CXA

User Manager

Quick Reference

MOMENTUM

powered by: akixi CX

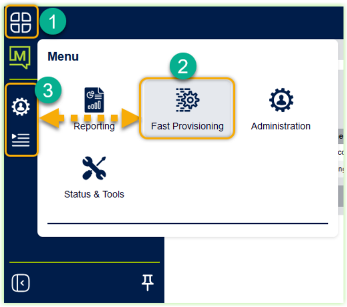
User Manager Introduction

This introductory guide provides an overview of the areas available for review by those given the additional **User Manager** Role to view useful areas in the Administration sections. The User Manager Role can only be authorized/granted by an Administrator. The User Manager role assignment is typically given to a few **CXA Advanced** license holders (Reporting Supervisor) at an organization to allow them to perform their typical Reporting tasks AND some helpful Administration tasks. This role can also be assigned to a NON-Reporting Admin (a manually created administrator account with NO CXA reporting or monitoring license assignment).

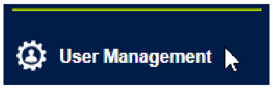
The User Manager role offers useful pre-defined Administration section tool access.

Fast Provisioning Tools

Note: The **Fast Provisioning** section is only displayed if signed in with credentials for Administration section access



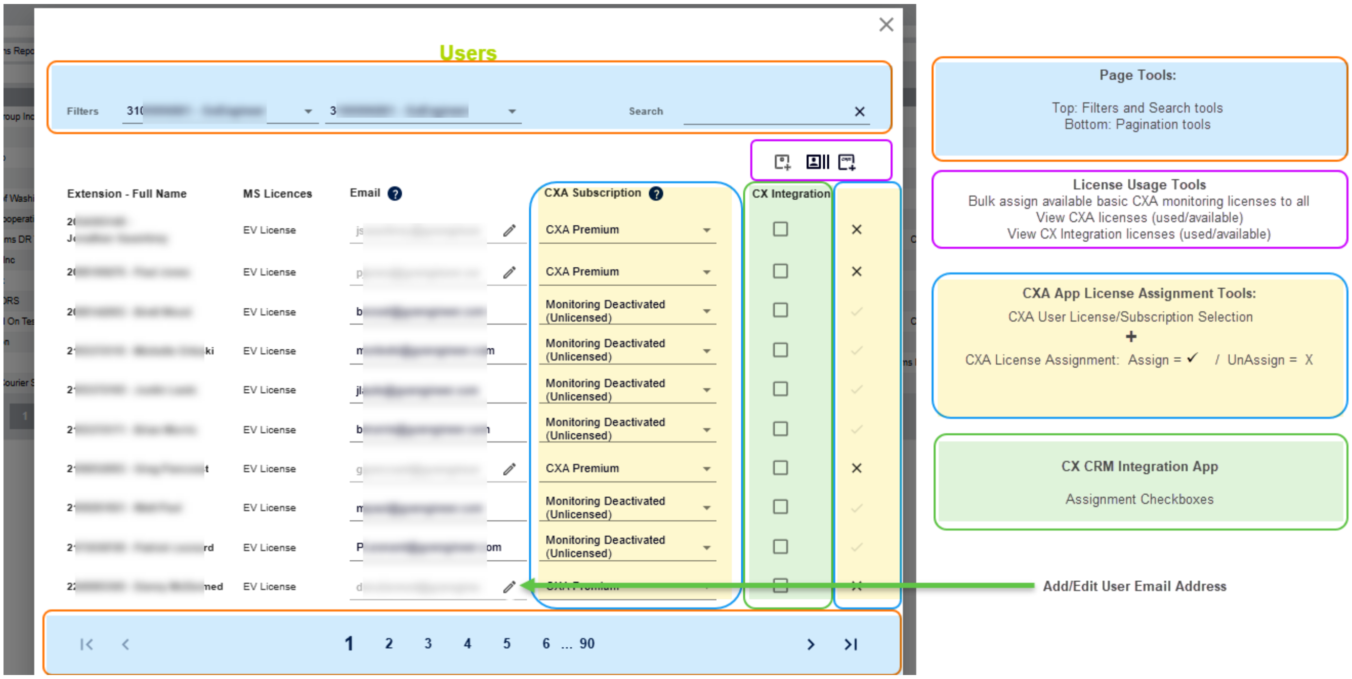
User Management



User Manager Administrators 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 synced data including a correctly formatted email address, a CXA license type selection PLUS license assignment (checkmark).



Users

Filters 31[redacted] 3[redacted] Search ×

Extension - Full Name	MS Licences	Email	CXA Subscription	CX Integration	
2[redacted] Jo[redacted]	EV License	js[redacted]	CXA Premium	□	×
2[redacted]	EV License	p[redacted]	CXA Premium	□	×
2[redacted]	EV License	b[redacted]	Monitoring Deactivated (Unlicensed)	□	✓
2[redacted]ki	EV License	m[redacted]m	Monitoring Deactivated (Unlicensed)	□	✓
2[redacted]	EV License	jl[redacted]	Monitoring Deactivated (Unlicensed)	□	✓
2[redacted]	EV License	b[redacted]n	Monitoring Deactivated (Unlicensed)	□	✓
2[redacted]t	EV License	g[redacted]	CXA Premium	□	×
2[redacted]	EV License	m[redacted]	Monitoring Deactivated (Unlicensed)	□	✓
2[redacted]rd	EV License	P[redacted]om	Monitoring Deactivated (Unlicensed)	□	✓
22[redacted]med	EV License	d[redacted]	CXA Premium	□	×

|< < 1 2 3 4 5 6 ... 90 > >|

Page Tools:
Top: Filters and Search tools
Bottom: Pagination tools

License Usage Tools
Bulk assign available basic CXA monitoring licenses to all
View CXA licenses (used/available)
View CX Integration licenses (used/available)

CXA App License Assignment Tools:
CXA User License/Subscription Selection
+
CXA License Assignment: Assign = ✓ / UnAssign = X

CX CRM Integration App
Assignment Checkboxes

Add/Edit User Email Address

Assigning User Licenses

1. While working in Fast Provisioning, click on the **User Management** option.
2. Ensure the correct filters are applied at the top of the window (by default these are set to the tenant)
3. Select the required Subscription Type (by default all listings show Monitoring Deactivated which means no license assigned yet – and the options for selection in the ▼ drop-down will only include license types available currently (unassigned/unused)
4. Once a license has been assigned, click the ✓ Check mark adjacent to the user to Save the change.
5. Repeat the Subscription Type selection and check mark steps to assign available licenses to other users, as appropriate.

Removing User License Assignments

To delete a user's license assignment and stop reporting on their line and/or allowing access to Reporting tools:

1. Navigate to the "User Management" 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 license assignment. This frees up the license for later assignment to a different user,

Queue Management

Administrators can review and manage the current reporting monitoring status for compatible Teams call queues in **Fast Provisioning** > **Queue Management**. Tools to filter, sort, search, and view more pages are included.

Searching and Filtering Available Queues

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.

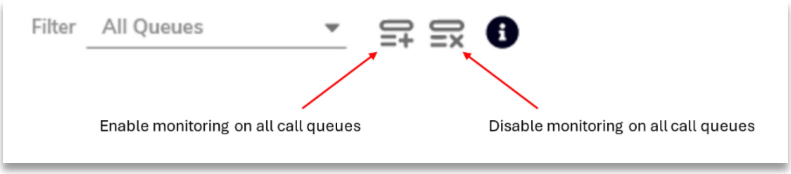
Any returned call queues can be filtered using the available dropdown menus in the top left corner of the screen, based on the application user specifying the telephony server and partition respectively. You can also select which call queues you wish to be displayed in the returned list view, by selecting one of the filter options from the dropdown menu.

Manage Queue Monitoring

Enable: For all call queues displayed to you, the monitoring status can be updated by clicking the dropdown icon beside the call queues current monitoring status selecting the appropriate option.

Disable: For call queues in the monitoring status Real-time (Forced), the call queue's real time monitoring can also be disabled by clicking the cross icon beside the associated call queue.

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


Filter
All Queues
Enable monitoring on all call queues
Disable monitoring on all call queues

Other Administration Tools

Administration

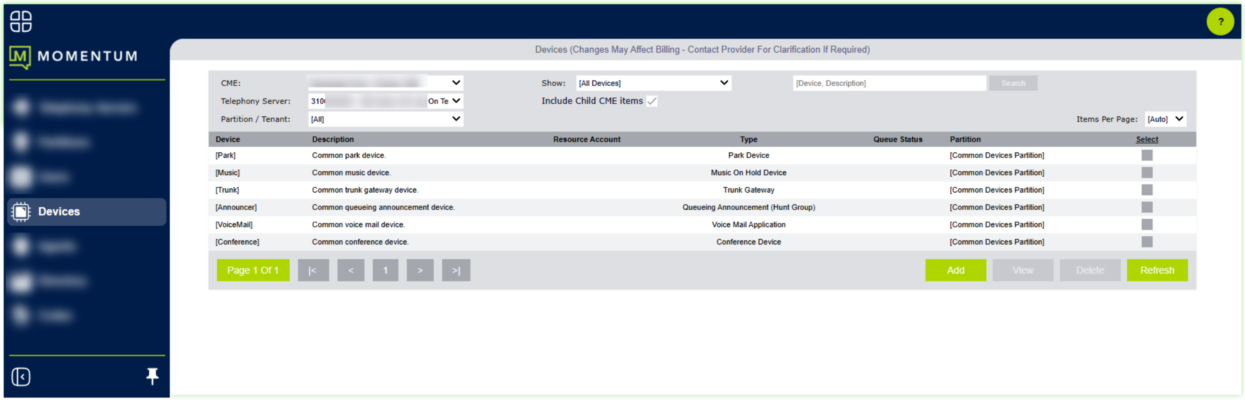
In order to access the administration features of the application, go to Menu > Administration. The Administration menu opens additional sections for administrators to review or work in (per access permissions).

Note: The Administration menu option and sections only display if signed in with credentials for access.

Devices

Devices

The devices administration area is where extensions, groups, trunks, and other device types are listed to allow the application to monitor call & device status activity for a designated telephone system.



Devices (Changes May Affect Billing - Contact Provider For Clarification If Required)

CME: [redacted]
Telephony Server: 310[redacted] On Te
Partition / Tenant: [All]
Show: [All Devices]
Include Child CME items ✓
[Device, Description]
Items Per Page: [Auto]

Device	Description	Resource Account	Type	Queue Status	Partition	Select
[Park]	Common park device.		Park Device		[Common Devices Partition]	□
[Music]	Common music device.		Music On Hold Device		[Common Devices Partition]	□
[Trunk]	Common trunk gateway device.		Trunk Gateway		[Common Devices Partition]	□
[Announcer]	Common queueing announcement device.		Queueing Announcement (Hunt Group)		[Common Devices Partition]	□
[VoiceMail]	Common voice mail device.		Voice Mail Application		[Common Devices Partition]	□
[Conference]	Common conference device.		Conference Device		[Common Devices Partition]	□

Adding Devices

Info: The system updates any new identified telephony devices added by an Administrator in Teams to the Devices listed here during routine syncs. Important Note! Manual additions of Devices made here can be billing impacting.

While in Devices list:

1. Click the Add button at the bottom of the table.
2. Enter the information requested in the fields presented.
3. Click Add when finished or Click Cancel to exit without making changes.

Changing Devices

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

Deleting Devices

To delete an existing device entry, select an item in the devices administration view and then click the Delete button at the bottom-right of the table. In the "Delete Device Entity(s)" page that is then displayed, click the OK button to confirm the deletion operation and return to the devices administration view. Alternatively, click the Cancel button to halt and exit without deleting.

not perform the deletion operation and return to the devices administration view.
You can also select several device entries at a time in the list and delete them together in one go.

When deleting devices for the BroadSoft BroadWorks, BroadSoft M6, & Panasonic NCP/TDA telephony platforms, any matching ACD agent configuration items are also automatically deleted too. To only delete the corresponding device(s), ensure that the "Automatically Delete Matching ACD Agents" setting within the final confirmation page is specifically not set (i.e. unchecked). Note that this setting is only ever displayed when matching ACD agent entries are actually detected within the same partition/tenant. The setting is also never displayed for partitions associated with the Siemens HiPath family of telephone systems.

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 Settings Help

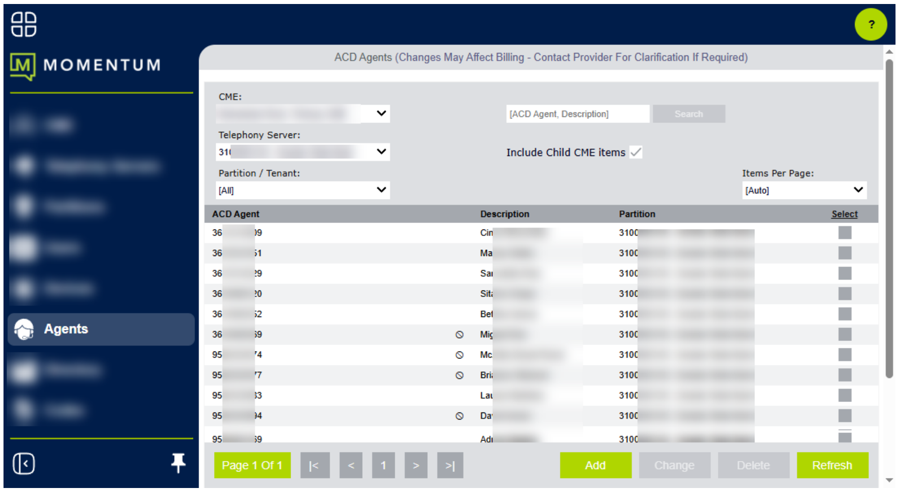
Click F1 or on the Help icon to review the full list of settings with descriptions within the Help File.

Agents

Agents ACD Agent Administration.

In order to access the agents administration area of the application, left-click the hamburger menu located in the top-left of the portal and select “Administration” followed by "Agents" found underneath in the sub-item area.

The ACD agents administration area is where ACD 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.



ACD Agents (Changes May Affect Billing - Contact Provider For Clarification If Required)

CME: [redacted]
Telephony Server: 31[redacted]
Partition / Tenant: [All]
[ACD Agent, Description] Search
Include Child CME items ✓
Items Per Page: [Auto]

ACD Agent	Description	Partition	Select
36[redacted]9	Cin[redacted]	3100[redacted]	□
36[redacted]1	Ma[redacted]	3100[redacted]	□
36[redacted]9	Sa[redacted]	3100[redacted]	□
36[redacted]0	Sit[redacted]	3100[redacted]	□
36[redacted]2	Bet[redacted]	3100[redacted]	□
36[redacted]9 ⦸	Mig[redacted]	3100[redacted]	□
95[redacted]4 ⦸	Mc[redacted]	3100[redacted]	□
95[redacted]7 ⦸	Bri[redacted]	3100[redacted]	□
95[redacted]3	Lau[redacted]	3100[redacted]	□
95[redacted]4 ⦸	Da[redacted]	3100[redacted]	□
95[redacted]9	Adı[redacted]	3100[redacted]	□

When the ACD agents administration page is first displayed, usually no agents are displayed until a telephone system is selected within the drop-down list shown at the top-left of the page's table area.
The drop down lists allow you to filter the list for agents within a particular telephone system and/or partition (tenant).
Central management environment (CME) filter can be used to filter out the available telephony servers that do not belong to selected central management environment or any its children if recursive loading is enabled. Central management environment of current users is selected by default.

Warning: Making ACD agent configuration changes within the 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 reporting functionality on.

Please contact your system or application provider for further clarification if required.

Note: Depending on your assigned telephone system and/or partition privileges you may only have access to configure ACD agents in a single partition (tenant) or telephone system.

Refer back to the application administrator that created your particular user account in order to gain

Also: On a non-hosted (single tenanted) telephony platform such as the Siemens HiPath 3000, it is recommended that you create all the required device & ACD agent configuration entries against the default common devices partition.

On the Panasonic TDA/NCP telephone system, ACD agents that are to be excluded from reporting should be added to the device exclusions partition (i.e. the automatically created partition that is named "[Excluded Devices Partition]"). All other ACD 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 telephone system configuration entry. Note that ACD agents are only added when the corresponding telephone system entry's "Licensed For" is configured for the "Akixi 1000", "Akixi 2000"

Once a telephone system is selected, the ACD agents page lists the ACD agents configured in the selected partition(s). Note that ACD agents for all partitions in a selected telephone system can only be viewed when there are 5 or less partitions in the corresponding telephone system. For telephone system containing more than 5 partitions, an individual partition must be selected in order to actually view ACD agent configuration items.

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

Agents Page Display Tools

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. The "[All]" option will show all ACD agents 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 being 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.

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 to locate data specified in the search box.

Adding ACD Agents

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 also the partition (tenant) it will belong to, 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.

Changing ACD Agents

To change an existing ACD agent, select a single item on its own in the ACD agents administration view and then click the Change button at the bottom-right of the table.

In the "Change ACD 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.

Deleting ACD Agents

To delete an existing ACD agent entry, select an item in the ACD agents administration view and then click the Delete button at the bottom-right of the table. In the "Delete Device Entity(s)" page that is then displayed, click the OK button to confirm the deletion operation and return to the ACD agents administration view.

Alternatively, click the Cancel button to not perform the deletion operation and return to the ACD agents administration view.
You can also select several ACD agent entries at a time in the list and delete them together in one go.

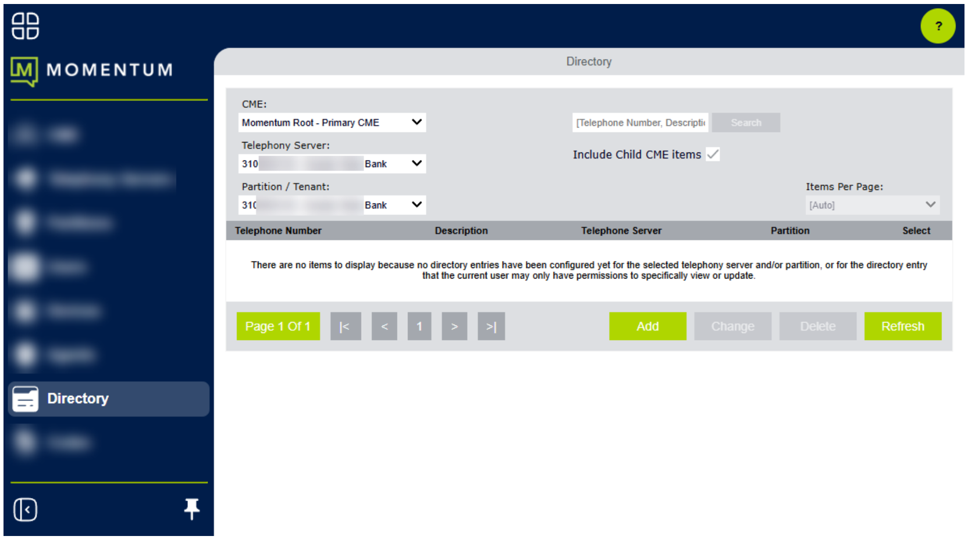
Agents Settings Help

Click F1 or on the Help icon to review the full list of Agent (ACD) settings with descriptions within the Help File.

Directory

Directory

This administration area is where directory entries are defined to allow the application to show the telephone number's description on various reports.



CME: Momentum Root - Primary CME

Telephony Server: 310 Bank

Partition / Tenant: 310 Bank

[Telephone Number, Descripti

Include Child CME items ✓

Items Per Page: [Auto]

Telephone Number	Description	Telephone Server	Partition	Select

There are no items to display because no directory entries have been configured yet for the selected telephony server and/or partition, or for the directory entry that the current user may only have permissions to specifically view or update.

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.

Adding 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. Then click the Add button at the bottom-right of the table.
In the "Add New Directory Entry" page that is then displayed, specify the details of the new directory entry and also the partition (tenant) it will belong to, and then click the Add button to save the new directory entry and return to the directory administration view. Alternatively, click the Cancel button to discard the new directory entry details and return to the directory administration view without adding the directory entry.

Changing a Directory Entry

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

Note: All fields on this page are required – Save will not be allowed if any field is left empty.

Deleting a Directory Entry

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

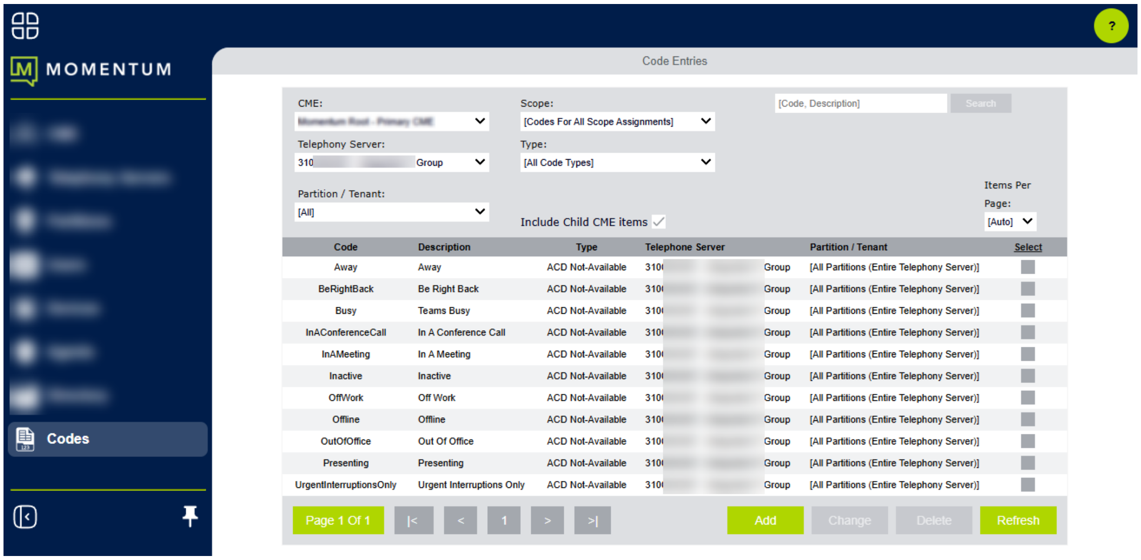
Cancel button to not perform the deletion operation and return to the directory administration view. You can also select several directory entries at a time in the list and delete them together in one go.

Directory Settings 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.



Code Entries

CME: [redacted]

Scope: [Codes For All Scope Assignments]

Telephony Server: 310[redacted] Group

Type: [All Code Types]

Partition / Tenant: [All]

Include Child CME items ✓

[Code, Description]

Items Per Page: [Auto]

Code	Description	Type	Telephone Server	Partition / Tenant	Select
Away	Away	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
BeRightBack	Be Right Back	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
Busy	Teams Busy	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
InAConferenceCall	In A Conference Call	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
InAMeeting	In A Meeting	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
Inactive	Inactive	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
OffWork	Off Work	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
Offline	Offline	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
OutOfOffice	Out Of Office	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
Presenting	Presenting	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□
UrgentInterruptionsOnly	Urgent Interruptions Only	ACD Not-Available	310[redacted] Group	[All Partitions (Entire Telephony Server)]	□

Code Entry Scoping: Code entries within the application have an assigned component scope. For example, code entries can be assigned to any/all telephone server configuration entries, which effectively means they're assigned application-wide and visible to all reporting users. 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.

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 as follows:

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.

Adding New Codes

To add a new code to the application configuration, click the Add button at the bottom-right of the table shown in the codes administration view.
In the "Add New Code" page that is then displayed, specify the details of the new code, and then click the Add button to save the new item and return to the codes administration view. Alternatively, click the Cancel button to discard the new code details and return to the codes administration view without adding the new item.

Changing 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.

Deleting Code Entries

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

Codes Settings Help

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

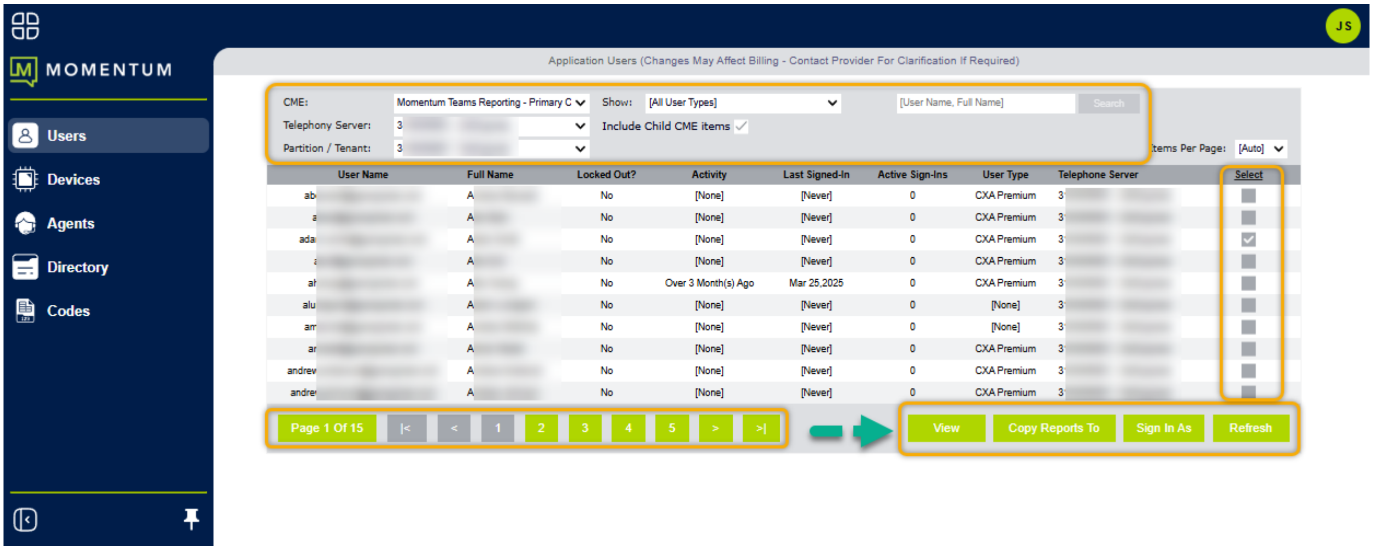
Users

Users

This Administration area is where user accounts can be managed. User Managers can come here to assist their organization's Application Users' access to and use of the application, or to sign in as the user, or move reports from one Supervisor to another..

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.



Application Users (Changes May Affect Billing - Contact Provider For Clarification If Required)

CME: Momentum Teams Reporting - Primary C
Show: [All User Types]
[User Name, Full Name] Search
Telephony Server: 3[redacted]
Include Child CME items ✓
Partition / Tenant: 3[redacted]
Items Per Page: [Auto]

User Name	Full Name	Locked Out?	Activity	Last Signed-In	Active Sign-Ins	User Type	Telephone Server	Select
ab[redacted]	A[redacted]	No	[None]	[Never]	0	CXA Premium	3[redacted]	☐
a[redacted]	A[redacted]	No	[None]	[Never]	0	CXA Premium	3[redacted]	☐
ada[redacted]	A[redacted]	No	[None]	[Never]	0	CXA Premium	3[redacted]	☑
a[redacted]	A[redacted]	No	[None]	[Never]	0	CXA Premium	3[redacted]	☐
ah[redacted]	A[redacted]	No	Over 3 Month(s) Ago	Mar 25,2025	0	CXA Premium	3[redacted]	☐
alu[redacted]	A[redacted]	No	[None]	[Never]	0	[None]	3[redacted]	☐
am[redacted]	A[redacted]	No	[None]	[Never]	0	[None]	3[redacted]	☐
ar[redacted]	A[redacted]	No	[None]	[Never]	0	CXA Premium	3[redacted]	☐
andrew[redacted]	A[redacted]	No	[None]	[Never]	0	CXA Premium	3[redacted]	☐
andre[redacted]	A[redacted]	No	[None]	[Never]	0	CXA Premium	3[redacted]	☐

Anyone requiring access to the CXA portal, regardless of role or use case, will require an Application User Account. The default Application User Accounts are created during implementation sync with Teams. The License assignments define the correct default Role for an application user. An Application User Account holds the basic information for a user, such as name, email address, access credentials, access permissions, and their user Role assignment.

An Application User Account must be created first in order for a role to be assigned.
Most user related management tasks are performed in **Administration > Fast PUsers**

There are 3 essential Default CXA 'user' types for the call reporting service:

- CXA Tenant Admin (Default assignment for the sole Teams Admin who manages the service setup and sync)
- CXA Advanced - Reporting Supervisor
- CXA [standard/premium] - Monitored Only

Two (2) additional User types are allowed to be created or assigned:

- Administrator - This is a Non-reporting user type + User Manager Role (ONLY)
- CXA Advanced Reporting Supervisor + User Manager Role (ONLY)

Please Note: Administrators can only manage or sign in as application user accounts with the same or lesser role access permissions. Attempts to edit or 'emulate' an account that has been granted higher access permissions will receive a notification that the user has insufficient access to do so.

⚠ **TO ENSURE SECURITY AND SLA ADHERENCE, THE DEFAULT ROLE SETTINGS/PERMISSIONS MUST <u>NOT</u> BE MODIFIED OR CUSTOMIZED.**

Add a Non-Reporting Administrator Account

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:

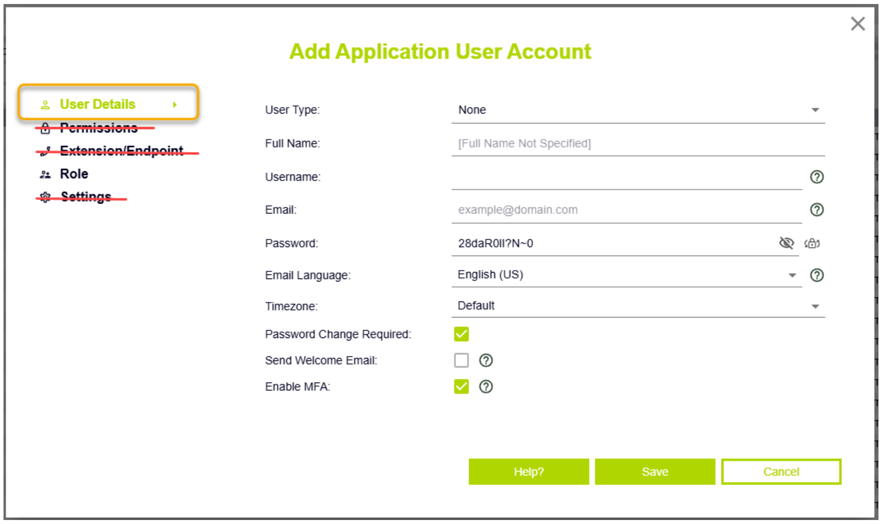
1. Click the menu icon in the top-left of the CXA portal.
2. Select **Administration**.
3. Select **Application Users**.
4. Click **Add**.

   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** = **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**: Use with **Password** field changes Highly 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 (or sms) they set up to assist with 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.



Add Application User Account

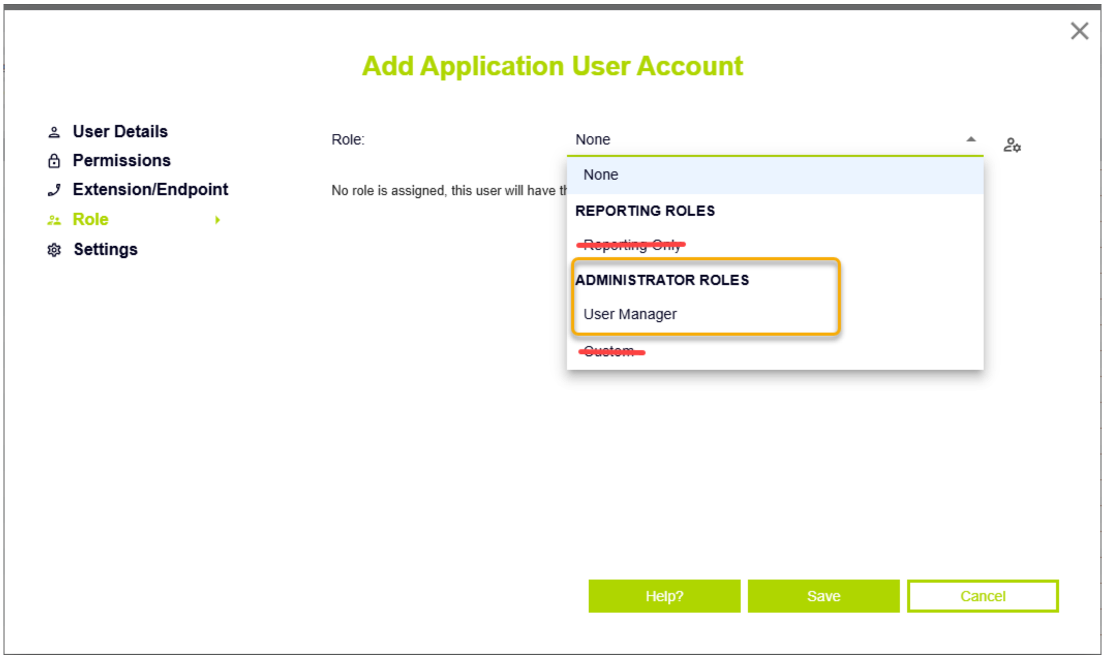
User Type:	None
Full Name:	[Full Name Not Specified]
Username:	
Email:	example@domain.com
Password:	28daR0lI?N~0
Email Language:	English (US)
Timezone:	Default
Password Change Required:	☑
Send Welcome Email:	□
Enable MFA:	☑

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.



Add Application User Account

Role: None

No role is assigned, this user will have th

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.

After clicking the Save button, the new permissions will be allocated to the user and available to them the next time they log in.

Create an Advanced Reporting User Manager Account

If a CXA Reporting Supervisor assigned an Advanced license requires the ability to copy reports to other Reporting Users, 'Sign in as' other Reporting Users, or help with passwords, they can be set as an Advanced Reporting *User Manager* to provide them them with sufficient Administrative access for these tasks.

Along with the Reporting section access the Advanced license provides this type of user by default, setting their Role to User Manager grants useful access to tools they might need within the Administration sections to view and/or perform the following:

- **View Devices**: Advanced Reporting Users can view all the Devices within their site that are available to report on.
- **View Agents**: Advanced Reporting Users can view all the Agents within their site that are available to report on.
- **View, Add, Modify and Delete Directory Entries**: Advanced Reporting Users have the permission to view the Directory and manage its entries in the Administration portal.
- **View Codes**: Advanced Reporting Users can view all the Account and Not-Available Codes that have been added to Akixi within their site that are available to report on.
- **Copy Reports To**: Advanced Reporting Users have the ability to copy reports between Reporting Users within their Akixi site.
- **Sign In As** (emulation/impersonation): Advanced Reporting Users can 'Sign In As' and ghost into user accounts. This allows them to view reports and make changes to reports for other users that exist within their site.

To configure an Advanced Reporting User Manager:

1. Go to Administration > Users
2. Select the CXA Advanced License Holder you wish to modify within the list (check box - far right)
3. Click on the **Change** button below the list.
4. Click on the **Role** tab.
5. Select **User Manager** for the Role in the drop-down selection tool and make no other changes.
6. Click **Save**. *Once the **Save** button has been clicked, you may exit. The Advanced Reporting Supervisor will be granted access to User Manager-level Administration tools upon their next login.*

Manage User Password or Basic Account Details

To manage things like password access or update a name for an existing user account:

1. Select a single user listing in the **Administration** > **Users** > **Application User** list view.
2. Click the **Change** button at the bottom-right of the table. *The "Change User" page is displayed*
3. Update the **User Details** of the existing user account - update Password or the name - as needed.
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 Manually Created Account

Use Caution. To delete an existing user account entry that was manually created (e.g., a Non-Reporting Admin):

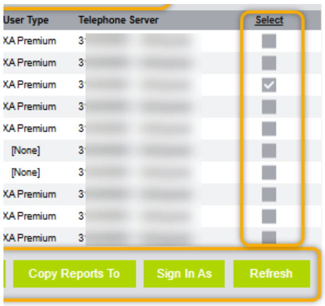
1. Select a single user listing in the Administration > Users view.
2. Click the **Delete** button at the bottom-right of the table.
3. In the *Delete User Entity(s)* page that is then displayed, click the **OK** button to confirm the deletion operation and return to the Application Users list view –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

Important Note: For Teams user accounts synced to CXA, it is suggested to Remove the license assignment in Manage Users and have the Teams Admin make any deletion changes to Teams user account information directly in TAC rather than simply deleting the user account information from CXA.

Copy Reports

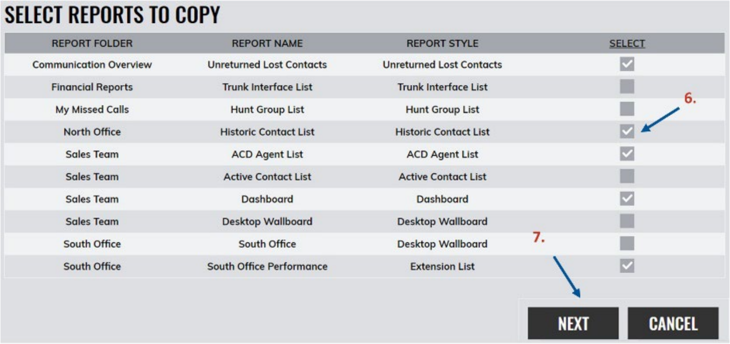
The copy reports feature allows Administrators to select reports to be copied from one Supervisor account to other Supervisors within the same site. Administrators have the flexibility to decide whether a single report or a collection of reports are copied over.

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.



User Type	Telephone Server	Select
XA Premium	3 [redacted]	□
XA Premium	3 [redacted]	□
XA Premium	3 [redacted]	☑
XA Premium	3 [redacted]	□
XA Premium	3 [redacted]	□
[None]	3 [redacted]	□
[None]	3 [redacted]	□
XA Premium	3 [redacted]	□
XA Premium	3 [redacted]	□
XA Premium	3 [redacted]	□

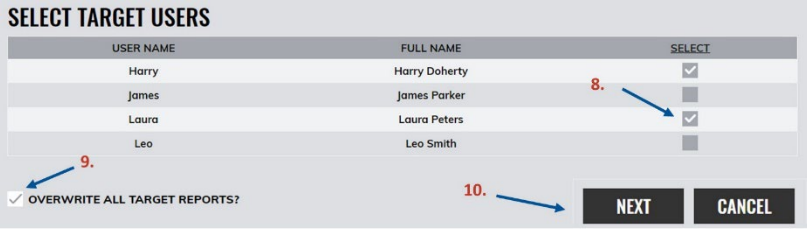
1. Click the menu button in the top-left of the portal
2. Select Administration
3. Chose Users
4. Tick the Select check box next to the user who has reports to be copied.
5. Click the Copy Reports To button.
6. Select the reports that to be copied from the user account
7. Click Next



SELECT REPORTS TO COPY

REPORT FOLDER	REPORT NAME	REPORT STYLE	SELECT
Communication Overview	Unreturned Lost Contacts	Unreturned Lost Contacts	☑
Financial Reports	Trunk Interface List	Trunk Interface List	□
My Missed Calls	Hunt Group List	Hunt Group List	□
North Office	Historic Contact List	Historic Contact List	☑
Sales Team	ACD Agent List	ACD Agent List	☑
Sales Team	Active Contact List	Active Contact List	□
Sales Team	Dashboard	Dashboard	☑
Sales Team	Desktop Wallboard	Desktop Wallboard	□
South Office	South Office	Desktop Wallboard	□
South Office	South Office Performance	Extension List	☑

8. Select the users that need to have the reports copied to their accounts
9. Optional: Click the check box if all of the users being sent the reports are to have all of their existing reports deleted and overwritten by the new reports being sent.
10. Click Next.

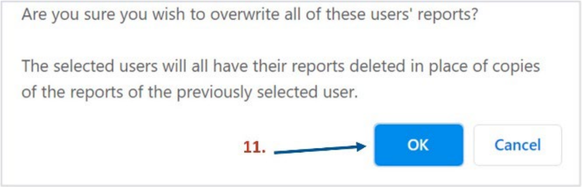


SELECT TARGET USERS

USER NAME	FULL NAME	SELECT
Harry	Harry Doherty	☑
James	James Parker	□
Laura	Laura Peters	☑
Leo	Leo Smith	□

✓ OVERWRITE ALL TARGET REPORTS?

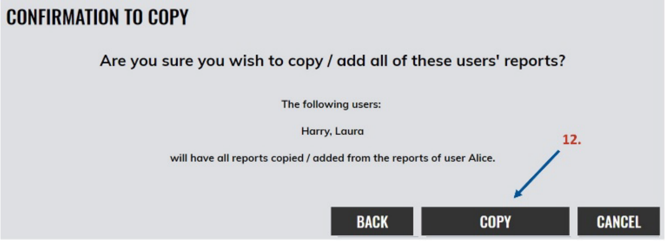
11. Click OK to provide confirmation that users' existing reports are going to be overwritten.



Are you sure you wish to overwrite all of these users' reports?

The selected users will all have their reports deleted in place of copies of the reports of the previously selected user.

12. Click the Copy / Overwrite (if step 9 has been followed) button to proceed. At this stage of the process, the Back button can be used to go back to the previous step in the wizard.



CONFIRMATION TO COPY

Are you sure you wish to copy / add all of these users' reports?

The following users:

Harry, Laura

will have all reports copied / added from the reports of user Alice.

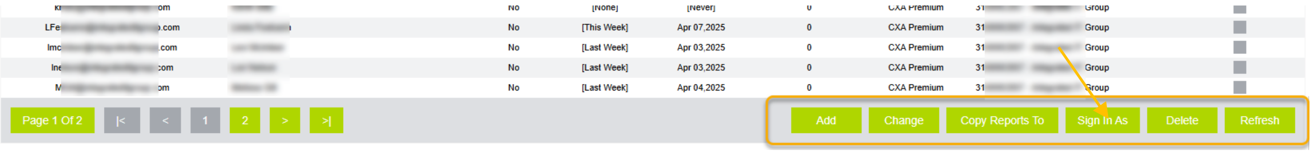
Once the Copy / Overwrite button has been selected, the copy reports wizard is complete, and all the selected reports will be copied across to the Application Users selected in step eight.

Sign In As

This feature allows the User Manager or Admin 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.

Please Note: An Administrator or User Manager cannot use *Sign In As* to access an account via emulation that has greater (higher) access permissions than their own account.

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



Kl[redacted]om	[redacted]	No	[None]	[Never]	0	CXA Premium	31[redacted]	[redacted] Group	■
LFe[redacted].com	[redacted]	No	[This Week]	Apr 07,2025	0	CXA Premium	31[redacted]	[redacted] Group	■
lmc[redacted].com	[redacted]	No	[Last Week]	Apr 03,2025	0	CXA Premium	31[redacted]	[redacted] Group	■
lne[redacted]com	[redacted]	No	[Last Week]	Apr 03,2025	0	CXA Premium	31[redacted]	[redacted] Group	■
M[redacted]om	[redacted]	No	[Last Week]	Apr 04,2025	0	CXA Premium	31[redacted]	[redacted] Group	■

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 Settings Help

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