinned.**

1.c. Set In-Service

REQUIRED Once sync completes, the CXA Teams Tenant Admin / Global Admin must return to their CXA Administration portal to set Call Reporting to **In Service**.

1. Go to: **Administration > Telephony Servers**
2. Select the check box next to the org's telephony server (right side of the list).
3. Click on the **Change** button below the list.
4. Click on the **Communication** menu option in *Modify Telephony Server* dialog.
5. Click to place a check in the box next to In-Service.
6. Click on the **Save** button.



2. Post-Sync User and Queue Setup

Once the initial Teams to CXA integration and data sync has been run and the system is running, and the Tenant Admin receives word via Email that the environment is ready to continue to perform more setup, some additional tasks must be completed to get licenses assigned appropriately for all of the accounts that will be monitored for call reporting and for those *people* who will also be allowed to access CXA to perform work (create and manage reports, etc.) within the Call Reporting portal.

These setup tasks can be performed by the CXA Teams Tenant Admin/Global Admin (the primary or first Admin created) initially – as well as by the Non-Reporting Admin accounts the Teams Tenant Admin/Global Admin creates or by Advanced license holding Supervisors that the Tenant Admin grants the **User Manager** Administrative Role.

Most user (or queue) management tasks will be performed in the *Fast Provisioning* section; however, this guide also offers a brief primer for some other Administration sections that may display but not be accessed or modified often – or that display information but may not allow changes.

Please note – some Administration sections offer Read Only views at the Tenant level.

To learn more and review useful information for the various sections in CXA for Administration:

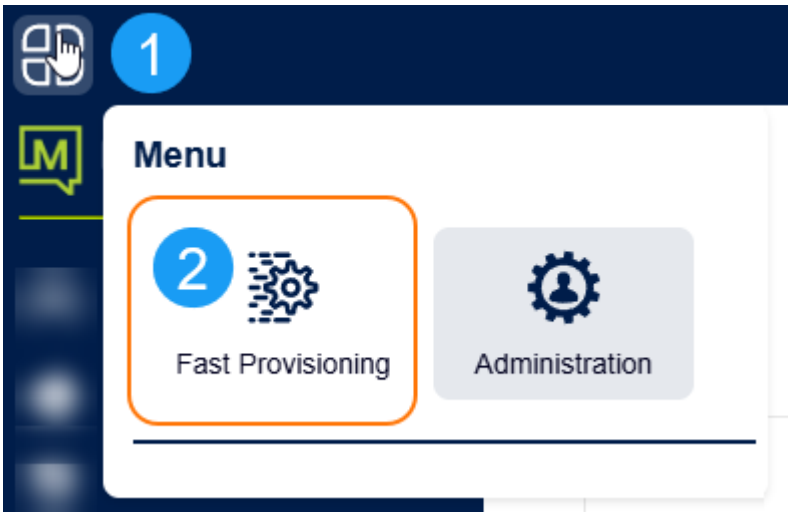
Reference the CXA Online Help File by clicking F1 while working in CXA.

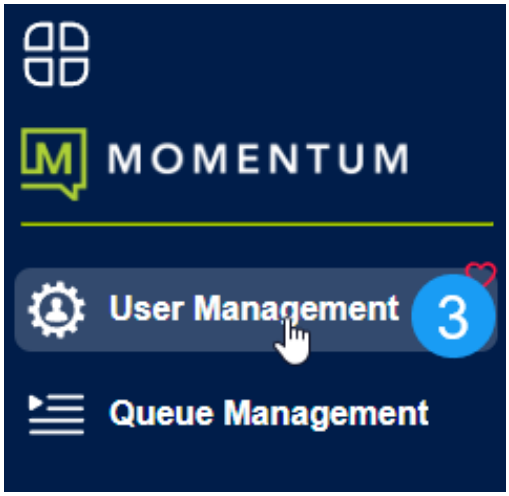
OR click on any of the ? Help icons you see while working in CXA Administration sections

2.a. Assign Licenses

REQUIRED. Once synced, the CXA Teams Tenant Admin / Global Admin must sign in and assign available licenses to each of their users. The Fast Provisioning section displays if signed in with credentials that were defined to allow Teams Tenant/ Global Admin access, or User Manager role privileges.

This section offers access to the User Management section – and for some roles it also displays the Queue Management.





Go To Fast Provisioning > User Management

Administrators can manage user license assignments in Fast Provisioning > User Management. This is where to assign/remove one or more user license assignments and review license usage statistics. Tools to filter, sort, search, and view more pages are provided.

Post sync, accounts shown in User Management are unlicensed and awaiting assignment. Account data includes the UID, compatible teams license type, and email address.

Basic configuration for user call data monitoring and/or reporting management tool usage requires the sync'd data including a correct email address, a CXA license type selection PLUS assignment (checkmark).

To Assign All Monitored User Licenses

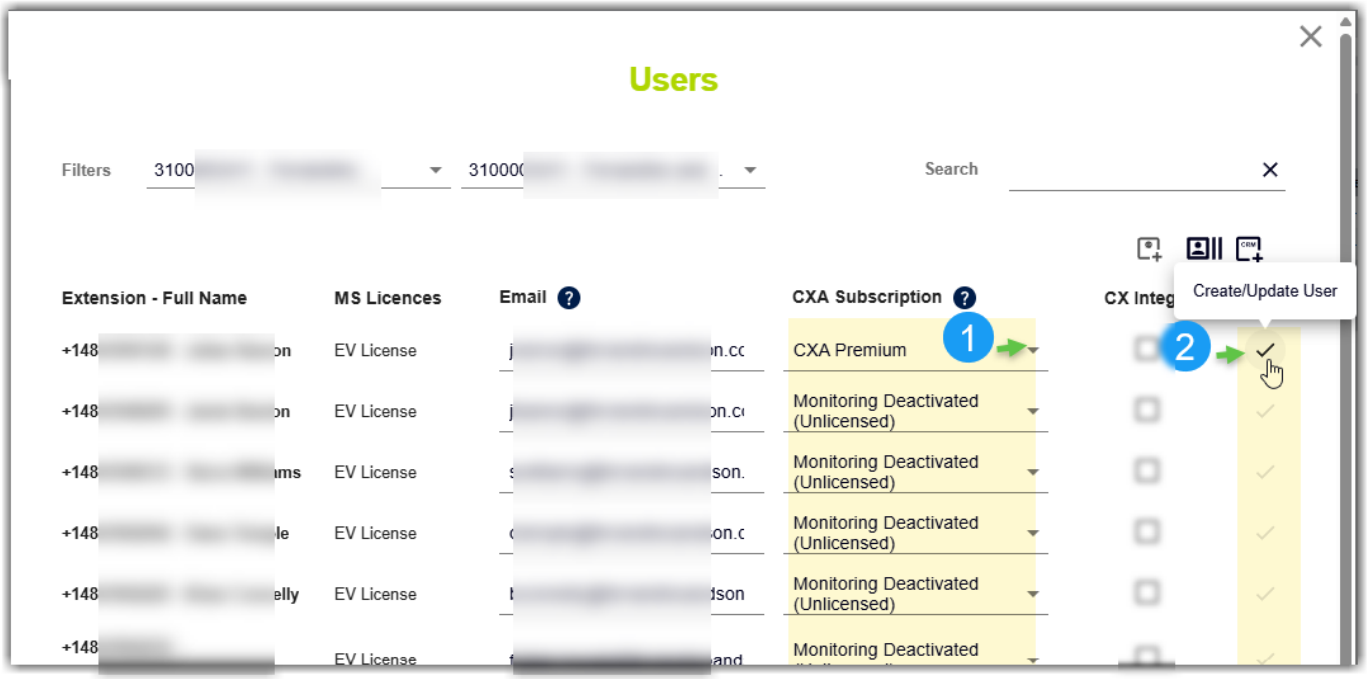
Any account that will be monitored for call reporting must be assigned a monitoring license and then Enabled.
By default all listed accounts are NOT being used or monitored and call data will not be retained for Call Reporting.
While working in User Management:

Locate the extension/user/device to be assigned a license within the table.
Note: By default, all identified accounts synced from Teams will be set as *Monitoring Deactivated (Unlicensed)* until assigned a CXA subscription (reporting license) type and enabled.

1. Select the required **Subscription Type** using the ▼ drop-down (right side of the list).
   The selection options will only include license types purchased and available to be assigned currently (unassigned/unused).

   - Assign a **CXA Standard** or **CXA Premium** license to the accounts whose calls will simply be monitored by CXA.

2. Once a license type has been assigned, click the adjacent ✓ check mark to **Save** the change.
   Once enabled and saved, the account now has an enabled license and will be monitored by CXA and if it is a user, they *may* be allowed limited read-only access to their own reporting statistics (if this was authorized by the Teams Admin and the Teams Analytics app has been implemented).
   REPEAT TO ASSIGN AND ENABLE AVAILABLE MONITORING LICENSES TO DESIRED ACCOUNTS IN THE LIST



To Assign All Reporting Supervisor Licenses

The **CXA Advanced** license is required to be assigned to any user who will be allowed to create, edit, schedule, run, and manage reports for statistical analysis using the tools in the CXA portal Reports areas. This means the **Advanced** License must be assigned to any user account that needs to access the CXA portal for report creation and management tasks, as well as to those who will be allowed to work with Reporting tools ***and*** might be granted a lesser Administrative role that offers additional access to assist other users or accounts.

Locate the extension/user/device to be assigned a license.
Note: By default, all identified accounts synced from Teams will be set as *Monitoring Deactivated (Unlicensed)* until assigned a CXA subscription (reporting license) type and enabled.

1. Select the required Subscription Type (ADVANCED) n the ▼ drop-down (right side of the list).
   The selection options will only include the license types purchased and currently available to be assigned (unassigned/unused). Contact the service provider if you determine you need to add more licenses for assignment.

   - Assign **Advanced** licenses to the accounts of individuals who will create and manage reports in CXA.

2. Once a license type has been assigned, the Admin must click the adjacent ✓ check mark to Enable and Save.
   The account now has an enabled Reporting Supervisor license with a Roll that will allow them to view, create and manage reports in CXA. The user is now ready to begin working with reports and analytics in CXA.

   REPEAT TO ASSIGN AND ENABLE AVAILABLE ADVANCED LICENSES TO DESIRED SUPERVISOR ACCOUNTS IN THE LIST

To Remove License Assignments

To delete a user's license assignment and stop reporting on their line, or to revoke Reporting Supervisor access:

1. Navigate to the "User Management" menu once more
2. Locate the user you wish to revoke reporting access within the list
3. Click the **X** in the far right column beside their account information
4. Click on the **Trash Can** icon to confirm removal of the license assignment from that account when prompted.
   The license assignment is removed from the selected account and then becomes available for assignment to another account.

Create a Non-Reporting Secondary Admin Account

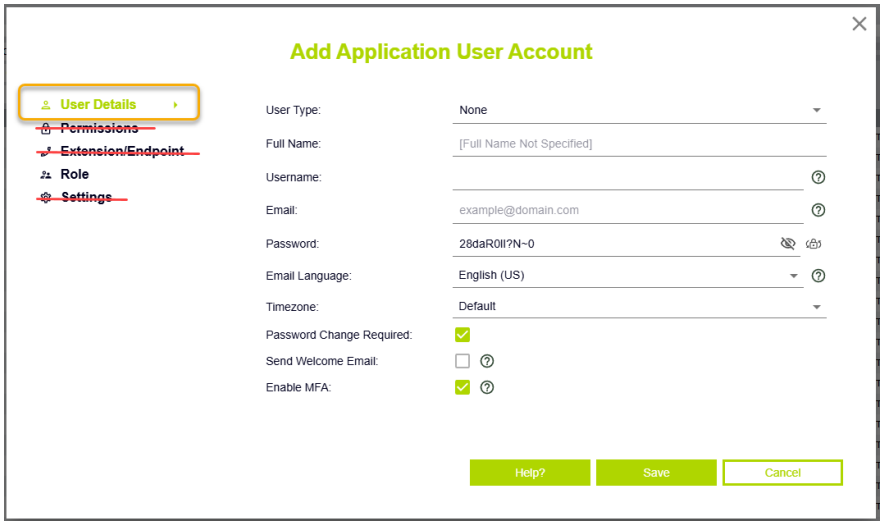
OPTIONAL This is the only manually created account type (and role) that does not require the assignment of a monitoring license (CXA Standard or Premium) or a **CXA Advanced** license as they will **not** be monitored nor will they be granted access to any of the Reporting tools. It can be created manually; however, it is important to build this type of account correctly. Use the following steps:

1. Click the menu icon in the top-left of the CXA portal.
2. Select **Administration**.
3. Select **Application Users**.
4. Click **Add**.

   This opens the Add Application User Account dialog with the User Details tab in view.

In the User Details Tab:

5. Enter or select the following in the User Details tab, as needed or required:
   - **Subscription Type** = Required. **NONE**. *Leave this field set to the default of None.*
   - **Full Name**: Required. *The full name of the user to be assigned to use this account.*
   - **Username**: Required. *This is the username that the Application User will use when signing into the application. This is often the same as the user's email address, although it does not have to be.*
   - **Email**: Required. *This field should contain the email address of the user. Email messages sent by the application will be sent to this email address, including the initial access email, password updates, and notifications.*
   - **Password**: Required. *This field determines the password that the Application User will need to sign into the application. Enter a password or use the Randomizer on the right to create a password.*
   - **Email Language**: *This field specifies the language to use for any emails sent to the user.*
   - **Password Change Required**: Suggested. *When the check box is selected, this setting forces the user to change their password when they next sign into the application.*
   - **Send Welcome Email**: *Click to enable this setting to send a welcome email to the email noted above as soon as this account is Saved.* ***Important****: If you are not ready to complete all setup for this user, do not enable this option yet.*
   - **Enable MFA**: *If displayed, when this check box is selected, the user must use Multi Factor Authentication when logging in. That means they will use both the username and password credentials set here and a One-Time-Passcode from an Authenticator app (or sms) they set up to assist with to sign in. If this check box is not set, they only need to use their username/password.*
   - You can click **Save** now and return later to complete the full setup for this user or continue to set the Role.

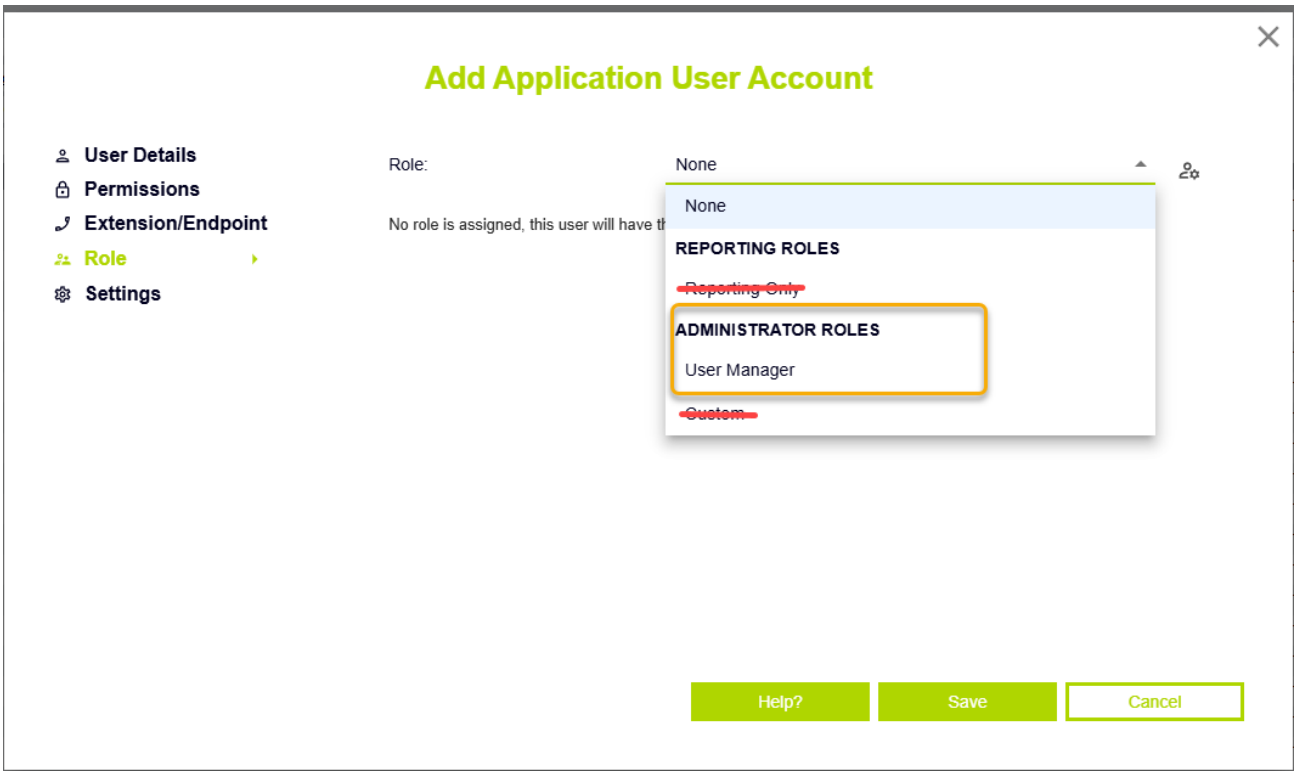


In the Roles Tab:

Once an Application User account has been created in the ***User Details*** tab, the next step is to assign the user their **Role** in the Roles tab. This determines the level of access for the account holder. Roles are categorized either as Reporting Roles or Administrator Roles. This role is an administrator role.

6. Choose the Role titled **User Manager** in the Administrator role section of the drop-down menu. This role offers the user sufficient access to assist other Call Reporting account holders as a non-primary administrator who can add/remove license assignments, assist with user access issues, copy reports from one user to another, and "sign in as" other users to verify cloned reports arrived as they should when sent or to review report setup.

   Note: Never select Custom or attempt to change the role to modify access permissions without consulting with the Service Provider first. These actions can have negative impacts on system access, functionality, and/or support service level agreements.



All Other Tabs

7. **SKIP** all of the other tabs and leave all fields and settings within them set to their defaults.

Setup for the Non-Reporting Admin account is now ready.

8. Click on the **Save** button to complete the account setup and send the welcome email with the initial access credentials.

About Permitted Reporting Portal Role Assignments Per License

The following roles are allowed to be assigned to Licensed CXA users:

Monitored User = Reporting Only Role

Set By Default. If an account is assigned a monitoring license (CXA Standard or Premium) in User Management, the system auto-assigns a limited access Role in their Application Users profile. These accounts will be given the **Reporting Only User** role by default which does not need to be changed. With a monitoring license assignment, this role allows a user to have limited read-only access to the user's own recent statistics in the Analytics Teams app (if in use or allowed by the Teams Admin). *Do **not** alter the Role settings or attempt to modify any default permissions.*

Advanced License + Reporting Only Role

Set By Default. When granted an **Advanced** license in CXA, the system assigns the user the **Reporting Only User** role by default. With an Advanced License, the *Reporting Only User* role permits the user to access all of the reporting management and creation tools provided for Report management within the CXA Portal or the Analytics Teams app (if in use or allowed by the Teams Admin). This is not an administration role - but does offer all of the useful tools a Supervisor might need to create and manage reports. *Do not alter the Role settings or attempt to modify any default permissions.*

Advanced License + User Manager Role

If a CXA Reporting Advanced license user requires the ability to work with Reporting tools *and* be granted administration-level access to copy reports to other Reporting Users, 'Sign In As' other Reporting Users, or view the list of Devices in their environment, PLUS assist the Teams Tenant/Global Admin with license assignment tasks in the Fast Provisioning > User Management section, they can be given the **User Manager** role if visible in their system. *Do not alter the Role settings or attempt to modify any default permissions.*

Along with access to the CXA portal Reporting management tools, those Advanced license holders assigned a *User Manager* role can also perform or see the following in the **Administration** section:

- **View Devices**: Review the Devices within their environment that are currently licensed to be reported on in the Administration section of the portal.
- **View Agents**: Review the list of Agents within their environment that are currently licensed to be reported on in the Administration section of the portal.
- **View, Add, Modify, and Delete Directory Entries**: Review the Directory listings and manage entries in the Administration section of the portal.
- **View Codes**: Review all the Account and Not-Available Codes that have been synced from Teams and are available to report on.
- **Application Users:** Review the list of users in their system, view user profiles, Change/edit user access credential information like passwords and user name, or resend a welcome email with credentials, plus:
  - **Copy Reports To**: Use the Copy Reports to other users feature in the Application Users section.
  - **Sign In As** (emulation/impersonation): Use the 'Sign In As' feature in the Application Users section to view and make changes to reports as though signed in as other users within their environment. Note: when using Sign in as, the user has only as much access to CXA features and tools as the person they are emulating.

And within **Fast Provisioning**:

- Access to User Management for some Admin-level user license assignment tasks.
- Access to Queue Management (if in use)

2.b. Review Queues

OPTIONAL Sufficient Administrator access permissions are required to view or modify Queue monitoring status settings for Teams call queues (resource accounts, etc.). Typically, once licensed to be monitored by an Admin, the monitoring status of queues should **not** be modified in this section . Admins can contact the Service Provider for assistance.

1. Click the menu icon in the top-left of the CXA portal.
2. Select **Fast Provisioning**.
3. Select Queue Management.

Search and Filter Available Queues

The search box allows data entry to specific terms for lookup. Simply type in the Search box and press the Search button to search through the pages of records to find matches. Use the available dropdown menus in the top left corner of the screen to filter the list view, as needed. Selecting one of the filter options from the dropdown menu and all matching listings display below.

Check Queue Monitoring Status

By default, all queues are set to Historic (up to 1 second ago) monitoring because that is always supported.

Queues should be compatible and be monitored for full reporting functionality.

Enable: For all call queues displayed to you, the monitoring status can be modified (if the option is available) by clicking the dropdown icon beside the call queues current monitoring status selecting the appropriate option.

Disable: Monitoring for call queues currently being monitored can also be disabled by clicking the cross icon beside the associated call queue.

Authorized Admins may also have the ability to choose all call queues and set monitoring to *enabled* or *disabled* in bulk by clicking on the respective icon.