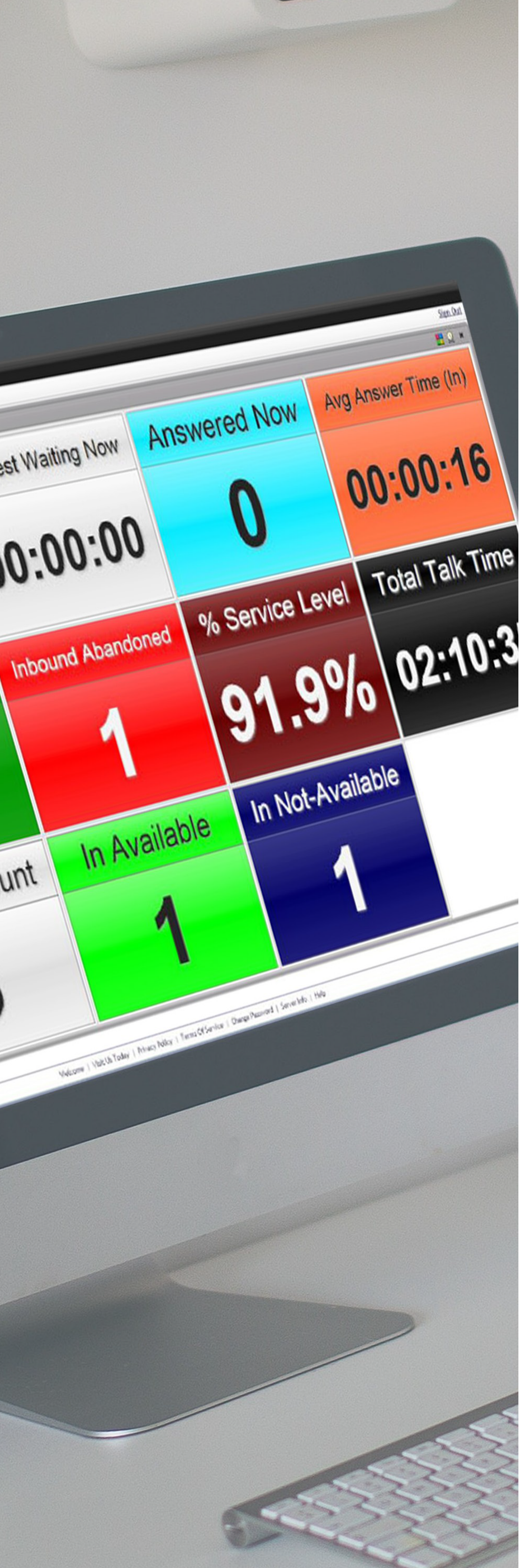


CXA

Teams + Call Reporting

Teams Tenant/Global Admin

Getting Started 101

Quick Reference Guide

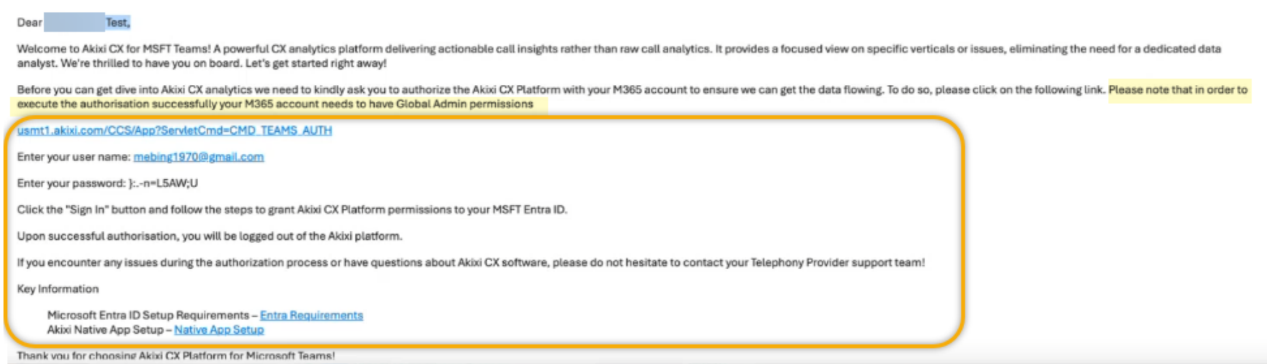
MOMENTUM

powered by: akixi CX

1. Teams Consent, Authorization, and Sync

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:



Dear 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

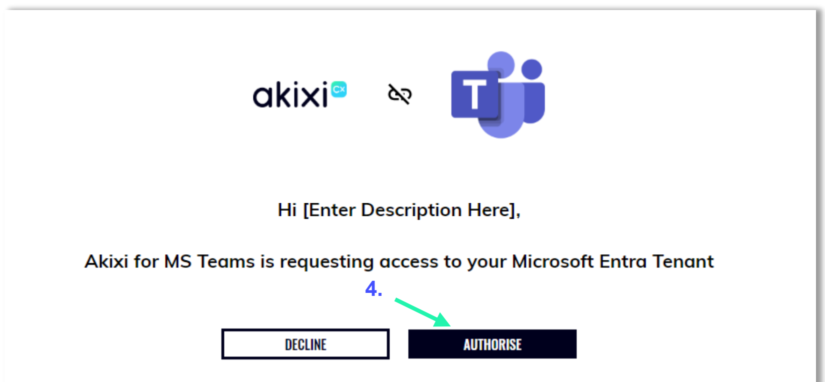
Microsoft Entra ID Setup Requirements – Entra Requirements
Akixi Native App Setup – Native App Setup

Thank you for choosing Akixi CX Platform for Microsoft Teams!

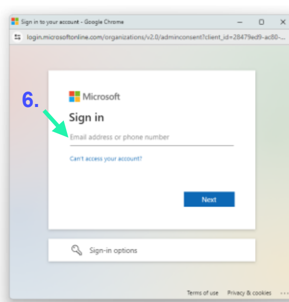
Authentication and Consent

Once the customer sysadmin has received the 'Consent Email', they will need to click the URL which will take them to the correct CXA instance. Contact the Service Provider to verify the URL and to work through the process with your Implementation Project Manager. The customer administrator will be required to:

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



5. A Microsoft Authentication screen will pop up
6. Enter username and new password here and click next



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.

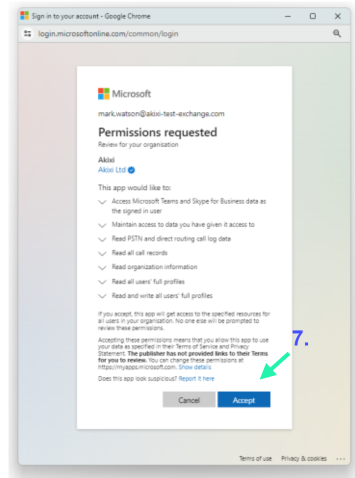
III. Read PSTN and direct routing call log data
Allows the app to read all PSTN and direct routing call log data without a signed-in user.

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.

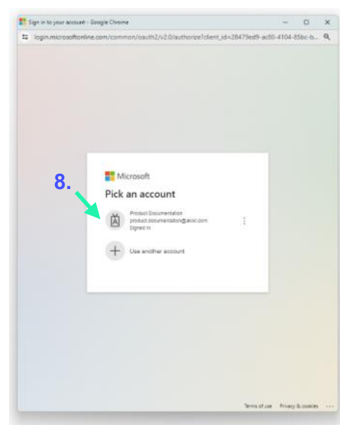
VII. Read and write all users’ full profiles
Allows the app to read and update user profiles without a signed in user.



8. Enter username and password and Click on User Name on next

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 logged out.



First Synchronization

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

1. MS Teams Users with OR without TPS/EV (telephony) licensing
2. All Voice Apps/Devices (resource accounts like Auto Attendants & Call Queues)

During the sync, MS Teams accounts are added to CXA in a Monitoring Deactivated (unlicensed) state. This means that 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 > Manage Users.

(Optional) Analytics Teams App Installation 101

Tenant Admin Preparation

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

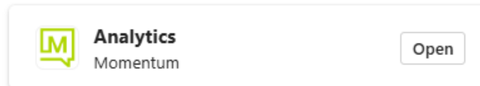
Manage the App in Teams Admin Center

- 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.

Steps for Your Teams Users to Add the CX Analytics App to their MS Teams

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**

Noted Limitations for the Teams CX Analytics App

In Browser Web App Use

- Strongly recommended not to create / use additional Dashboards

App Installed on Local Machine

- Limit to (4) individual reports within any Dashboards you create or use

2. Post-Sync License & User Management Tasks

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 should 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 *Easy 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:

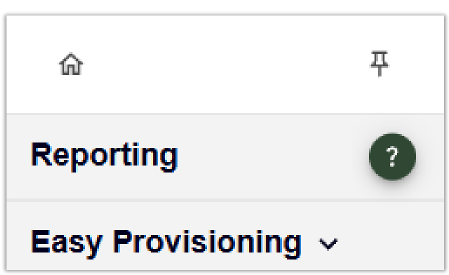
Reference the CXA Online Help File by clicking F1 while working in CXA.
OR click on any of the ? Help icons you see while working in CXA Administration sections

Assign Licenses

Easy Provisioning > Manage Users

Once synced, the CXA Teams Tenant Admin / Global Admin must sign in and assign available licenses to each of their users. The Easy 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 Manage Users section – and for some roles it also displays the Manage Queues section.

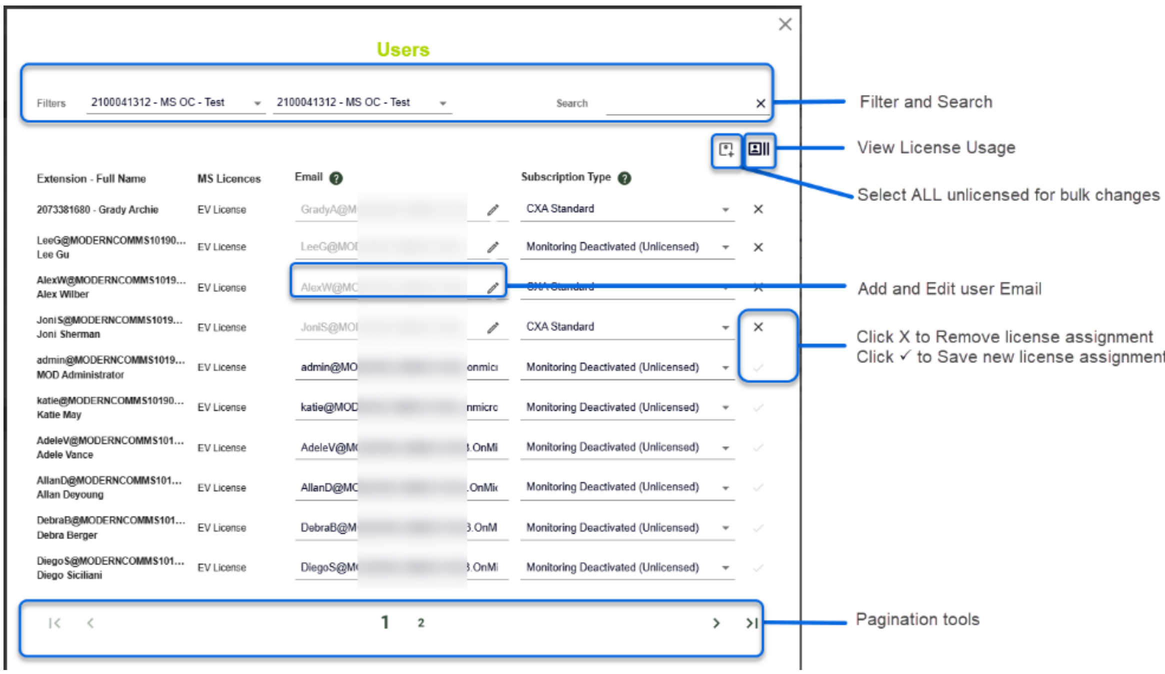


Manage Users

Easy Provisioning > Manage Users

In Easy Provisioning, Administrative users can assign licenses to accounts. In this area, those with Admin access can update one or more user's license assignments and review license usage statistics.
Tools to filter, sort, search, and view more pages are included in this area.

The sync between Teams and CXA adds information required for configuring users via the Easy Provisioning section.
The Username information is the telephony platform user ID (auto filled). This data is displayed within the table.
An Email address is required for license assignment. Admins must assign and enable the subscription (license) type assignment for any accounts that must be monitored or who will be allowed to work in CXA.



CXA License Assignments

Monitored User License Assignment

Any account that will be monitored for call reporting must have a license assigned and enabled.
While working in Manage Users:

1. 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.

2. 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.

3. 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).
   See the Application Users section to view role assignment information

Reporting Supervisor License Assignment

The **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.

1. 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.

2. Select the required Subscription Type in 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.

3. Once a license type has been assigned, click the adjacent ✓ check mark to ***Save*** the change.
   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.

   See Application Users for further Role assignment instructions, if needed.

Delete User License Assignments

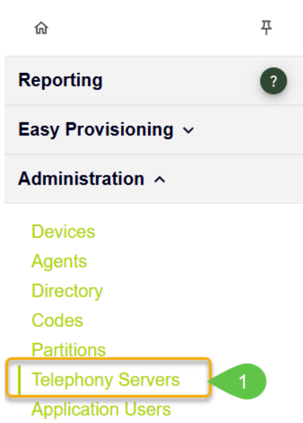
To delete a user's license assignment and stop reporting on their line, or to revoke Reporting Supervisor access:

1. Navigate to the "Manage Users" menu once more
2. Locate the user you wish to revoke reporting access
3. Click the **X** beside their account information
4. Click on the **Trash Can** icon to confirm removal of the license assignment from that account when prompted.

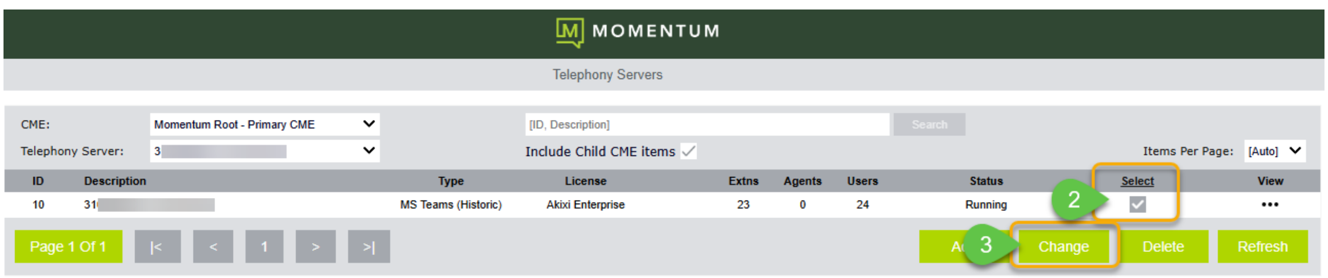
   The license assignment is removed from the selected account and then becomes available for assignment to another account.

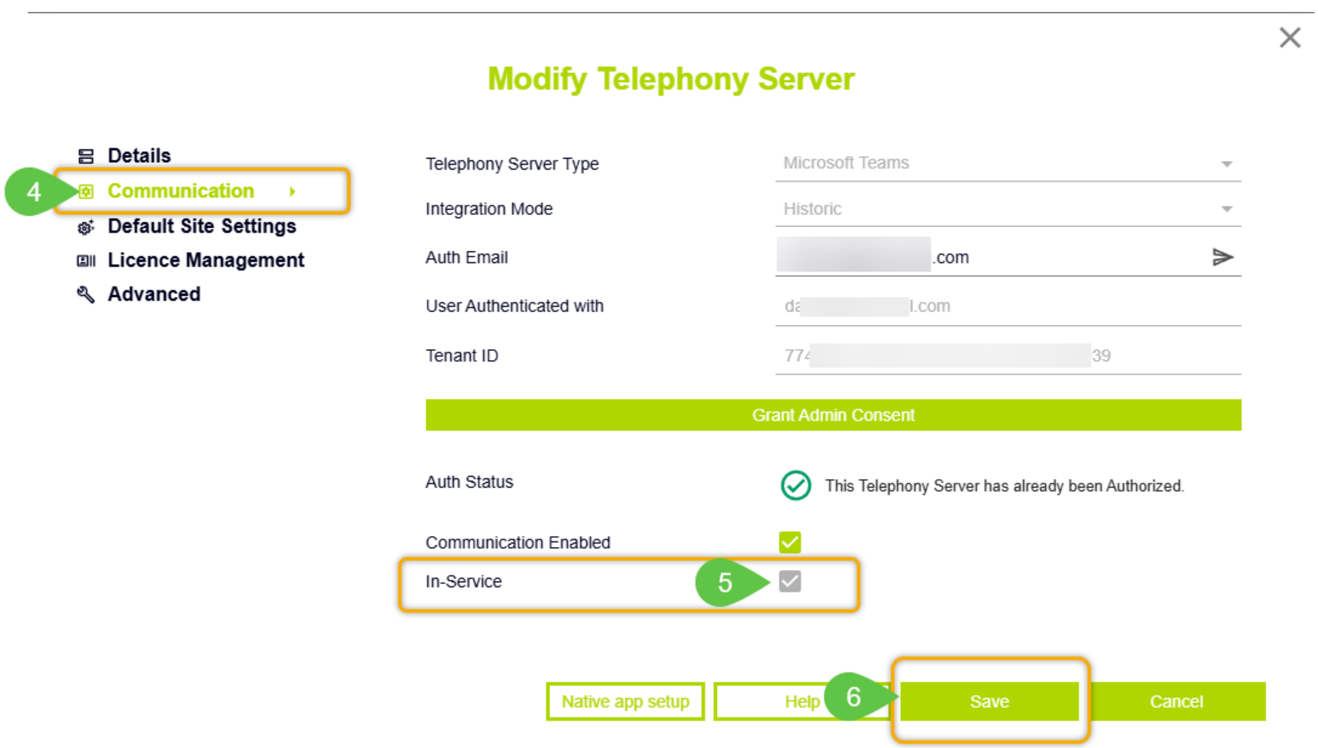
Set In-Service

Once synced and available licenses are assigned, the CXA Teams Tenant Admin / Global Admin must sign set Call Reporting to **In Service**.

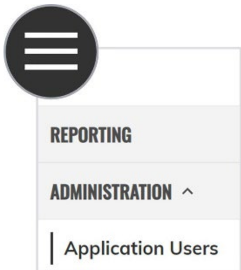


1. Go to: **Administration > Telephony Servers**
2. Select the check box next to the org's telephony server (right side of the list).
3. Click on the **Change** button below the list.
4. Click on the **Communication** menu option in *Modify Telephony Server* dialog.
5. Click to place a check in the box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





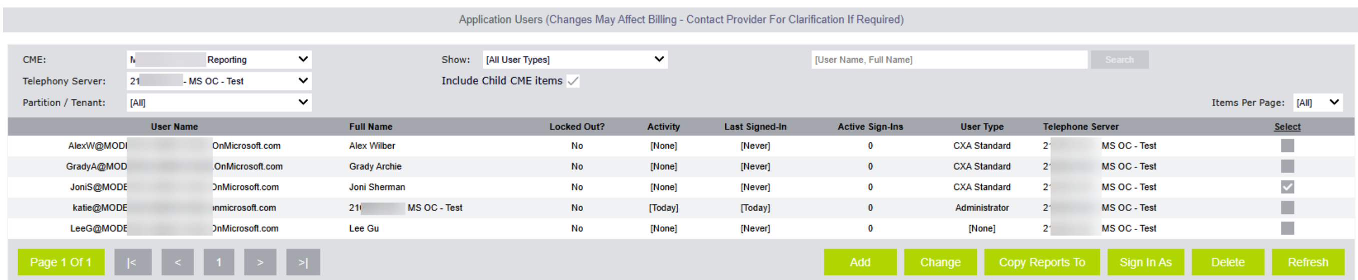
Administration > Application Users Section Tasks



This Administration area is where user account profiles are displayed for review and management. The Profile defines any license limitations and access to / use of the CXA application.

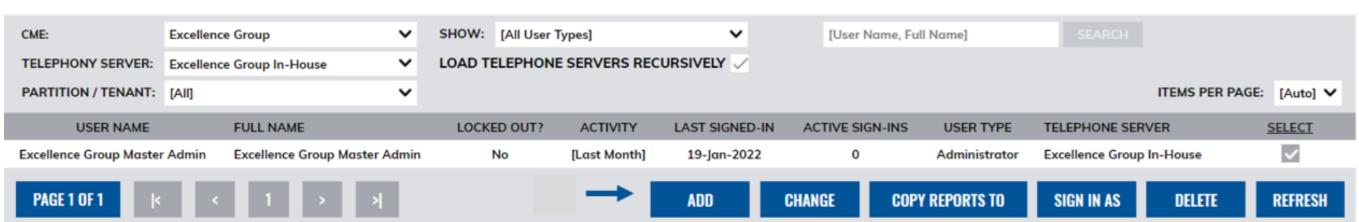
When the number of user accounts configured exceeds the boundary of a page, then the list shows the entries over multiple pages. Each individual page can be displayed by left-clicking the page number links at the bottom-left of the browser window.

Tools are provided to Search, view more pages in a long list, and to filter the list.



Anyone requiring access to the CXA portal, regardless of role or use case, will require an Application User Account. An Application User Account holds the basic information for a user, such as name, email address, credentials, access permissions – and where necessary, their Role assignment(s).

An Application User Account must already be created before any role can be assigned.
Application Management tasks are performed in **Administration > Application Users**



Allowed Reporting Portal Role Assignments Per License

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

Monitored User = Reporting Only Role

If an account is assigned a monitoring license (CXA Standard or Premium) in Manage Users, 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 of its default permissions.*

Advanced License + Reporting Only Role

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 of its 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 Easy Provisioning > Manage Users 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 of its default permissions.

Along with access to the CXA portal Reporting management tools, those with 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 **Easy Provisioning**:

- Access to Manage Users for Admin-level user license assignment tasks.

Edit a User Account

To Edit an existing user account entry - including updates to username, password, etc.:

1. Select a single user listing in the Application Users view.
2. Click the **Change** button at the bottom-right of the table. *The "Change User" page is displayed*
3. Update the details of the existing user account as needed in the User Details or Role tabs.
4. Click the **Save** button to update the user and return to the users administration view – or, click the Cancel button to discard the updated user account details and return to the users administration view.

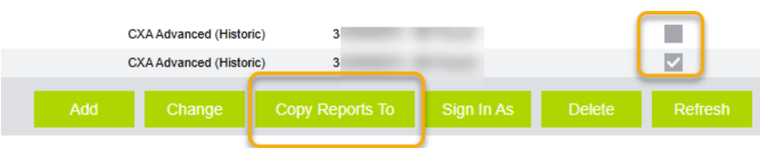
Delete a User Account

Use Caution. It is best to simply remove license assignments in CXA and Delete the account from Teams.
To delete an existing user account entry:

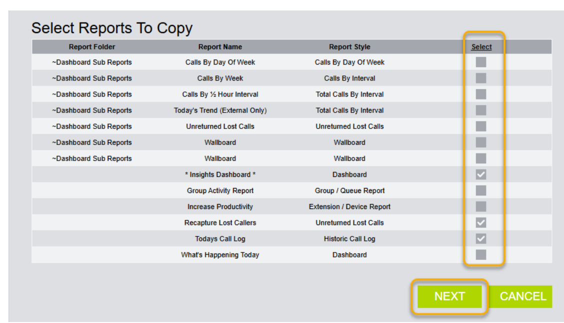
1. Select a single user listing in the Administration view.
2. Click the **Delete** button at the bottom-right of the table.
3. In the *Delete User Entity(s)* page that is then displayed, click the **OK** button to confirm the deletion operation and return to the application user administration view – or, click the **Cancel** button to not perform the deletion operation and return to the users administration view.

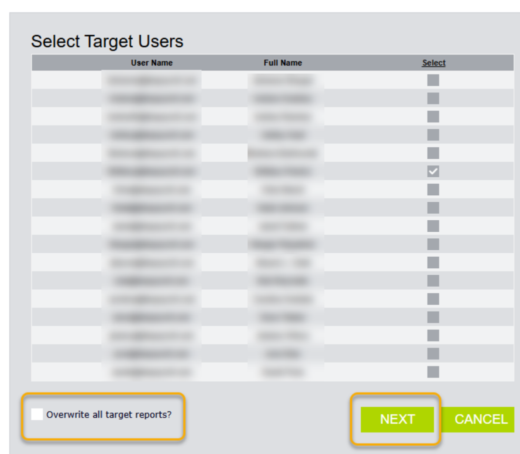
Copy Reports To

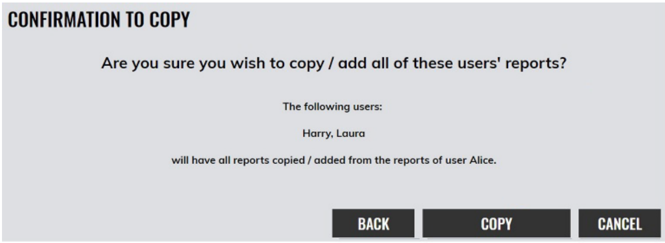
The **Copy Reports To** feature allows Administrators to select reports from one Supervisor account and copy them to other Supervisors within the same site. When copying reports from a Supervisor account, reports can only be sent to other Supervisors who have access to the same Telephony Server and Partition as the original user.
The system provides a useful Wizard to walk you through the process.



1. Go to: **Administration > Application Users**
2. Tick the **Select** check box next to the user who has one or more reports you wish to copy to another Supervisor.
3. Click on the **Copy Reports To** button.
4. Select the reports to be copied from the selected user's account.
5. Click Next.
6. Select the user(s) that will receive the copied reports.
7. ☑ **Overwrite all target reports?** – Optional.
   Enable this check box if **all** of the currently existing reports of the selected target users will be deleted and overwritten by the reports you selected .
8. Click **Next**.
9. Click **OK** to provide confirmation that users' existing reports are going to be entirely overwritten. (if you elected to enable the 'overwrite' checkbox)
10. Click the **Copy | Overwrite** (if step 9 has been followed) button to proceed and complete the task.
    At this stage of the process, the ***Back*** button can be used to go back to the previous step in the wizard to make changes, as well.





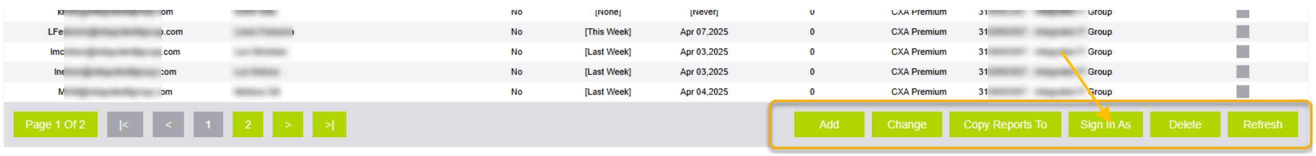


Once the Copy | Overwrite button has been selected, the task is completed, and all of the selected reports will be copied across to the target user(s) you selected.

Sign In As

This feature allows the viewer to select someone within the list above and then sign in to the user's account via emulation as though viewing CXA the way the selected user does.

1. Go to: **Administration > Application Users**.



2. Click to place a check in the box adjacent to the desired user account (far right under Select.)
3. Click on the **Sign In As** button
4. Confirm that you wish to continue on to view CXA as the selected user does when prompted.

   Important Note: *While emulating, you will have only as much access to tools or tasks as the selected user does.*

5. Click **Sign Out** (top right) when you are finished emulating.

Application Users Section Help

Click **F1** or on the **Help** icon to review the Application Users section of the Help File.

Add a Non-Reporting Admin Account

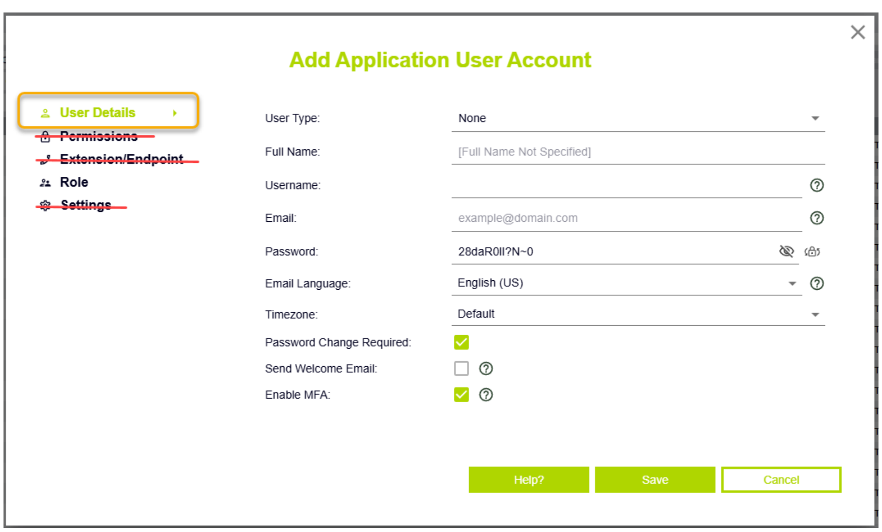
This is the only account type and role that does not require the assignment of a monitoring license (CXA Standard or Premium) or an **Advanced** license as they will **not** be monitored nor be granted access to any of the Reporting tools. It can be created manually; however, it is important to build 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** = **NONE**. *Leave this field set to the default of None.*
   - **Full Name**: *The full name of the user to be assigned against the account.*
   - **Username**: *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**: *This field should contain the email address of the user. Email messages sent by the application will be sent to this email address.*
   - **Password**: *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 checkbox 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 checkbox 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 to sign in. If this checkbox 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.

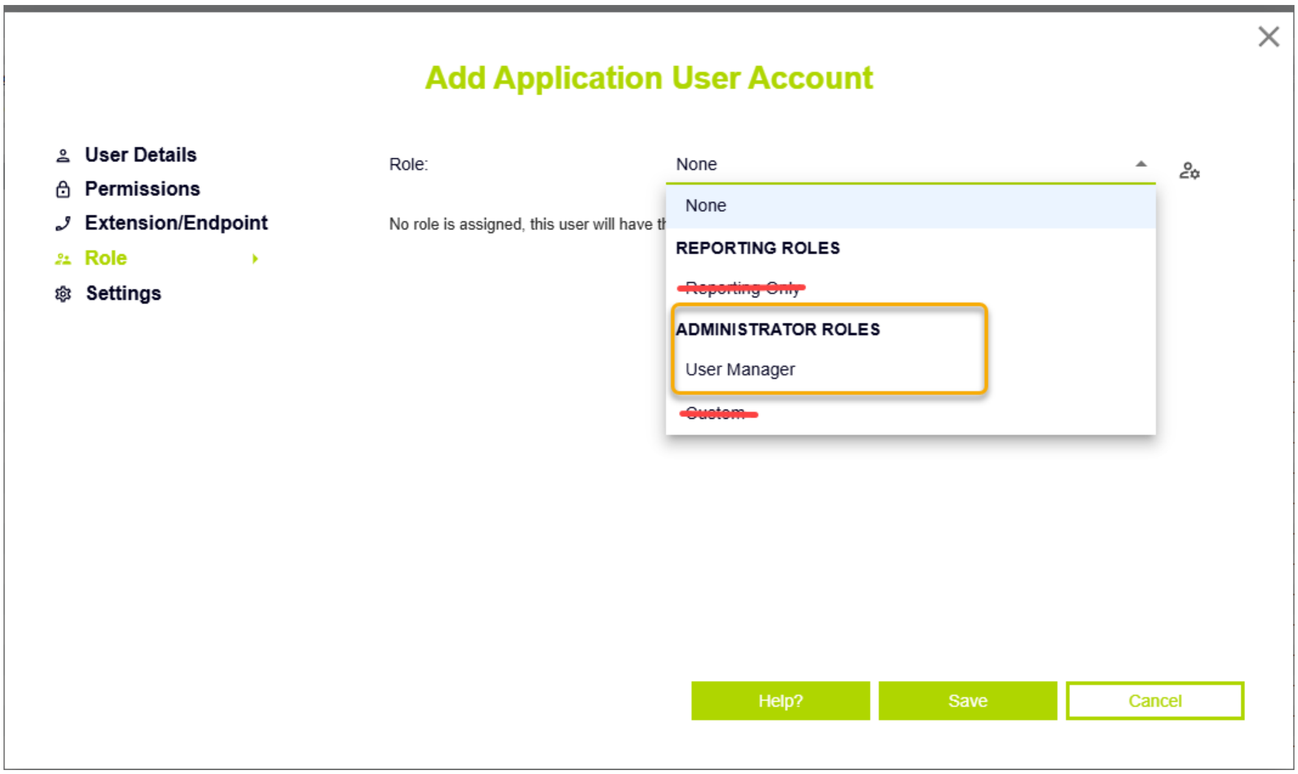


In the Roles Tab:

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

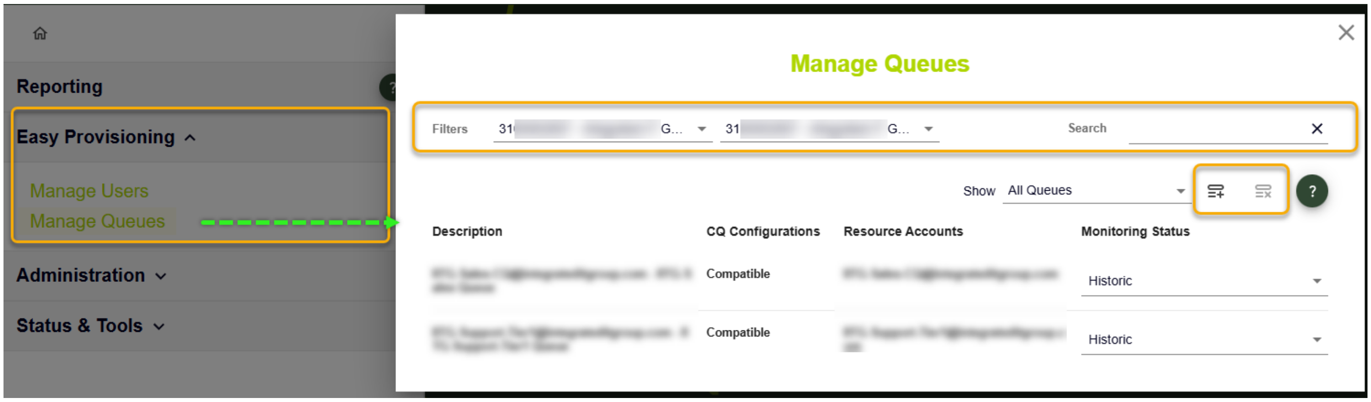
7. **SKIP** all of the other tabs and leave all fields and settings within them set to their defaults.

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.

Easy Provisioning > Manage Queues

Sufficient Administrator access permissions are required to view and 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. Admins can contact the Service Provider for assistance .



Searching and Filtering 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.

Manage Queue Monitoring

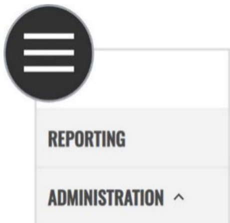
By default, all queues are set to Historic (up to 1 second ago) monitoring. Queues should be compatible and be monitored for full reporting functionality.

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.

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

Other CX Analytics Administration Sections 101



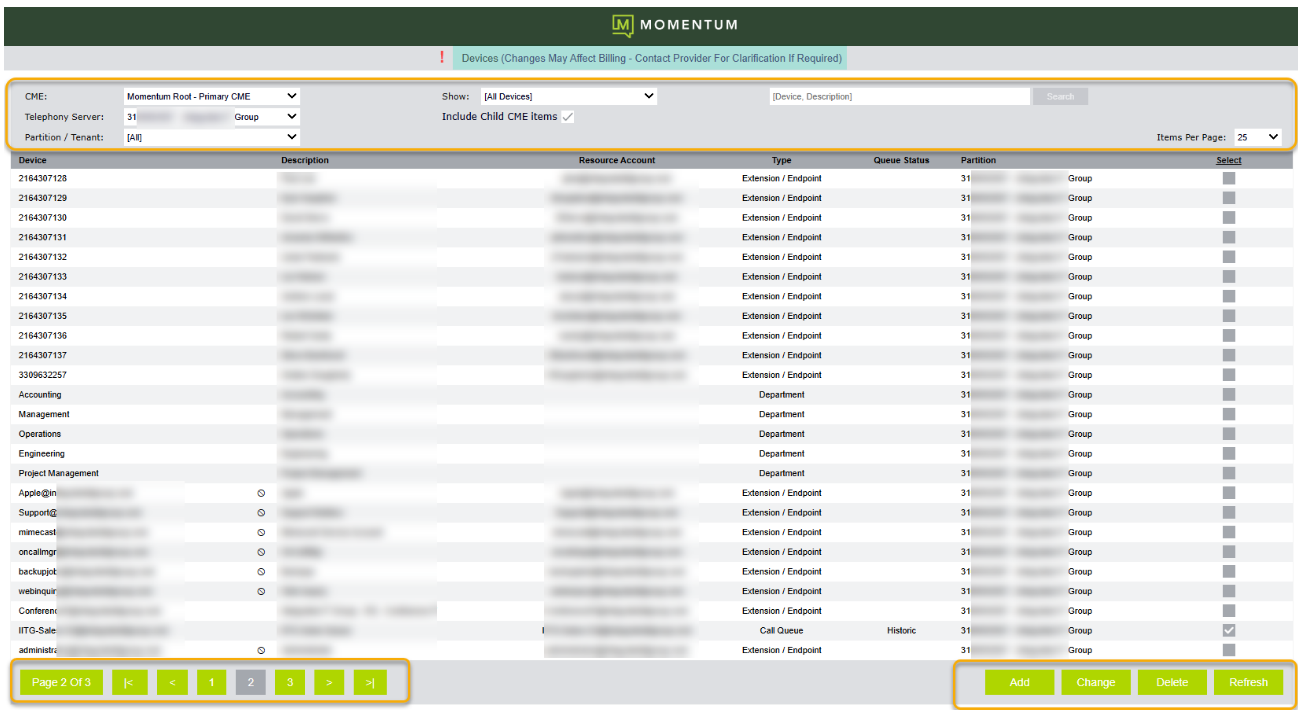
In order to access the administration features of the application, go to Menu > Administration.

The Administration drop-down menu offers additional sections for those with some level of Administration access to review information or to perform tasks.

Note: The Administration section is only displayed if a user has signed in with credentials that allow some Administration privileges.

Devices

The Devices administration area is where extensions, groups, trunks, and other device types are specified to allow the application to monitor call & device status activity for a designated telephone system. Devices must be compatible and monitored for full functionality. Note: Changes to Devices made in Teams are synchronized routinely to CXA. Erroneous changes made to Devices in CXA can negatively impact reporting or functionality.
Note: Most administration roles see this section as read-only.



Change a Device

To change an existing device:

1. Select a single item in the Devices list by clicking to place a check in the adjacent checkbox under <u>Select</u>.
2. Click the **Change** button at the bottom-right of the table.
3. In the "Change Device" dialog, update the details of the existing device. Use Caution!
4. Click the **Save** button to update the Device data and return to the Devices list view.
5. Click **Refresh**, as needed.
   Or - click the Cancel button to discard the updated device details and return them to the Devices list view.

Add a Device

Use Caution.

To add a new device manually:

1. Click the **Add** button at the bottom-right of the table.
2. In the "***Add New Device***" dialog, specify the details of the new device,
3. Click the **Add** button to save the new device and return to the devices list view.

   Or - click the **Cancel** button to discard and return to the devices list view without adding the device.

Delete a Device

Use Caution.

To delete an existing device entry:

1. Select an item from the list using the Select checkbox adjacent to it.
2. Click the **Delete** button at the bottom-right of the table. The "Delete Device Entity(s)" page displays
3. Click the **OK** button to confirm the deletion operation and return to the devices list view.
   Or - click the **Cancel** button to exit and return to the devices list view without deleting.

   You can also Select several similar device entries at a time in the list and delete them in bulk.

Warning:	Unless specifically directed to by your system or application provider, you should be particularly careful not to delete the special (pseudo) device such as the "[Trunk]" or "[Conference]" entries, which are required to model certain call scenarios on some telephone systems and should not be removed.
Also:	In order to avoid accidental device deletion operations, there are a number of inbuilt restrictions that apply when deleting multiple devices together at the same time. For example, you cannot delete more than one device without specifically choosing the partition to do that delete operation for at the top-left of the Devices Administration page. Also, you cannot delete special (pseudo) device items when deleting normal device entries at the same time, and additionally you cannot delete more than 5 special devices in one single deletion operation.

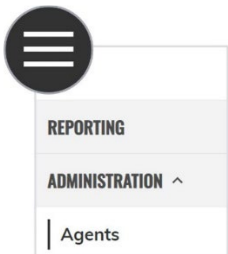
Devices Help

Click on the **Help** icon (or press F1) to review the Devices section of the online Help File.

Agents

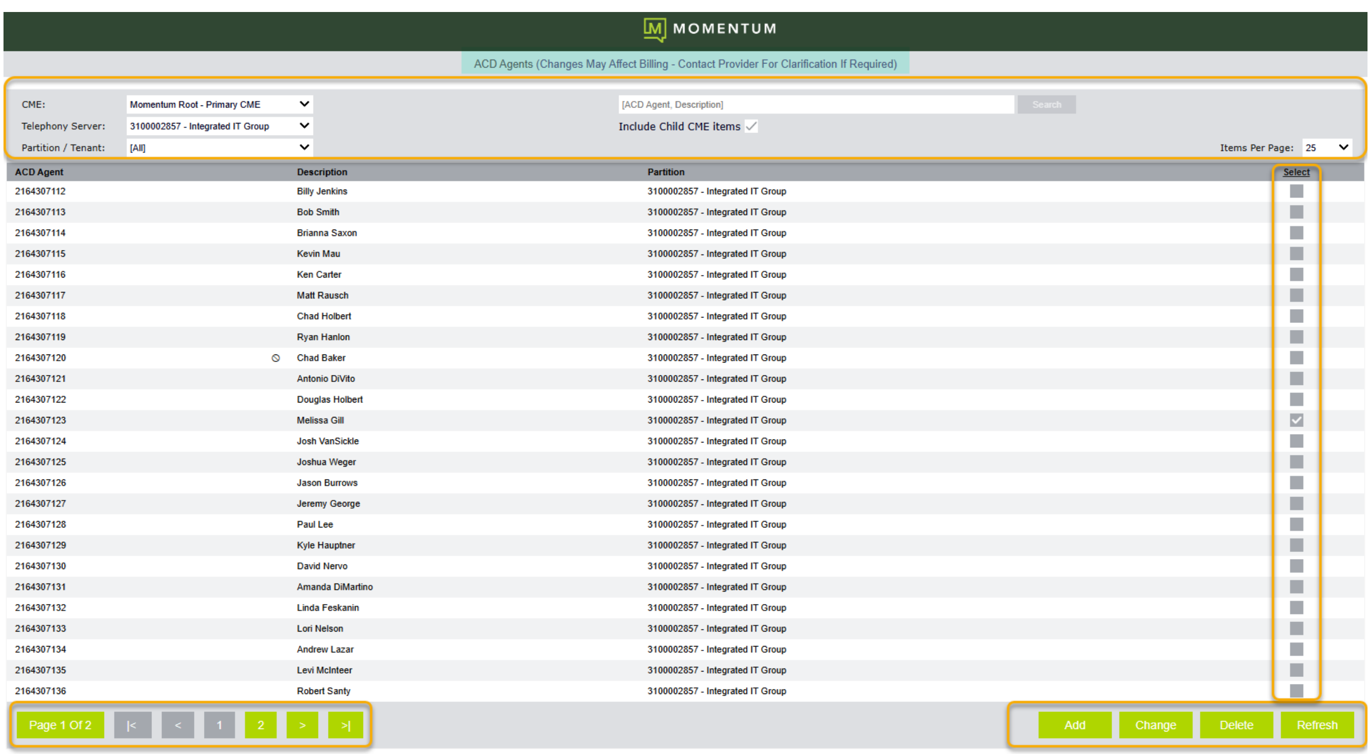
User/Agent information Administration.
The Agents page lists the Agents configured in the tenant.

Go to: **Administration > Agents**



The Agents administration area is where Agent identifiers are specified to allow the application to monitor call & ACD status activity against them for a designated telephone system. ACD agents are normally used on the telephone system in formal call center environments to allow individual call center worker's performance to be measured by assigning them an individual ACD agent identifier, which they use to sign in and out of a telephone extension with.

Warning:	Making Agent configuration changes within the CXA application will often directly affect the monthly billing charge applied to the corresponding customer. Generally speaking, the application administrator should specifically only add ACD agents that the customer *specifically* wishes to pay for in-application reporting functionality. Please contact your application Service Provider for further clarification if required.
Also:	Agent entries are automatically added to the default common devices partition by the application's automatic inbuilt synchronization logic, which can also be invoked immediately using the "Perform Synchronization Now" check box against the application's corresponding telephony configuration entry. Note that ACD Agents are only added when the corresponding telephone system entry's "Licensed For" field is configured for the "Enterprise" option in Teams environments.



Agents Page Display Tools

Filter, Search and Pagination tools are provided. You can define the number of individual agents shown per page of the list view, by selecting a particular number from the "Items Per Page" drop down list at the top-right of the table area. If you select the "[Auto]" option, then the page automatically calculates approximately how many items can be shown per page for your particular computer's current monitor resolution. Note that the "Items Per Page" control is actually disabled when there are currently no items to display in the page at all. Use the search box to search through records to find a specific item or term.

Add an Agent

To add a new ACD agent to the application configuration, ensure that the appropriate telephone system is selected in the drop down filter list at the top of the table in the ACD agents administration view. Then click the Add button at the bottom-right of the table.

In the "Add New ACD agent" page that is then displayed, specify the details of the new agent, and then click the **Add** button to save the new agent and return to the ACD agent administration view. Alternatively, click the Cancel button to discard the new agent details and return to the ACD agents administration view without adding the agent.

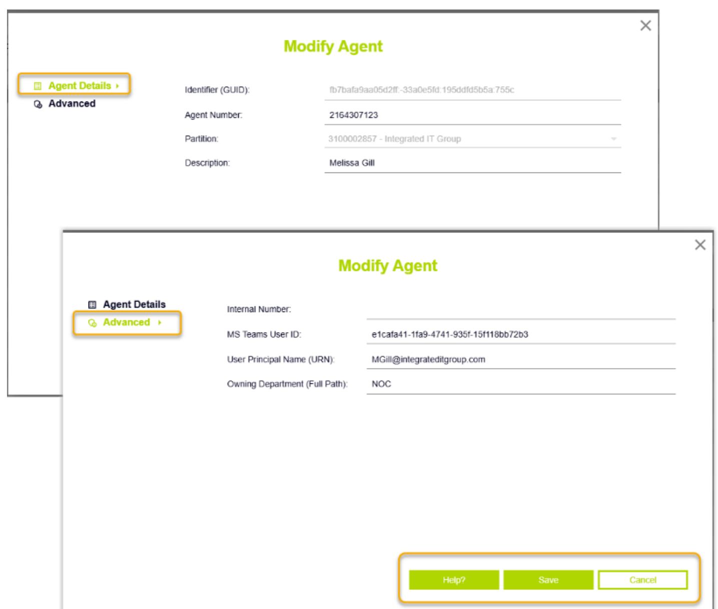
Change an Agent

To change an existing ACD agent:

Select a single ACD agent in the list and then click the Change button at the bottom-right of the table.

In the "Modify Agent" page that is then displayed, update the details of the existing agent, and then click the Save button to update the device and return to the ACD agents administration view.

Alternatively, click the Cancel button to discard the updated agent details and return to the ACD agents administration view.



Delete an Agent

Use caution. To delete an existing Agent entry:

1. Select an item within the Agents list view.
2. Click on the **Delete** button at the bottom-right of the table.
3. Click **OK** to confirm the deletion operation when prompted and return to the Agents list view.

   Or – Click the **Cancel** button to exit without making changes and return to the Agents list view.

   You can also select several ACD agent entries at a time in the list and delete them simultaneously.

Agent Help

Click on the **Help** icon (or press F1) to review the list of Agent settings and their descriptions within the Help File.

Directory

The directory administration area is where directory entries are specified to allow the application to show the telephone number's description on various reports. When the number of directory entries configured exceeds the boundary of a page, then the list shows directory entries in multiple pages. Each individual page can be displayed by left-clicking the page number links at the bottom-left of the browser window.

Directory Page Display Tools

You can use the search box to search through records to find a specific item. This avoids having to search through multiple pages to find a specific record. Simply type in the Search box and press the Search button to search through the pages of records. The search box scans through the columns of data specified in the search box.

You can also select how many individual directory entries will be shown per page of the list view, by selecting a particular number from the "Items Per Page" drop down list at the top-right of the table area. If you select the "[Auto]" option, then the page automatically calculates approximately how many items can be shown per page for your particular computer's current monitor resolution. The "[All]" option will show all directory entries in a single page. Note that the "Items Per Page" control is actually disabled when there are currently no items to display in the page at all. You can specifically view the number of items displayed in the current page, and also the total overall item count for the currently selected telephone system and/or partition, by floating the mouse over the page count text at the bottom-left of the web page.

Add a Directory Entry

To add a new directory entry to the application configuration, ensure that the appropriate telephone system is selected in the drop down filter list at the top of the table in the directory administration view.

1. Click the **Add** button at the bottom-right of the Directory table.
2. In the "Add New Directory Entry" page that is then displayed, specify the details of the new directory entry
3. Click the Add button to save the new directory entry and return to the directory administration view.
4. Or click the **Cancel** button to discard the new directory entry details and return to the Directory list view without adding the directory entry.

Change a Directory Entry

To change an existing directory entry:

1. Select a single item within the Directory list view.
2. Click on the **Change** button at the bottom-right of the table.

   In the "***Change Directory Entry***" dialog, update the details of the existing directory entry, as needed.
   Note: All fields in this dialog are required – Save will not be allowed if any field is left empty.
3. Click the **Save** button to update the Directory entry and return to the Directory list view.
4. Or – Click on the **Cancel** button to discard the changes and return to the directory administration view.

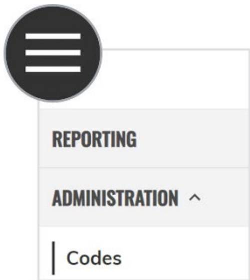
Delete a Directory Entry

Use Caution. To delete an existing directory entry, select an item in the directory administration view and then click the Delete button at the bottom-right of the table. In the "Delete Directory Entry Entity(s)" page that is then displayed, click the OK button to confirm the deletion operation and return to the directory administration view. Alternatively, click the Cancel button to not perform the deletion operation and return to the directory administration view. You can also select several directory entries at a time in the list and delete them together in one go.

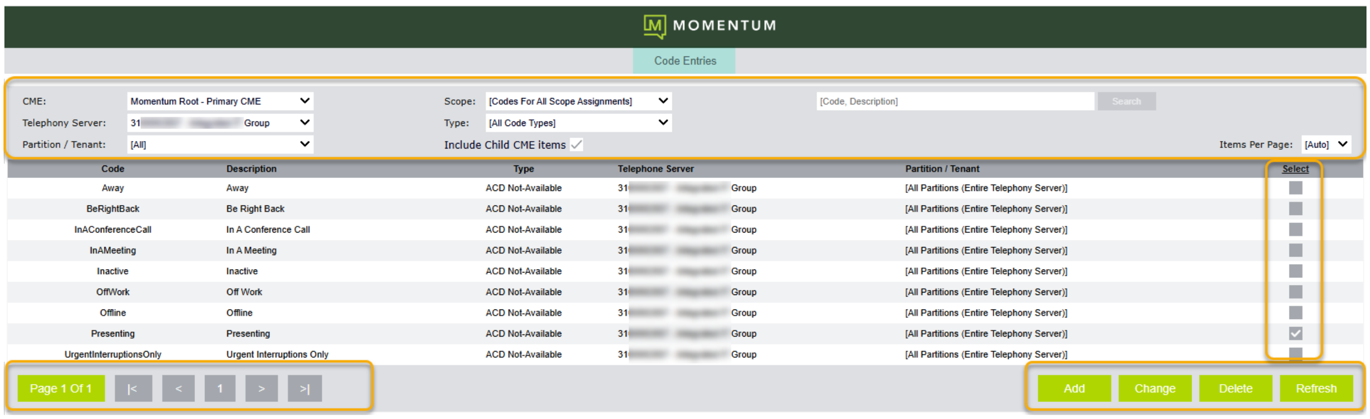
Directory Help

Click F1 or on the Help icon to review the full list of Directory settings with descriptions within the Help File.

Codes



The Codes administration area is where code configurations can be set to recognize, match, and display descriptions for account/authorization & ACD Not-Available codes, whenever they are entered in for calls and/or the appropriate ACD state transitions. When the number of codes configured exceeds the boundary of a page, then the list shows the entries over multiple pages. Each individual page can be displayed by left-clicking the page number links at the bottom-left of the browser window.



Code Entry Scoping: Codes are defined within the **Teams** environment. Code entries may have an assigned component scope and can be assigned to any/all telephone server configuration entries, which effectively means they're assigned application-wide and visible to all reporting users, or for specific groups. The use of application-wide scoped codes is not recommended as their naming (description) tends to be different for the same underlying code value across different telephony environments. Codes can also be assigned specifically to a particular telephone server, but visible to reporting users attached to any sub-partition within that telephone server. Finally, codes can be individually assigned to a specific partition, where they are only visible to reporting users with scope permission set to the corresponding partition.

Code Matching Within Reports: Codes and their code descriptions are shown within certain reporting fields. This occurs when the application has previously captured that an extension or ACD agent has specified an account/authorization or ACD Not-Available code within the telephony environment (Teams).

The description for a code is shown based on the application performing a search within the code configuration list. Code search operations are performed by the application in order to try and match the code items that are most "tightly" scoped against the corresponding telephony environment (Teams).

Codes Page Display Tools

You can use the Search box to search through records to find a specific item. This avoids having to search through multiple pages to find a specific record. Simply type in the Search box and press the Search button to search through the pages of records. The search box scans through the columns of data specified in the search box.

You can use the Filter drop-down list shown at the top-left of the page's table area in order to filter the list to show you codes by assignment, code scope, and code type.

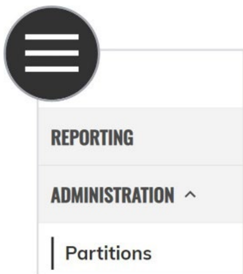
Change Code Entries

To change an existing code entry, select a single item on its own in the codes administration view and then click the Change button at the bottom-right of the table.
In the "Change Code" page that is then displayed, update the details of the existing code item, and then click the Save button to update the code and return to the codes administration view. Alternatively, click the Cancel button to discard the updated code details and return to the codes administration view.

Code Help

Click **F1** or on the Help icon to review the full list of Code settings with descriptions within the Help File.

Partitions (Tenants)

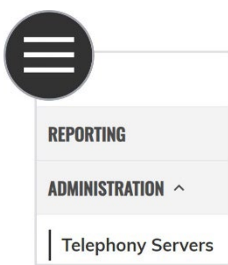


This area is typically managed by the Service Provider.

Partition Help

Click F1 or on the Help icon to review the full list of Partition (Tenant) Settings with descriptions within the Help File.

Telephony Servers



This area is typically managed by the Service Provider or Teams Tenant Admin.

Telephony Server Help

Click F1 or on the Help icon to review the full list of Telephony Server settings with descriptions within the Help File.