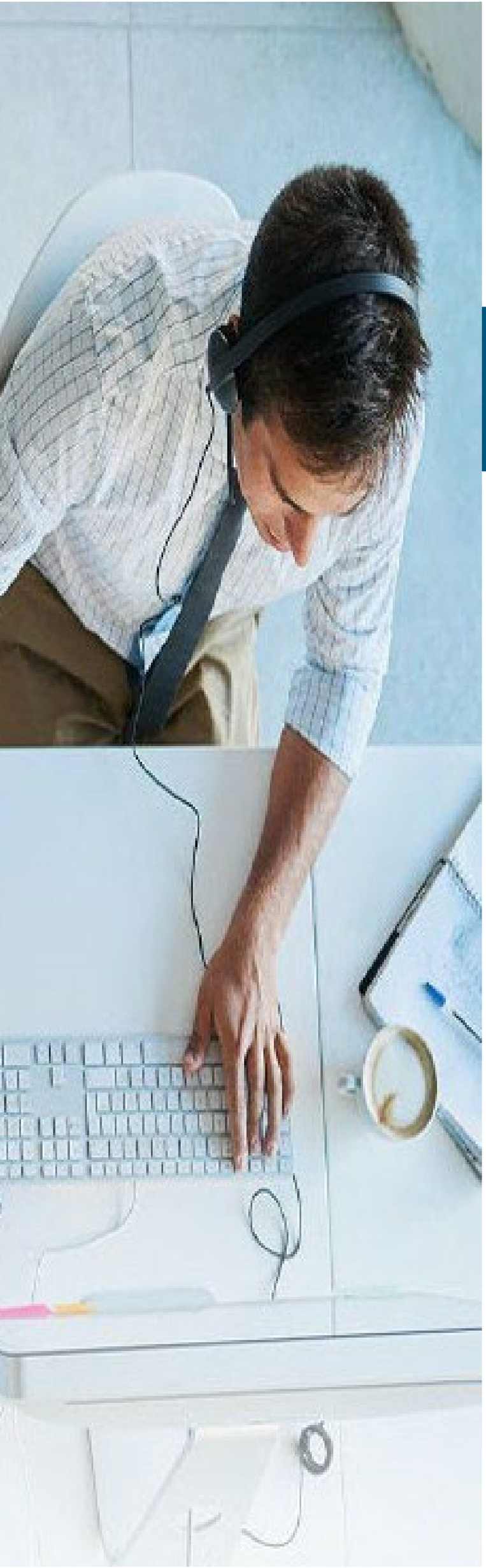


CALL RECORDING

Teams Tenant Admin

Quick Reference

MOMENTUM

Powered By: miarec

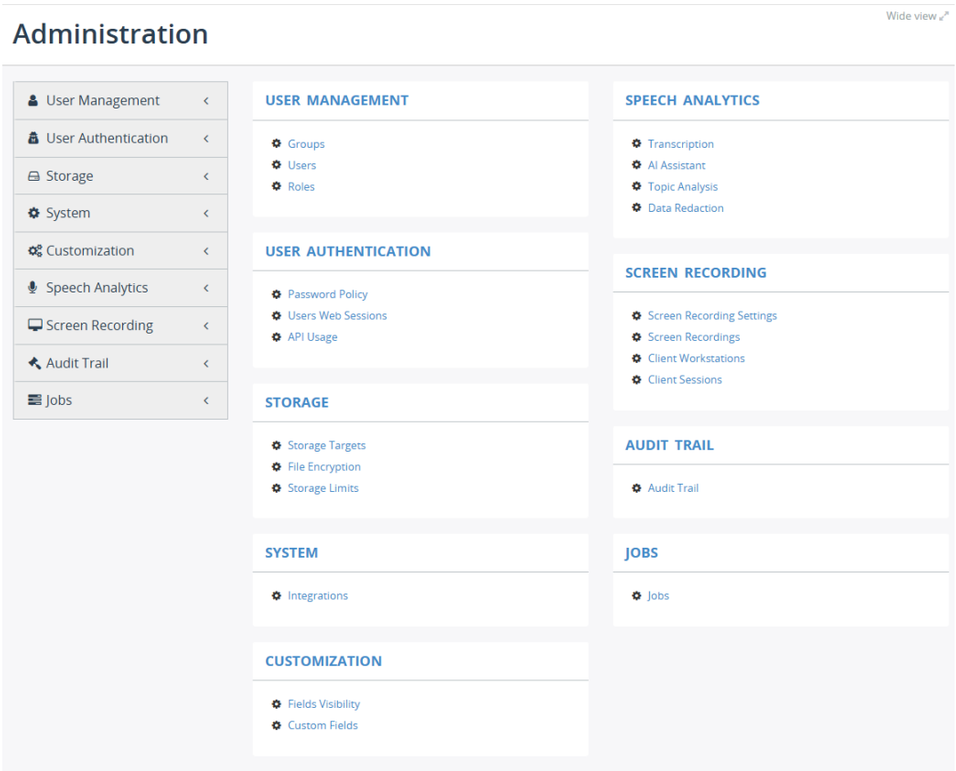
25Q1e

Introduction

This guide provides an introduction to the standard tenant-level Administration sections in the Call Recording platform (a MiaRec service). It is targeted to those granted Administrator-level access to Call Recording (typically System Administrators, IT, Teams Admins, Call Center Upper Management, etc.) whose job is to support and maintain the overall system for the licensed users within their organization. Administrators have access to all areas of the portal to view their organization's Dashboard account activity, Recordings, Reports, QA, and of course the Administration section tools.

The Administration section of the Call Recording Portal offers access to the tools necessary for management and maintenance of the Call Recording portal views, user assignments, storage, system, AI Tasks, and more *at the Tenant level*.

When first getting started once implemented, the Administrator will likely begin by reviewing the Roles, setting up their Groups, and then assigning the users to specific Roles, Groups, and (Teams only) some access permissions like license(s) or website credentials.

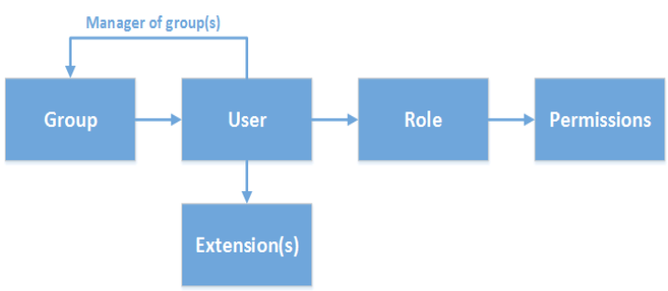


Standard Administration section view for tenant-level Administrators.

User Management

The Call Recording software provides role-based access control features with granular permissions. The tools for these tasks are located in the *User Management* section of the **Administration** tab.

Each user's account must be associated with one (1) Role and the correct license(s), and each Role is provided with a pre-defined set of access permissions designed to provide best practice use for security and compliance. Call Recording license holders should also be added to relevant Admin-defined Groups (either as a member or to manage) as needed for supervision and performance evaluation.



When you set for your Call Recording tenant users' permissions, you specify their levels of access along with group memberships:

- **Access Scopes**. These are a set of pre-defined permissions that can be applied in one go.
- **Managed Group**. Each user is assigned to the organization's tenant User Group by default, however the Admin may create the groups needed for their organization's use and then assign each user (or Supervisor or Admin) to one or more, as needed.
- **Permissions**. These are the permissions to specific features and tools that have been configured within a certain access scope.
- **License**. (Teams integrations only) Assignment of necessary license(s) for the user from the available license pool (purchased).
- **Restrictions**. Set restrictions based on IP network/address etc. for security.

Roles

Each user in the Call Recording (MiaRec) system needs to be assigned a Role. The role defines what system resources are accessible by each user and what operations are permitted on these resources.

Note: Tenant Administrators cannot create, edit, or delete Roles or Role settings.

Example Standard Tenant Roles that may be assigned to a licensed User may include:

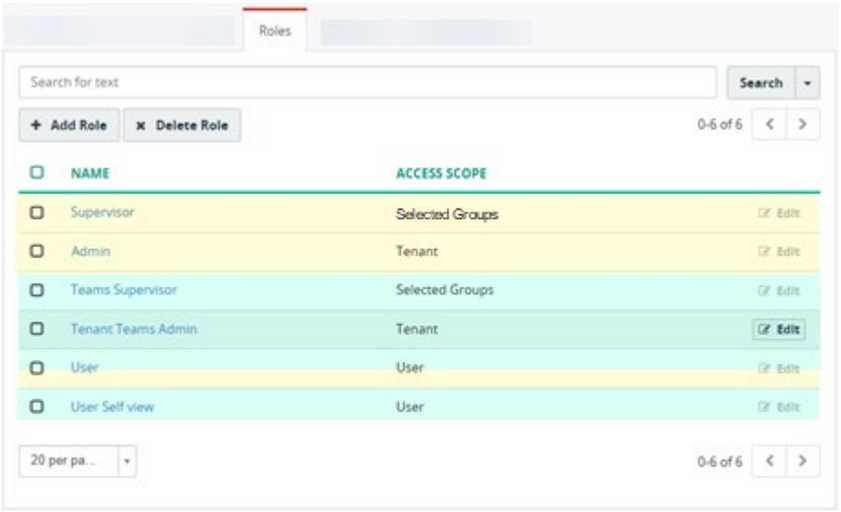
User (legacy: Recorded User or Agent) – This is the default Role for all license holders in most systems and should be the Role assigned for any users in the recording group who will be recorded but do not need to be granted access permissions to view or work in the Call Recording portal. This Role is designed to be assigned to most Call Recording license holders, as the vast majority of license holders should not access Call Recording.

User Self View (legacy: Agent View or User View) - Select this role for any users in the recording group who will be recorded and will be granted limited permission to access Call Recording to view, playback, and add notes to their own recordings (calls or screen). This user Role also allows for Teams tenants to assign a user sufficient access to log into Call Recording to utilize the Pause/Resume or Start/Stop recording functions for compliance. This user type is rarely assigned but made available to allow for essentially read-only access to the user's own call (or screen) recordings and some compliance tools. Those with this Role assignment typically perform tasks only in their own Dashboard and the Recording Tab.

Supervisor | Teams Supervisor - Select this role for any users in the Recording Group who are granted access permissions to Call Recording to review the recordings of themselves AND others in the Managed Groups assigned to them in order to monitor recordings and evaluate performance for Quality Assurance. This role is typically granted to Call Center Managers, Contact Center Supervisors, Management, etc. This role has full access to monitor and annotate the call recordings for any assigned groups of users in the Recording Reports and QA sections, and may also be allowed visibility and limited access to view or work in a few areas in the Administration Tab by the Service Provider (e.g.: Evaluation Forms (if purchased), Fields/columns Visibility Configuration, Manage Users, etc.)

Admin | Teams Admin – The Administration Role is for the licensed users who have been assigned Admin license add-ons and are authorized by the organization to perform all Supervisor level tasks **plus** the Administration-level tasks for the Call Recording environment. This role manages user groups, manages user profiles and access, assigns users to groups, views and manages key integration and token usage data, manages users' web sessions, administers AI tasks, storage targets, administers automated and manual Jobs, and can review/annotate the work of other Admins/Supervisors/Users. This is a tenant-level administration Role and should be granted to more technical individuals (or in Teams accounts to Teams Admins).

Navigate to **Administration > Users Management > Roles** to see a list of available roles and review the settings for each.
These can include:



In this example, the yellow highlighted items are the standard BroadWorks Call Recording Tenant Roles and the blue highlighted items are standard Teams Call Recording Tenant Roles.

The default User Role (recorded only - no access to work in the Call Recording portal is - or should be - granted) is used in both Call Recording tenant types.

Note: One additional Role not shown is **API User**. This role is rarely used and should only be assigned to an API developer for sufficient access to connect for organization in-house development of API Calls to Call Recording. It is important to note that the use of Custom developed API calls to Call Recording is “use at your own risk” and can impact Service Provider Support SLAs.

Clicking **Edit** next to a Role allows the Admin to review the pre-defined settings for each Role.

Reminder: The access scope and feature/tool permissions are pre-configured for each Role and cannot be modified by an Admin at the Tenant level.

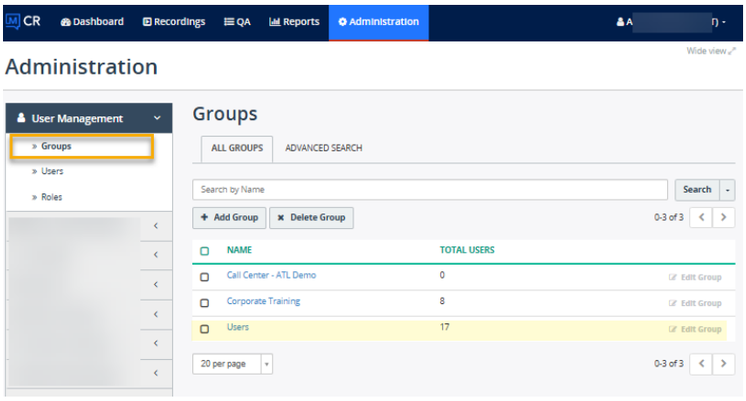
Groups

Each licensed User will be added to the default **User** group and must remain there. The default User group should never be edited, and users added to it should not be removed from this group to ensure their Call Recording functionality remains intact.

All users can belong to more than one group created within the Administration tab. Most users are just members of their default group and any others they are assigned to, with their calls being recorded. However, some license holders may need access the call recordings of others to perform work – these would be Supervisors. For example, a Supervisor may be assigned to perform tasks for the call recordings of themselves and the Users in one or more Managed Group assignments. In this case, s/he would be a member of the default User group and can be a *member* of one or more other groups of users *and* can be assigned by an Admin to one or more Managed Groups of users to oversee.

Access Groups

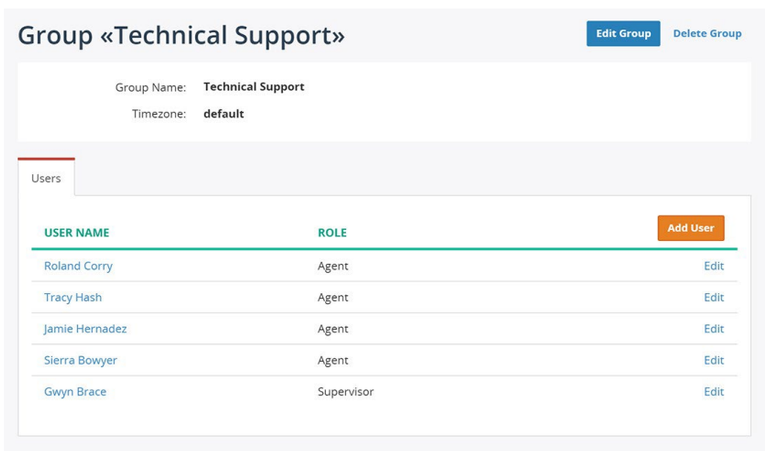
Navigate to Administration > User Management > Groups to view Group management tools.



The Administrator may create new groups or edit existing ones in this section – other than the original Group that all users are assigned to. The default ***Users*** group must remain untouched. Changes to that group of any kind will result in negative impacts on call recording functionality for Call Recording license holders.

Once created, the licensed users in the User List may be assigned to Groups as needed in their User Profiles.

The Group's profile view (click on the Group Name link) displays a list of all users who are assigned to the Group as members.
The display offers the user's name and their assigned Role, as well.



Add a Group

Go to: Administration > Manage Users > Groups:

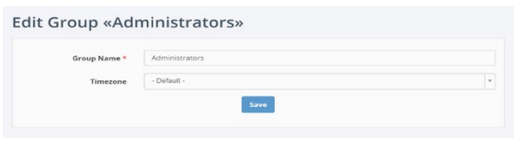
1. Click on the Add Group button
2. Define the Group Name (required) and the Timezone (optional)
3. Click Save.

Search Groups

Use the Search feature at the top of the page to enter a name and press **Search** to find matching results.

Edit a Group

Click on the Edit option adjacent to a Group in the list (far right) to modify the Group Name or Timezone (note the default group timezone assigned here can be overridden by the Timezone noted in a User's profile).



Delete a Group

Use Caution. If your role allows you to use the delete function:

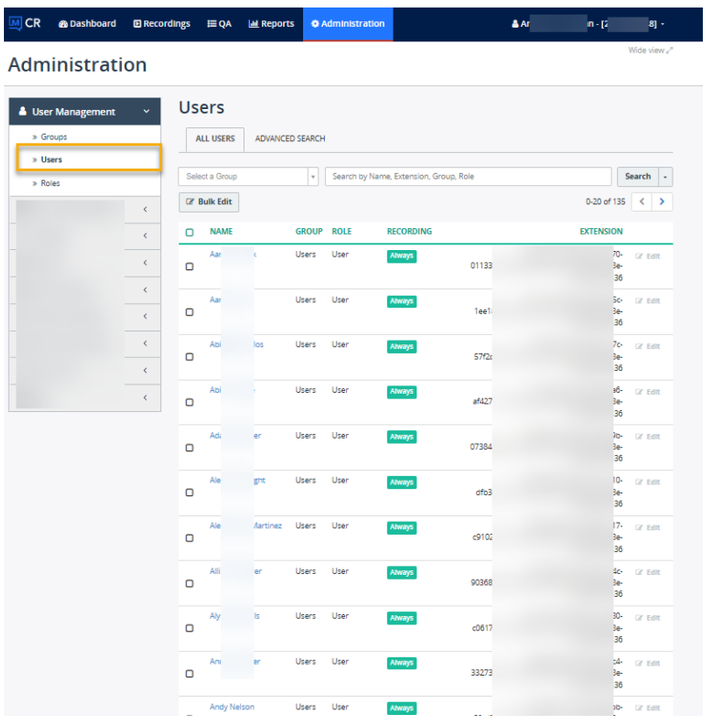
Select the group by placing a check in the adjacent box (column 1) and then click on the Delete button above the list. Once deleted all users assigned to the group will have that assignment removed and Supervisors assigned to manage the members of the group will no longer see those users in the recordings they manage.

Best practice: Check the users and supervisors who are members of the group and reassign them to alternate groups as needed prior to deleting the desired Group.

Users

Go to **Administration > Users Management > Users**.

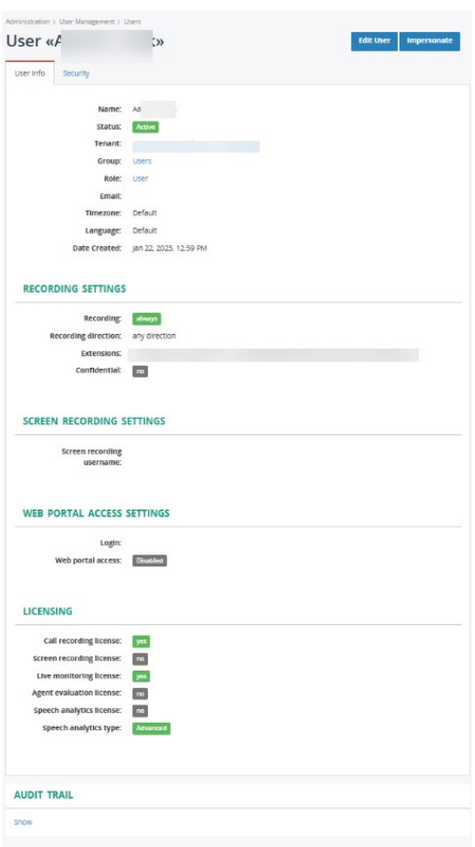
This area provides the tools needed for Call Recording portal user management. This includes recording policy, role, license(s), permissions, and Group assignments.



You can **Search** users by name, group, role, or extension (once those last three have been defined and assigned to users).

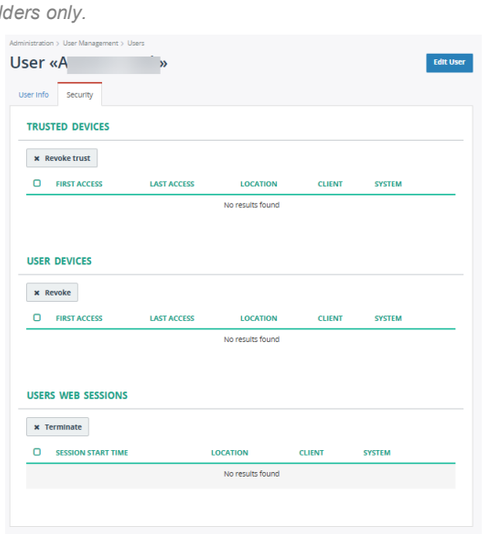
View User Info

Click on the user's name in the Users list to display the User Info view. From here Admins can also elect to Edit or Impersonate the user.



View User Security

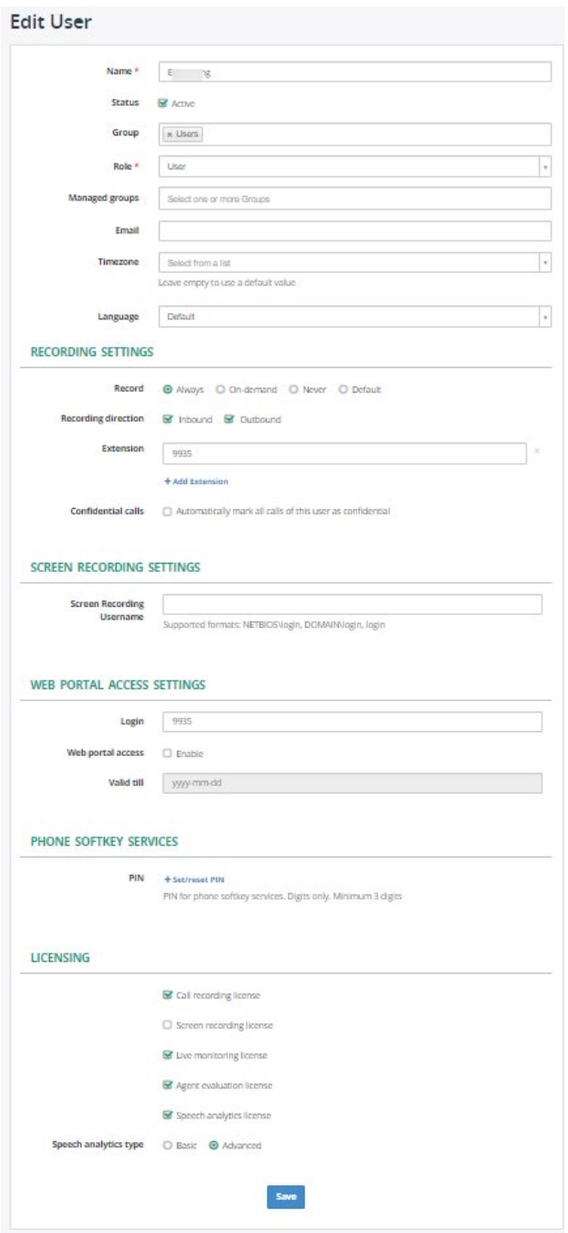
The **Security** tab is displayed in a User's Profile while an Admin is in **View** Mode. This section also allows an authorized Admin to terminate or revoke access as needed. *Some information here is for active Screen Recording license holders only.*



Edit User

1. Click on the Edit option adjacent to the desired User in the Users list (far right column)
   - or while viewing the User Info dialog, click on the Edit User button (top)
2. Modify the following, as needed:

USER INFO



- **Name***: Required. Enter the user's name.
- **Status**: Click to place a check in this box to ☑ enable/activate this user.
- **Group**: Type the name of a Group currently defined in the system for your organization to add this user to it as a member. Repeat to add the user to more than one group.
- **Role**: Select the correct role type for this user from the drop-down selection tool
- **Managed Groups**: (For a Supervisor or Admin) Select one or more groups defined within your system for which this user will be authorized to view/edit/annotate/QA/Monitor/etc. the recordings of members. Repeat to assign more than one managed group to the Supervisor.
- **Email**: Enter the email address for this user.
- **Timezone**: *Default = The timezone noted for the tenant during implementation*. This field defines the user's timezone and overrides any set at higher levels.
- **Language**: *Default is English*. Select the display language from available options in the drop-down list.

RECORDING SETTINGS

- **Record**: Choose one of the following:
  ⦿ Always
  ○ On-Demand = unavailable for use
  ○ Never
  ○ Default = unsupported
- **Recording Direction**: Click to specify whether this user's Inbound and/or Outbound calls will be recorded
- **Extension**: Optional - enter the number or extension for this user (requires at least 3 digits)
- Use the +Add extension option to enter additional extensions for this user
- **Confidential Calls**: Click to enable ☑ if you want all calls recorded for this user to set to Confidential automatically
- **Coming soon**: Record Teams Meeting: Click to enable ☑ if you want all Meetings this user joins or starts to be recorded by MiaRec. Note: Enabling meeting recording in Call Recording can impact billing, reporting, and QA metrics. Use with caution.

SCREEN RECORDING SETTINGS

- Screen Recording Username: (if $Add-On license purchased)
  Enter the login credential following the format noted directly below the field.

WEB PORTAL ACCESS SETTINGS

- **Login:** Enter the user's login for Cloud Services Portal access IF they will be allowed to access Call Recording to perform work using SAML 2.0 authentication. The basic login credential format is [the user's 10-digit teams phone number]@mymtm.us. Example: 8885551212@mymtm.us All authorized Call Recording Portal users must access Call Recording via the link in their Cloud Services Portal Dashboard when SAML 2.0 authentication is in use.
- **Web Portal Access:** Enable ONLY if this user will be allowed to access the Call Recording Portal to perform work on call recordings. The Service Provider system synchronizes this data with the Cloud Services Portal at least once a day to update and allow for SSO access from the Cloud Services Portal to the Call Recording Portal, where authorized in both portals. An additional setting in the Cloud Services Portal must also be set to display the link to the Call Recording Portal in the user's Cloud Services Portal dashboard (or Call Recording section for Admins). Since provisioning may take a few days to complete for all users, the Teams Call Recording Admin will need to return to the Cloud Services Portal to allow access link visibility as the data updates. See steps below. These security measures help keep sensitive call data safe.
- **Authentication Type:** SAML 2.0 is the supported option here for Teams Call Recording organizations. This option ensures the correct SSO protocols are met and the connection to synchronize with the Cloud Services Portal is in place. Any other authentication options that could be selected here are either unsupported or will require additional setup by the Admin (outside the scope of the standard/recommended integration steps). The other Authentication type options are 'use at your own risk.'
- **Valid till:** Optional. Enter a date to define the end of access permissions for this user. Once this date has passed the user cannot access Call Recording Portal without Administrator intervention. Leave blank if there is no end date for access.

PHONE SOFTKEY SERVICES

- +Set/Reset PIN - Enter the 3-dgit minimum softkey PIN for this user. NOTE: Not needed or available to set up for Teams integrations.

LICENSING

For BroadWorks customers, licensing is assigned based on the licenses and add-ons purchased and assigned to users during the ordering process. This is handled by the Service Provider and is not available for editing here.

For Teams Integrations (only): Choose the appropriate license(s) for this user from the following:

☑ **Call recording license**: Default = enabled. Click to enable/disable. (Needed for call recordings to be saved for this user)

☐ **Screen recording license** (Always an $Add-on). Assigning this license tells Call Recording that a user also uses the Screen Recording service on their desktop during active calls (this option requires additional add-on license and installation plus setup on the desktop as well as credentials to sign into the desktop screen recorder which are defined above).

☑ **Live Monitoring license** (Typically an $Add-On/Option). Default = enabled. Assigning this license tells Call Recording that the calls for this user can be live monitored and/or can utilize real-time calling features (like Pause/Resume).

☐ **Agent evaluation license** (Always an $Add-on/Option). Default = disabled/unassigned. Enabling / assigning this license tells Call Recording that the calls for this user can be evaluated either manually or (if setup) automatically by **AI** if in use with an assigned Speech Analytics license.

☐ **Speech analytics license** (Typically an $Add-on/Option). Default = disabled/unassigned. Enabling / assigning this license tells Call Recording to turn on analytics and transcription for this user's calls, which also allows the use of AI-driven features like auto-Evaluate/QA, call summary, redaction, and more.

3. Click **Save** when finished to submit all changes and exit the Edit dialog.

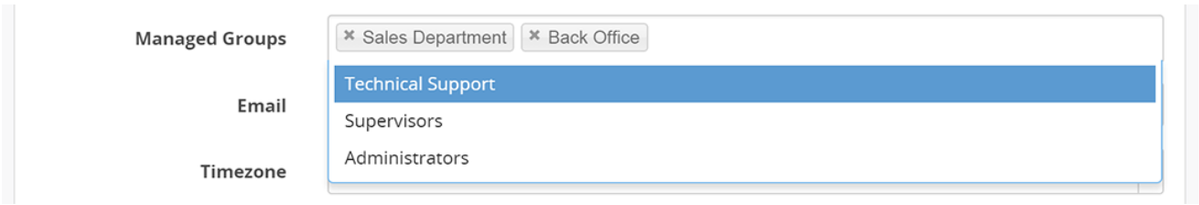
Impersonate

Administrators have the option to **Impersonate** users in their Tenant and view the web portal as though they had logged in as that user.

Note: Administrators may only function with the same level of access as the user they are impersonating while *impersonation* is underway. To return to performing Administrative tasks once again and stop impersonating, the Admin must click on the Profile drop-down (top right) and select the option found in the menu there to End Impersonation.

Managed Groups

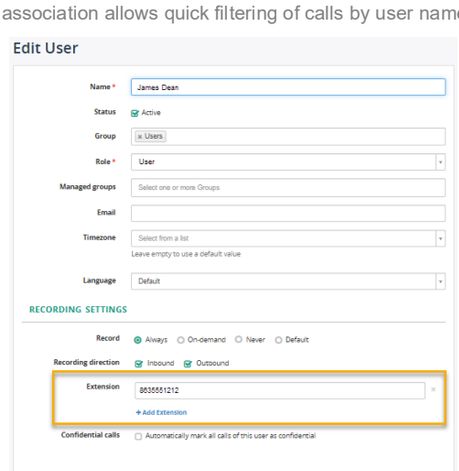
If the user's role has access level "Supervisor or Admin", then you can configure which groups are managed by this user. The group manager has access only to users and their calls recordings, which belong to his managed groups. You may select one or more managed groups from the list of Groups already created.

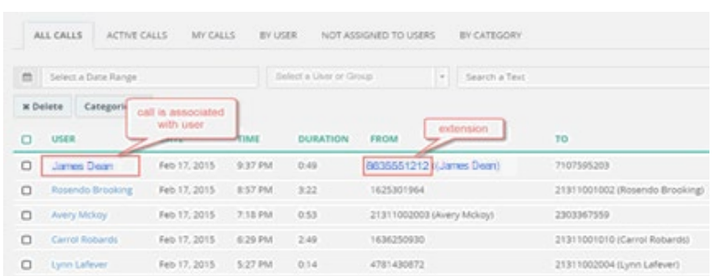


Associating Calls with Users

Call Recording automatically associates calls to each user based on the users' known extension, TN (telephone number), or for those in Teams Tenants, the User's Teams ID which contains their TN/Extension information.

Extensions are Configured on the User's Profile page. Typically, Call Recording gains that information and configures it in the Profile when the user is added to the User Group. In the example below, user "James Dean" is configured with extension "8635551212". When Call Recording recognizes a call with extension "8635551212", then the call is automatically associated with user "James Dean". This association allows quick filtering of calls by user name or assigned TN/Extension/ID.



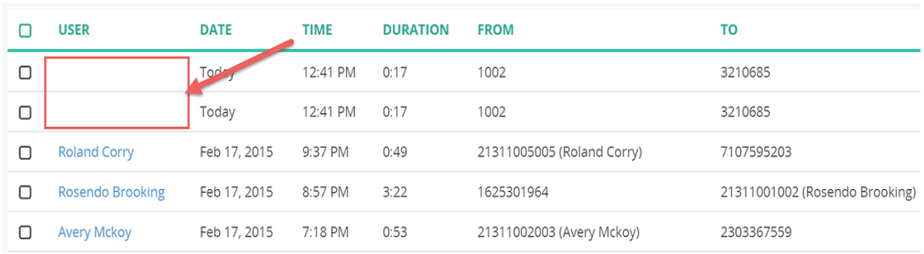


Also, this information is used when granting access to recordings. For example, a Supervisor will be able to view only the call recordings which are associated with users in his/her group and the account profile User Name (along with its extension information) of the members of the group to help to identify that association.
If 'James Dean' is in a Managed Group assigned to the Supervisor, s/he will be able to view and work with James Dean's call recordings.

Manage Unknown Extensions

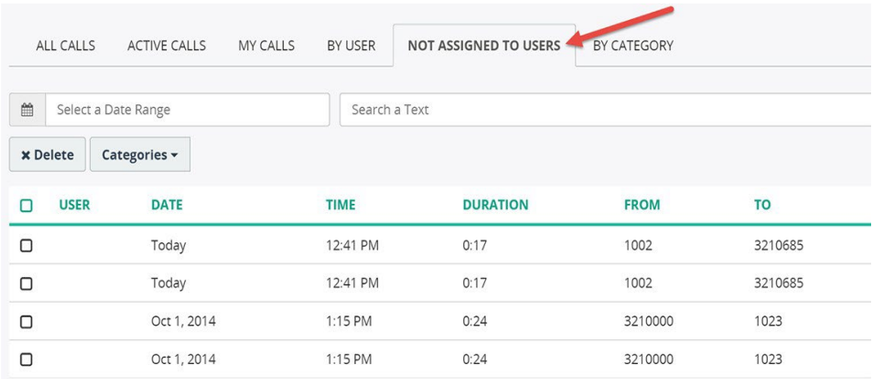
If Call Recording doesn't recognize the extension for a recorded call, then a default recording rule applies.
By default, Call Recording is configured to record such unknown calls and note the missing User / Extension assignment for Admin review.

When a call with an *unknown* extension is recorded, then the column "User" will be empty in the Recording section.



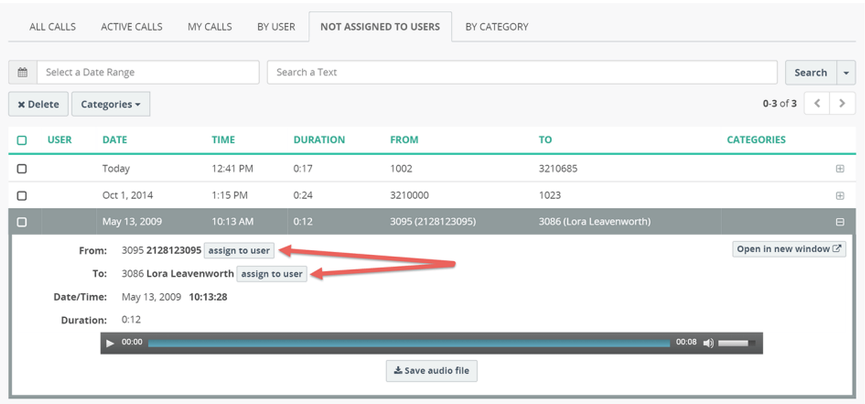
USER	DATE	TIME	DURATION	FROM	TO
	Today	12:41 PM	0:17	1002	3210685
	Today	12:41 PM	0:17	1002	3210685
Roland Corry	Feb 17, 2015	9:37 PM	0:49	21311005005 (Roland Corry)	7107595203
Rosendo Brooking	Feb 17, 2015	8:57 PM	3:22	1625301964	21311001002 (Rosendo Brooking)
Avery Mckoy	Feb 17, 2015	7:18 PM	0:53	21311002003 (Avery Mckoy)	2303367559

Also, these calls are shown in the panel called "Not assigned to users" (visible only to Administrators in the Recordings view).



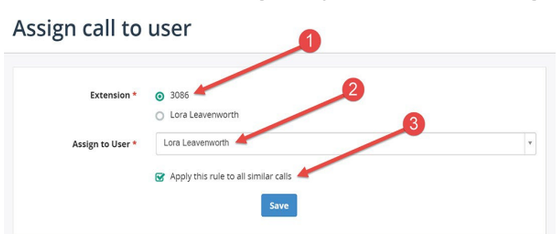
An Administrator can manually assign a call with missing extension information to one of existing users in their Tenant.

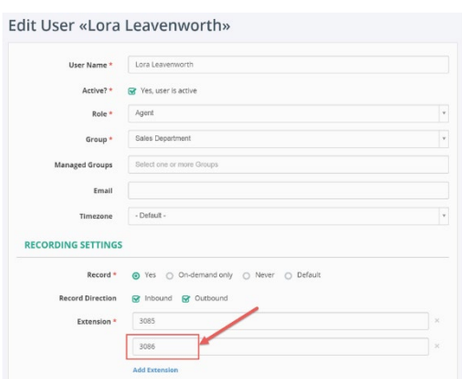
1. First, s/he needs to click on an 'unknown' call to display the Call Details.



2. Then click on the button "**Assign to user**" for the correct number listed (From or To)… this tool is available to the Admin in this view. A new page opens to show the following options:

   - **Extension:** Administrator should decide whether to use the phone number/extension or the phone name to associate matching calls to a user.
   - **Assign to User:** Choose the User with whom to associate this call using the drop-down list.
   - **Apply this rule to all similar calls:** When checked, all other calls with the matching information will be automatically assigned to this user. *Note: Call Recording will only search for matches among those calls that are not yet assigned to any other users.*



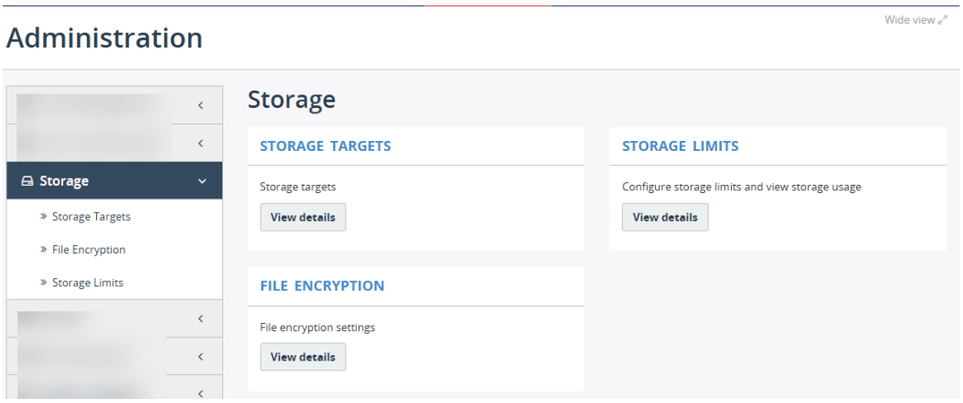


3. Click on the on Save button when ready. The matching recorded calls in history will be searched and automatically assigned to the selected user.

   Additionally, the selected extension will be automatically added to the Extensions section in the User's Profile.

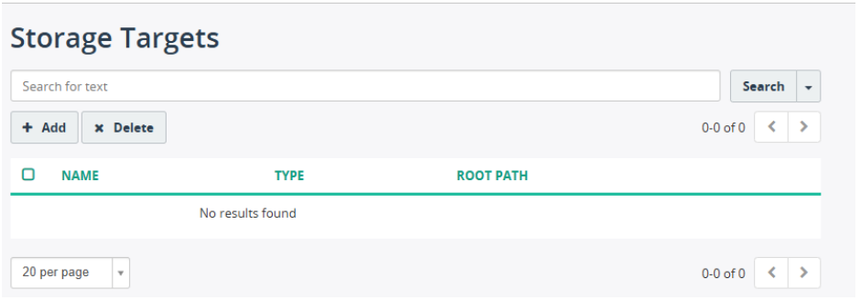
Storage

This section offers tenant-level tools for reviewing or managing data storage.



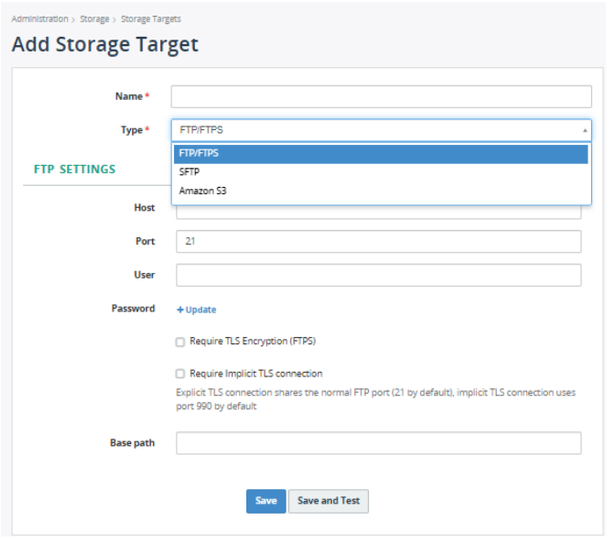
Storage Targets

Click View details under Storage Targets to review a list of created targets and some administrative tools to Add, Edit or Delete these targets.



Add a Storage Target

1. Click the Add button to open the Add storage target dialog.



2. Enter or define the following:
   - Name: Required. Enter a unique identifier to make it easy to locate this storage target in lists.
   - Type: Required. Choose from FTP/FTPS, SFTP, or Amazon S3 and then define the corresponding settings offered below:

FTP/FTPS Settings	SFTP Settings	Amazon S3 Settings
Host	Host	S3 Bucket
Port	Port	AWS Access Key ID
User	User	AWS Secret Access Key
Password	Password	S3 Endpoint URL
Base Path	SSH Key	Region
	Base Path	AWS Signature Version
	Atomic POSIX rename	Use Server-Side Encryption

3. Click on Save and Test to verify functionality.
4. Click Save when tests are good, and you wish to put this into production.

Edit a Storage Target

Choose a created Storage Target in the list and select Edit.

Make changes as needed, click Save and Test to verify functionality, and click Save when finished.

Delete a Storage Target

Click to place a check in the box adjacent to a specific Storage Target in the list and click Delete.

File Encryption

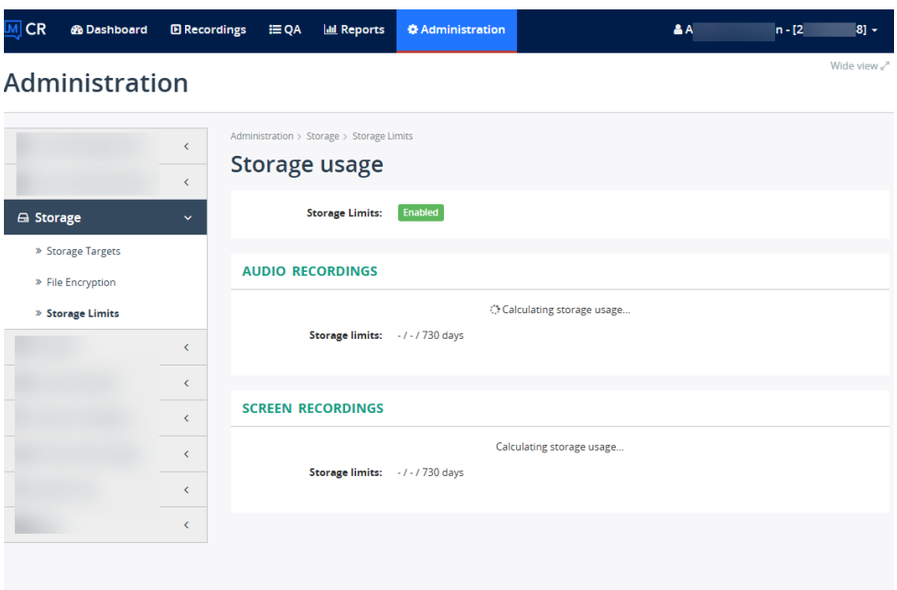
If enabled for use / access at the tenant level by the Service Provider, Admins may be granted permissions to manage some settings for file encryption.

Call Recording provides rock-solid audio encryption functionality by default, ensuring all call recordings are securely stored. Call Recording encryption functionality helps companies confidently adhere to the highest corporate security standards and comply with legal regulations such as PCI-DSS, HIPAA, Dodd-Frank, and Sarbanes-Oxley.

Check the vendor documentation Here to learn more.
Note: This documentation is mainly for Service Providers, information about how things work could be useful as a knowledge resource.

Storage Limits

When Storage Limits is clicked, this section opens, updates the data, and displays the current storage usage for audio (and screen recordings if in use) based on the specific storage package purchase. Note: it may take some time for the data to update and display.

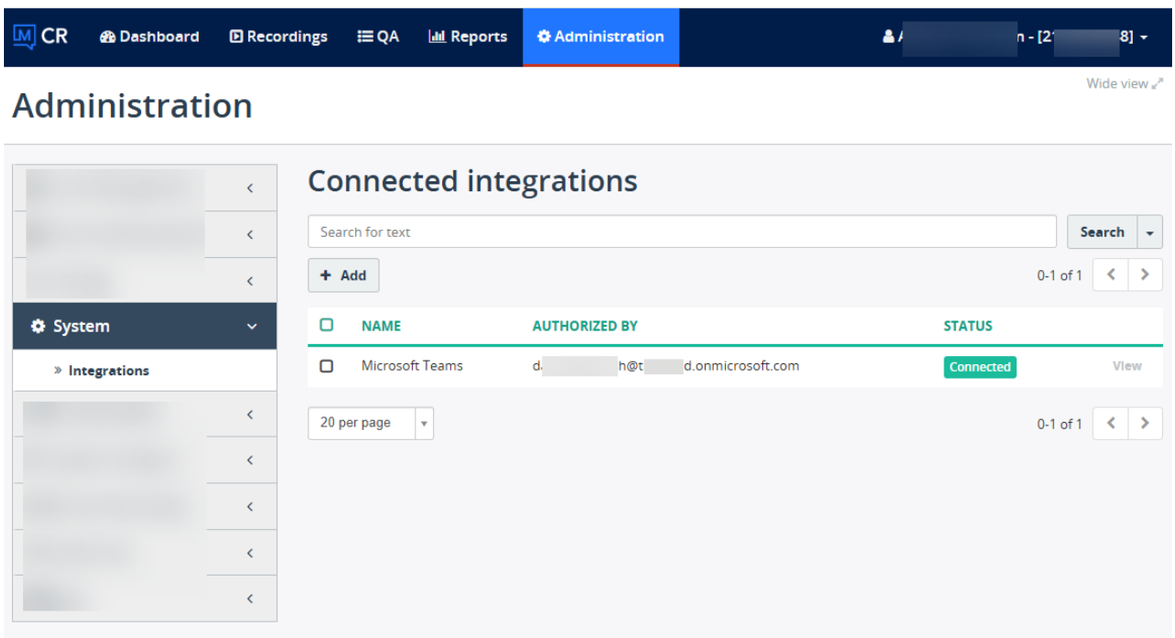


System

NOTE: This area may be shown to Teams Tenant Admins.

This is where the Global Teams Admin will use the wizard to connect Call Recording to Teams during implementation. Once completed, this area allows the Admins to review the current connection status information.

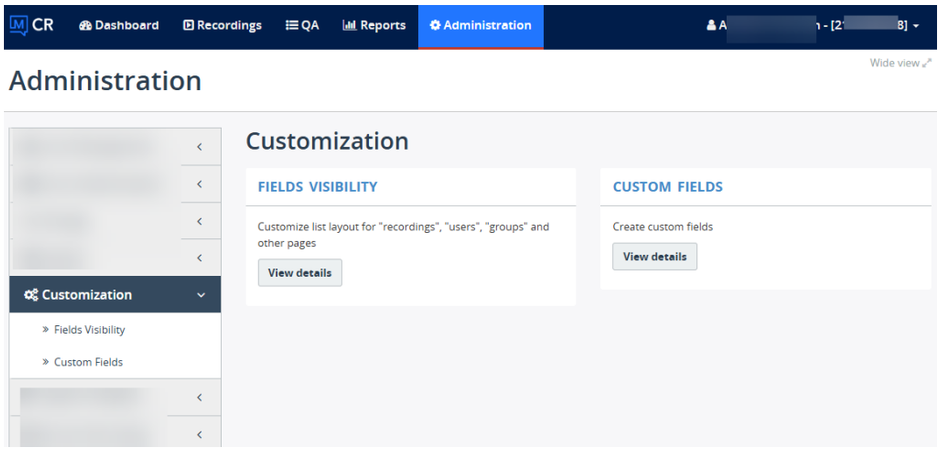
Use Caution. This area should be left to the Teams Global Admin to manage. The Teams Tenant Admin should instruct any other Admins for their Organization not to access or make any unauthorized changes or use the +Add option in this area post-integration as this can result in a loss of functionality.



Information about Administration tasks that can be performed above the Tenant level (Service Provider Level) can be found in the CR System Admin Guide. Note: If changes to the standard Tenant setup (a Customized Tenant) are requested to be performed by the Service Provider, Professional Services charges may be incurred and modifications to the Support SLA may be initiated.

Customization

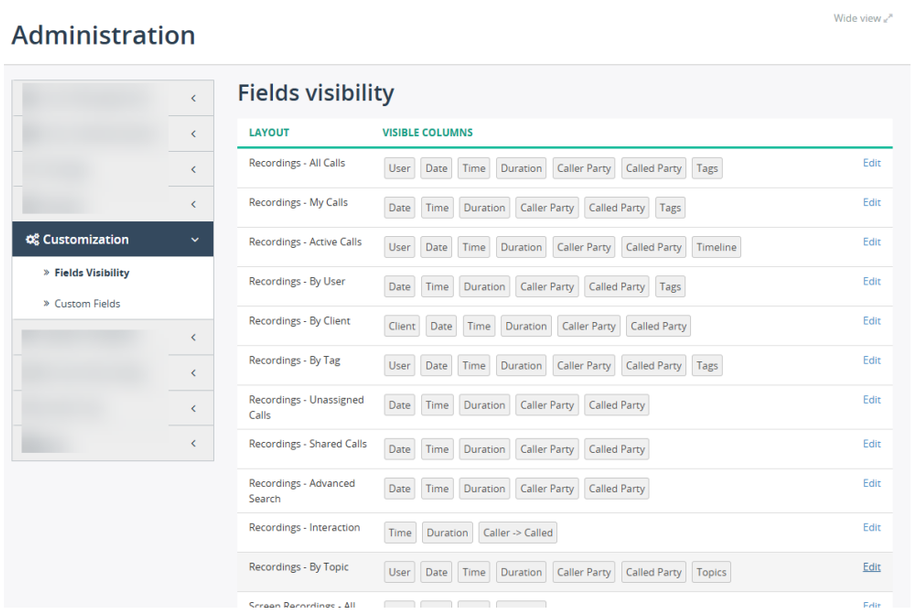
In this area of Administration, authorized Admins can modify how the tables and report data views display to Call Recording users by selecting specific data types and arranging the column orders.



Fields Visibility

Here an Admin may edit the fields visible in any of the listed views (pages, sections, and reports).

The current fields for each layout are listed in the Visible Columns section for quick review.



Edit Field Visibility

Click on Edit next to a listing in Fields Visibility to review the display management tools.

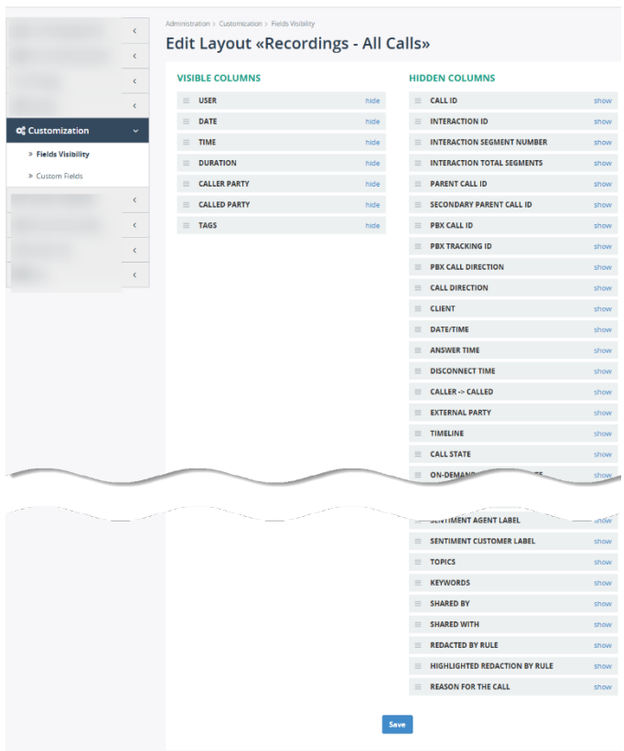
Simply click on Show next to an option in the *Hidden Columns* to add it to the Visible Columns list – or use drag-n-drop to move the item over to Visible to perform the same task.

You may also change the order of Visible columns to suit your organization's needs.

The field listed at the top of the Visible Columns list displays as the first column shown in the table and the rest display in the order set here from left to right in the table within the selected view.

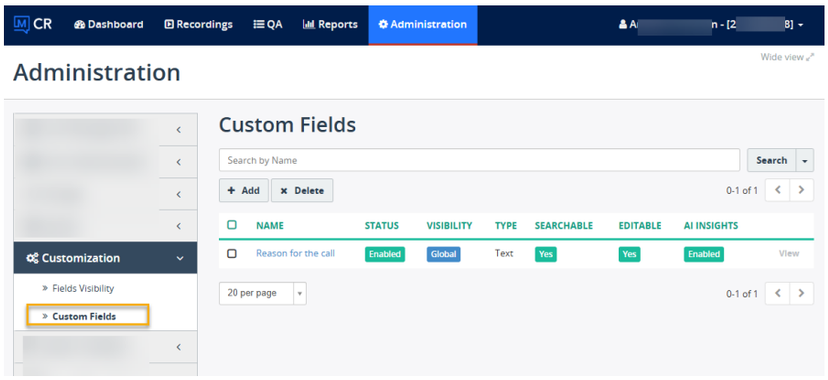
Use the Hide option (or drag-n-drop) for any items in the Visible Columns list to remove a selected field's data from view.

Click Save at the bottom of this section when finished to close the dialog and update the selected view in Call Recording with your changes.



Custom Fields

This area offers the ability to add, edit and delete customized fields for Call Recording user visibility.

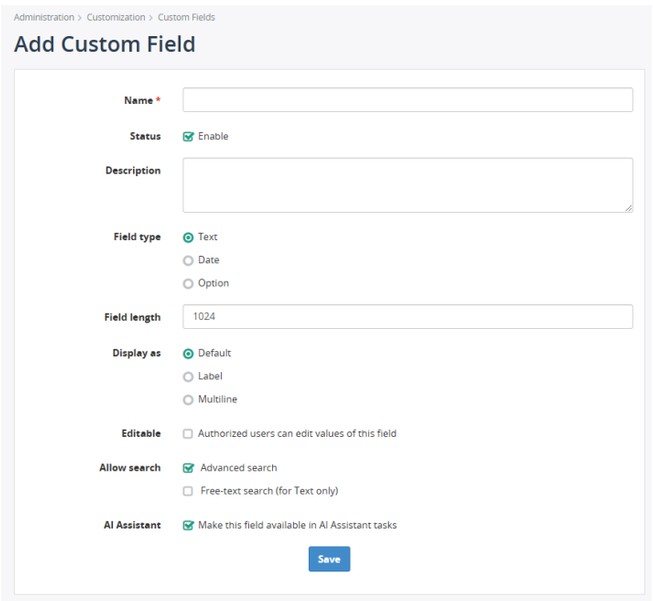


A default field called *Reason for the call* is created during implementation. This item is necessary and cannot be edited.

Add a Custom Field

1. Click on the Add button above the list to begin.
2. Enter or select the following:
   - **Name**: (required) – a unique identifier should be entered here.
   - **Status**: ☑ Enable / ☐ Disable
   - **Description**: Use this field to describe the purpose of the custom field.
   - **Field Type**: Admin must select an option and define related settings.
     - Text: this option allows the admin to define the field length (characters and spaces) allowed.
     - Date: This option allows the admin to add a Date option as a custom field.
     - Option: This selection opens the ability to create options the viewer can select. This is useful for creating buttons and using the Add option feature to label the buttons.

   Additional settings include:
   - Display As: choose the display type from Default, Label or Multiline
   - Editable: define whether authorized Supervisors can edit the field value
   - Allow Search: choose Advanced or Free-text search for text only use
   - AI Assistant: ☐ Choose whether the AI will use the data in this custom field in its tasks.
3. Click Save at the bottom of the dialog to exit and submit the changes.
   If set to Enabled, this new Custom field will now be available for selection in the Fields Visibility list while editing a view.



Edit a Custom Field

If the Edit option is available for a Custom field, the Admin may modify its settings and Save to update or disable it.

Delete a Custom Field

Use Caution. If you elect to Delete a Custom Field, it will become unavailable immediately in any views it may have been assigned to.

Speech Analytics

Reference the *CR Speech Analytics Guide* to review additional information about how Speech Analytics can work in Call Recording.

The Administrator or Teams Tenant Admin Role has access to the following tools within this section:

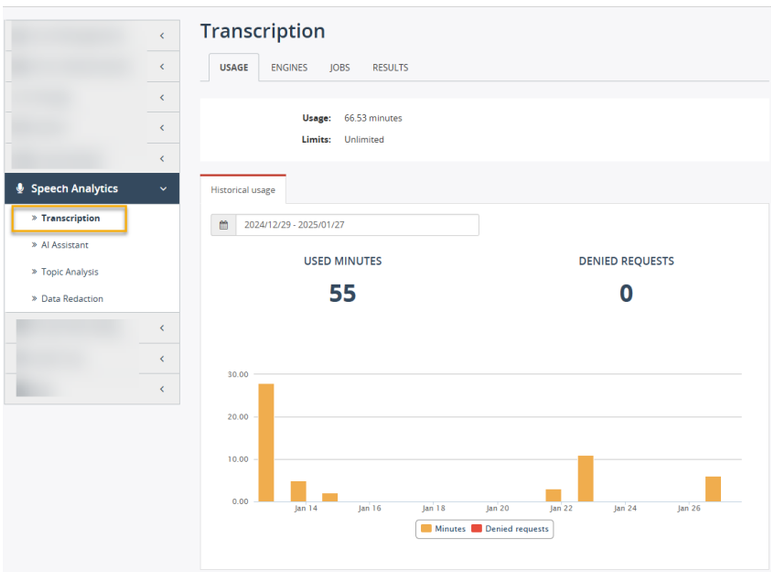
Transcription

Manage the Speech to text transcription configuration(s).

Click **View Details** to open the view to see the following tabbed views:

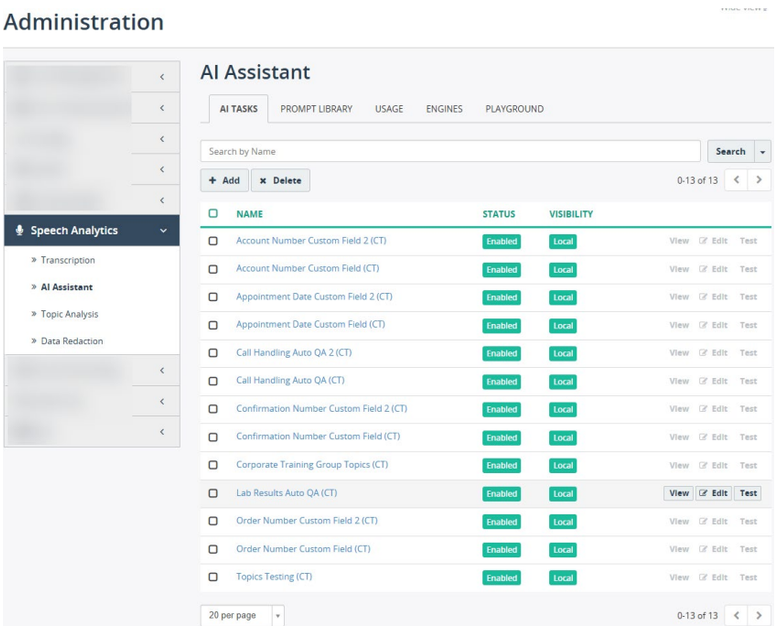
- Usage: This tab displays historical usage data – tools to select a timeframe are provided.
- Engines: This tab displays information about the engines driving transcription.
- Jobs: This tab shows all created Jobs and the history of transcription Job usage.
- Results: This tab displays transcription job performance data.

  The initial view when call recording is first integration will be zeros for Used Minutes and Denied Requests. Historical Usage information is added as usage begins.



AI Assistant

If Speech Analytics is in use in the system, the AI Assistant section offers management tools for AI Tasks and ways to create or clone prompts along with a test playground and usage review tools.



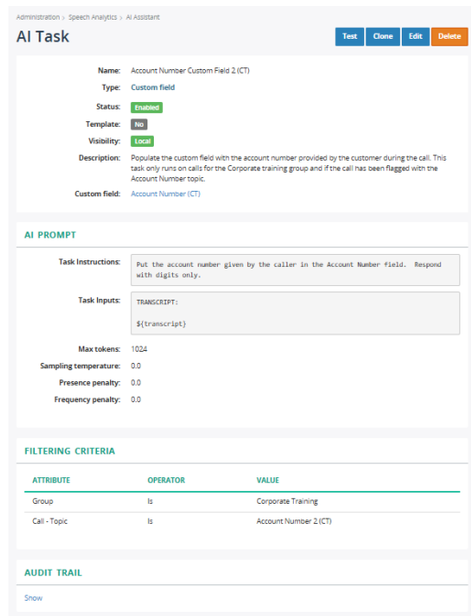
AI Tasks

This area allows authorized Admins to build, edit and remove AI Tasks (where the Speech Analytics & Transcription and Evaluate licenses are enabled and in use). Please note that for Teams customers all AI tasks created and put into production will accrue token and task usage and will impact monthly billing charges.

Tools here allow Admins to Search or use pagination to find listings, and Add, Delete, View, Edit, Clone, and Test AI tasks.

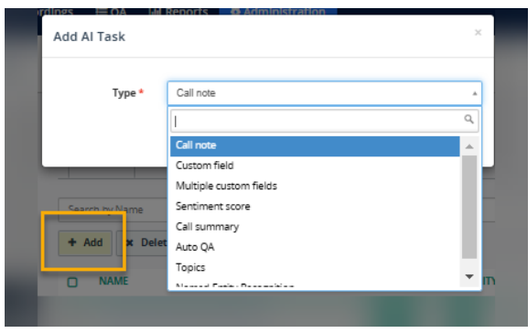
View AI Task

This is initially a read-only view of current AI Task settings.
The dialog also offers access to Test, Clone, Edit, and Delete the current task.

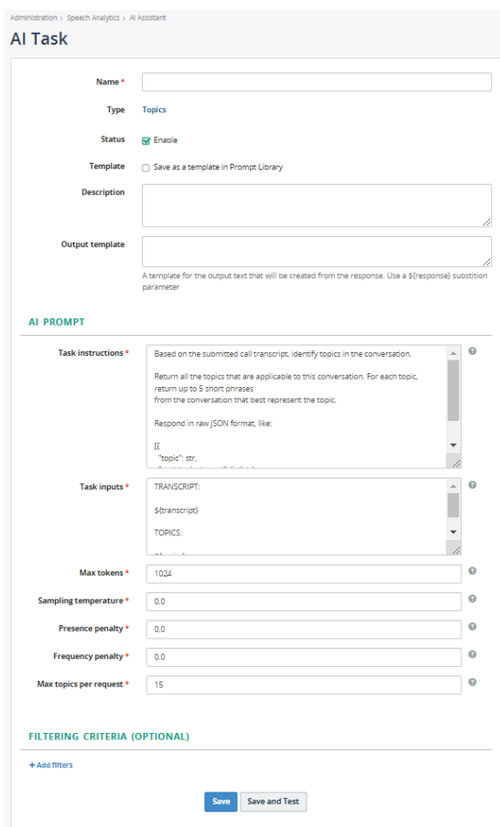


Add an AI Task

1. Click on the Add button
2. Select a task type and click Continue to view and define the setting options for the type selected



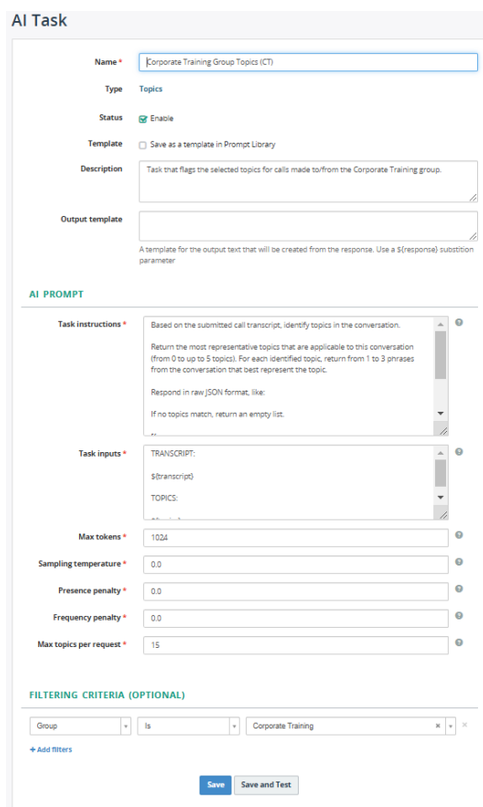
In this example, the Type 'Topics' was selected.



3. Click Save and Test to locate a call and test the AI task.
4. Click Save once your AI Task tests are good and you are ready to use this AI task in production.

Enter or select for all *required information and define the AI Prompt information settings as you wish to put in place for this automated AI task.

It is important to always define the Max Tokens per run, and to include Filtering criteria to tell the AI when to act - like only for fun for the users in a specified Group.



Edit an AI Task

1. Select a Task in the list and click on the adjacent Edit option – Or click the Edit button if you are reviewing an AI task's settings.
2. Make changes to the task as needed, including the name, enable/disable, update the instructions, token or topic usage max numbers and filtering criteria,
3. Click on Save and Test to check its performance against a real call to verify functionality.
4. Click on Save when you are ready to use this AI Task.

Clone an AI Task

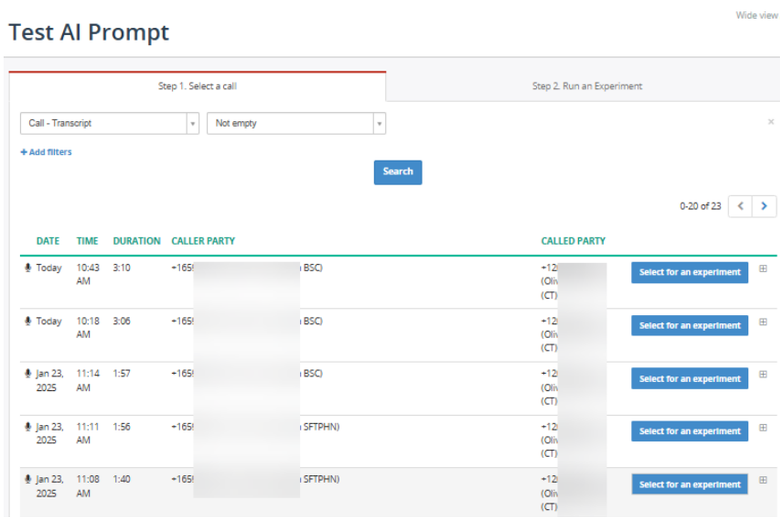
While viewing the settings of an AI Task, click on the Clone button.

This option allows an Admin to make a copy of the selected AI Task to modify it so that it has a unique name and change any other settings, as needed. Then simply Test and Save it when the AI Task performs well enough to go live.

Test an AI Task

Click on the **Test** option in the list, or the Test button at the top of the dialog while in View mode for an AI Task.

*This opens the **Test AI Prompt** dialog where the Admin may select a call to test the prompt against and then Run the Experiment.*



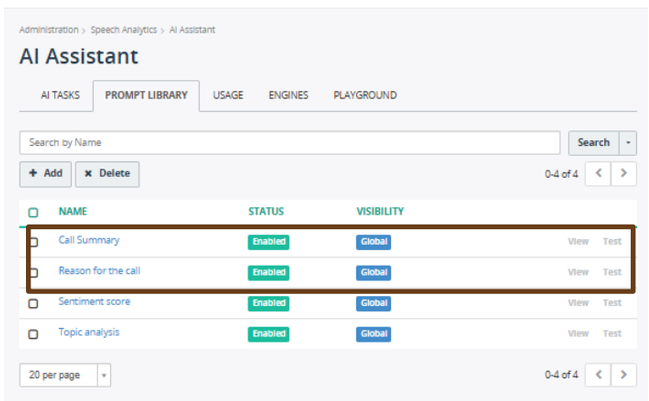
Delete an AI Task

Use Caution. If erroneously deleted, the Admin must recreate the AI Task.

- Select an item in the list by placing a check in the adjacent checkbox and click on the Delete button.
- If deleting from within the AI Task in View mode, click on the Delete button at the top of the dialog.
  A Confirmation dialog will display prior to the item being deleted.

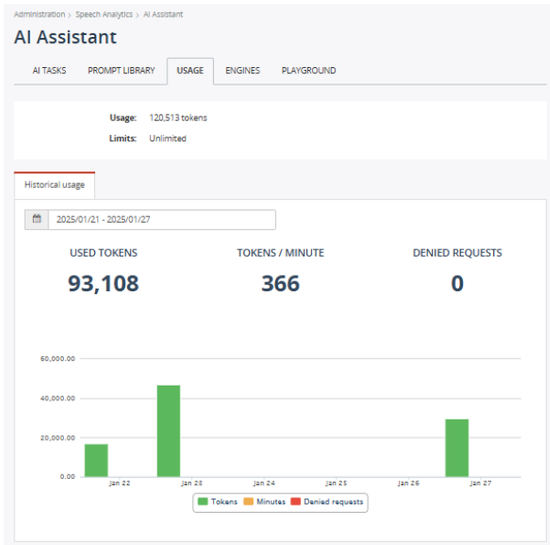
Prompt Library Tab

A small library of two (2) AI Tasks (Call Summary and Reason for Call) is included during implementation to make it easier for Admins to get started. Those may be used as they are - and they may be Cloned to speed up the process of AI prompt creation. It is recommended that these not be edited to allow all Admins to have access to known working AI Tasks from the vendor as a useful reference resource. This library list will grow as Admins create new Prompts. Admin Tools to Search, Add, Delete, View, Test, and Clone AI Prompts are made available here.



Usage Tab

This area displays the Token usage history. This is helpful for discovering billing usage costs and as a way to identify when to modify max tokens settings for AI tasks, as needed



Engines Tab

This tab displays information about the engine used to run AI tasks. If access to edit or delete is available, it is strongly recommended that the setting for OpenAI API listed here should NOT be modified or deleted.

Playground Tab

This tab is another quick way to get to the **Test AI Prompts** view described above and locate calls with specific information to run AI task experiments.

Topic Analysis

This area allows Admins to manage the Topics (and sets of Keywords) used in analysis.

Topics Tab

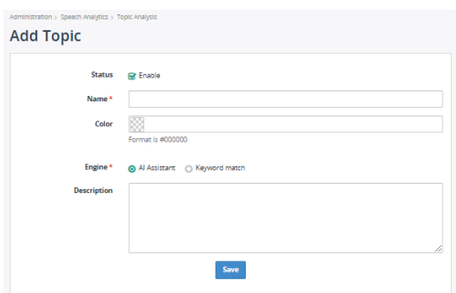
This area displays all of the topics that have been created for use in your call recording analytics. Administrators have access search by name here in this view and use pagination tools to find items in the list. Additional Administration tools are available to perform the following tasks in this tab view area:

View a Topic

Click on View to see the current settings for a Topic. Additional Admin tools are provided

Add a Topic

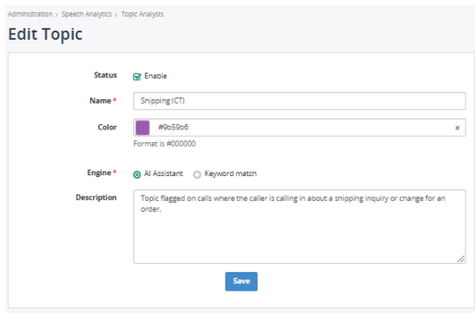
1. Click on the Add button to begin to create a New Topic that can be selected for use in analysis.
2. Select or enter the following:
   - **Status**: Enable/ Disable
   - **Name***: Required. Enter a unique identifier that will make it easy to spot in lists or in the Recordings views.
   - **Color**: Optional - Select a color (hexadecimal is used) to make is easy to spot this topic.
   - **Engine***: Required. Choose from AI Assistant (tokens used) or Keyword Match
   - **Description**: Optional. if AI Assistant is selected, enter information for the AI to locate for analysis; if Keyword Match is selected, enter the keyword(s) to be used in analysis.



3. Click Save when finished to close the dialog and review the updated Topics list.

Edit a Topic

Click Edit while working in the Topics tab or while in View Mode for a Topic to modify the current settings for a Topic.
Click Save when finished to update the topic within the system.



Clone a Topic

This feature found while in View mode for a Topic allows an Admin to make a copy of the selected Topic and edit to be unique, then save.

Export Topics

Click on the Export button above the table to create a list of current Topics and their settings and send it to a downloadable CSV template format. This template CSV may be used to modify or update and save to the File Explorer locally. This file can then be used to Import updated Topics data into Call Recording using the correct format.

Import Topics

Once a Topics CSV template has been edited locally as needed, it can be saved to a file in your File explorer. Click the Import button to find that file and import it into Call Recording using the correct format.

Delete a Topic

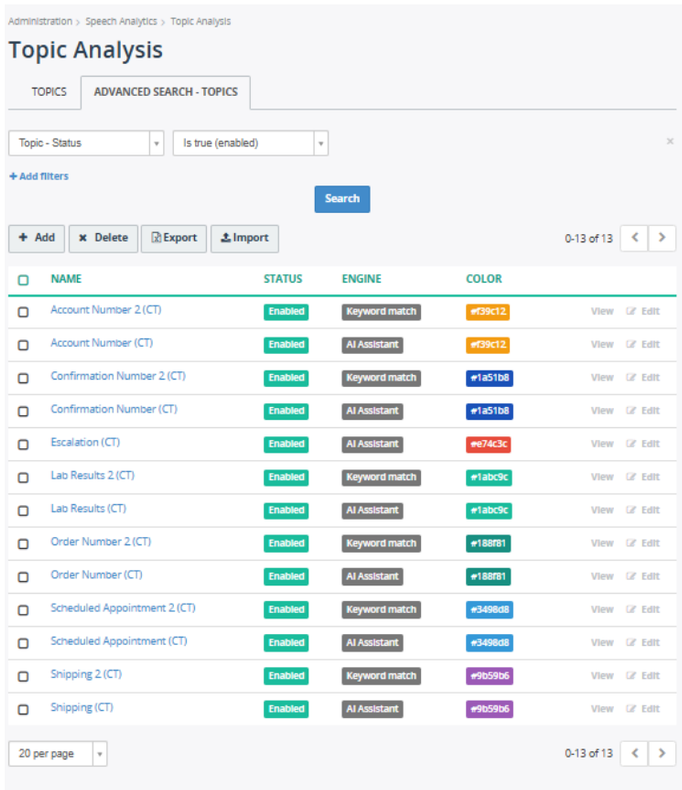
Select a topic listing and click on Delete. **Use Caution**. If a Topic is deleted erroneously and needs to be added back in, an Admin must re-create that Topic again.

Show Topic Audit Trail

This tool within a Topic allows the Admin to view instances where this topic has been applied to calls in history.

Advanced Search – Topics Tab

This tab allows an Admin to search through all topics and filter by useful criteria. Once a search has been performed, the Admin tools for managing the items in the list are presented as well.



Data Redaction

Rules

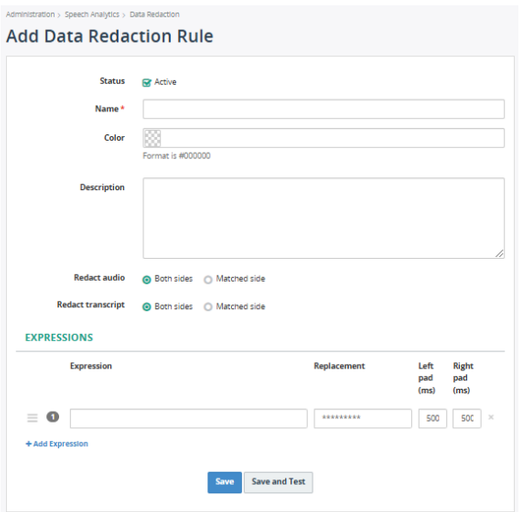
This area displays Data Redaction rules that have been created by authorized Administrators. These rules tell the analytics engine what to redact in a call recording and how it should appear in the transcript or when reviewing the call. Search and pagination tools are provided here to help locate a redaction rule in the list. Admins can perform the following tasks in this area for Redaction Rules:

View a Redaction Rule

A read-only look at the current redaction rule settings. Additional Administration tools are provided in this view.

Add a Redaction Rule

1. Click on Add above the Redaction Rules list to create a new rule.
2. Select or enter the following information for the new rule:
   - Status: ☑ Active / ☐ Inactive
   - Name*: Required. Enter a unique identifier.
   - Color: Optional. Select or enter a color (hexadecimal) to make it easy to spot when this redaction rule is used.
   - Description: Enter useful information about the redaction rule.
   - Redact Audio: Choose Both Sides to silence the audio when it matches to the rule(s) below for both parties or Matched Side to silence the audio only for the party that said the redactable terms (the credit card number, etc.) in the call.
   - Redact Transcript: Choose Both Sides to redact the transcript as noted in the rule below for both parties, or Matched Side, to redact the transcript as noted in the rule below for the side of the conversation that said the redactable information.



Expressions

- Expression: This field is where the admin will define the regular expression that tells the system what to redact.
- Example: R"[0-9][0-9\-\,.]{2,}[0-9]" AFTER:10 ("credit card" OR "card number") tells the system to redact all of the digits spoken within 10 words after the terms ‘credit card’ or ‘card number ‘ have been spoken.
- Replacement: This field describes how the transcript should mask the redacted text. For example: **********
- Padding: Left and Right padding are defaulted to 500
- Add Expression: adds a line to create another regular expression for this rule to follow.

3. Click **Save and Test** to run an experiment on a recorded call to verify the rule(s) redact correctly per the settings defined.
4. Click **Save** when tests confirm it is useful to close the dialog and add this new rule to the list.

Edit a Redaction Rule

Click Edit to make changes to a selected Redaction Rule. Click Save and Test to check functionality and then Save when finished.

Clone a Redaction Rule

Use the Clone feature while in **View** mode to make an editable copy of the selected Redaction Rule. Edit as needed, ensuring it has a unique name and passed call testing prior to saving.

Test Expressions

This tool is available while in **View** mode. Click the button to choose a call and then test the Rule to verify redaction is performed correctly per the rule settings when this rule is applied.

Delete a Redaction Rule

Select a rule and click Delete. Use Caution. Erroneously deleting a needed rule will require an Admin to re-create the rule.

Export Redaction Rule

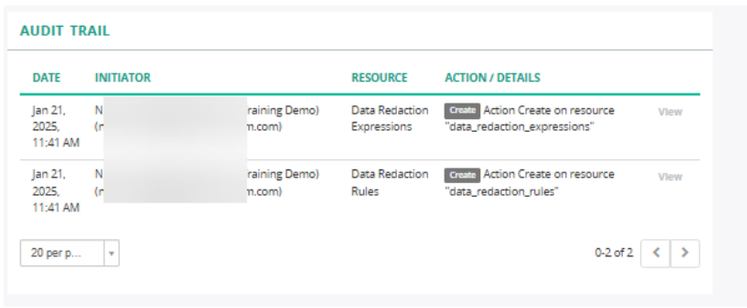
When viewing the list clicking on Export creates a downloadable CSV template of the list of Redaction Rules and their settings to save and edit locally. It is also a tool option while in **View** mode for a single Redaction Rule. Once edits to the downloaded CSV are completed and saved locally, the resulting CSV template file can be imported into Call Recording to update the redaction rule(s) using the correct format.

Import Redaction Rules

Click on Import above the Rules list and use the file locater tools provided to find the rule(s) CSV template file saved in your folders and import into Call Recording to update redaction rules.

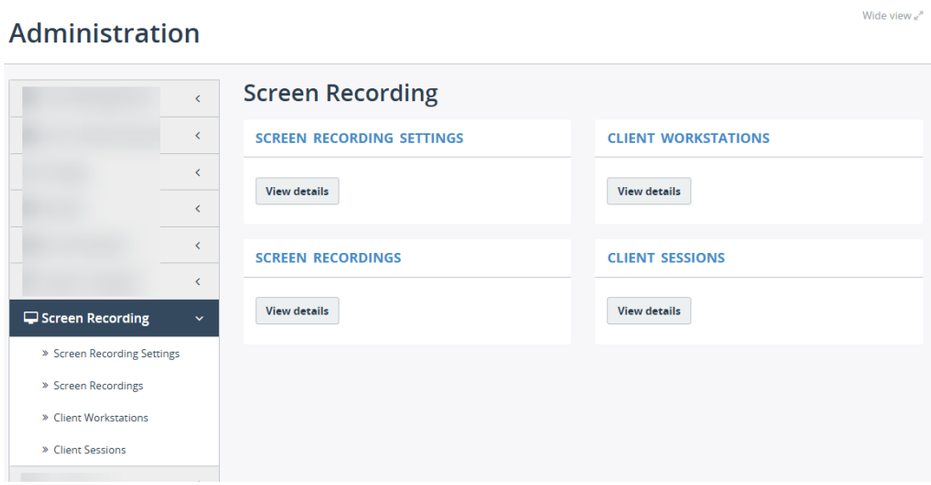
Show Redaction Rule Audit Trail

This tool within a Redaction Rule allows the Admin to view instances where this rule has been applied in history.



Screen Recording

Add-On related tools. This section of Administration offers management tools that are only useful or available to those organizations who have ordered Screen Recording licenses and installed and implemented the desktop screen recording Add-On ($) module for some or all of their recorded users. Note: This add-on requires additional user profile setup and installation and setup per desktop.



Screen Recording Settings

This area shows how many Screen Recording Tokens have been assigned/used.

Screen Recordings

This area allows Admins to search through any Screen Recording sessions in the available history (note: default is up to 90 days in history)

Client Workstations

This area allows Admins to review the list of Client Workstations and assign or remove access permissions to screen recording. The first Tab shows All identified workstations. The other Tab sections here allow the Admin to filter down to those workstations that are Authorized, Pending Authorization, and Forbidden.

Tools that allow the Admin to Authorize, Forbid and Delete any listings are also provided .

Client Sessions

This section offers tools for the Admin to review information about Screen Recording client sessions.

A tool to Delete selected screen recording sessions is also made available here.

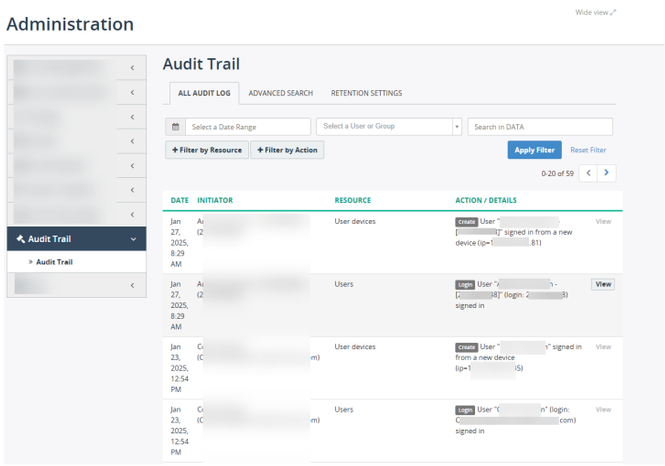
Reference the *CR Screen Recording Guide* to learn more.

Audit Trail

Click on Audit Trail to check out Call Recording user audit logs.

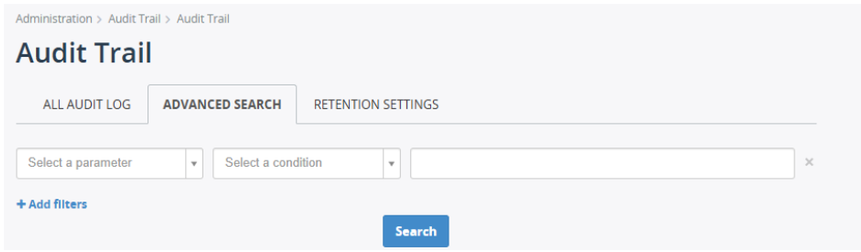
All Audit Log Tab

Search and filter tools are available as well as pagination tools to help locate specific audit logs.



Audit Trail Advanced Search Tab

This view offers more advanced searching tools.

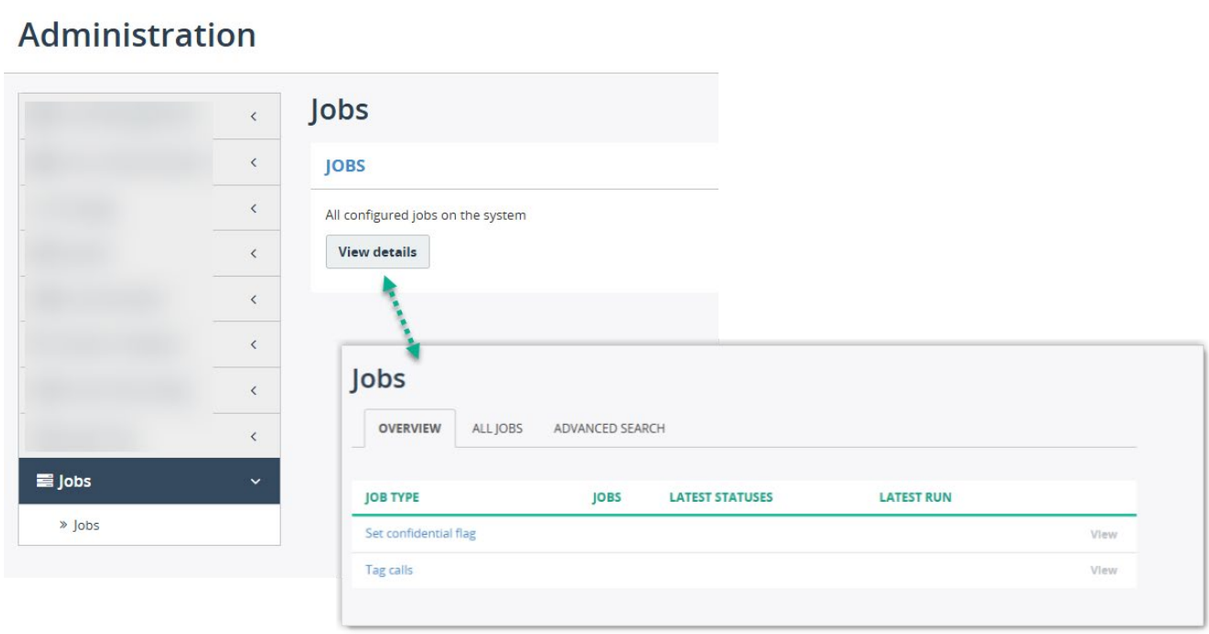


Audit Trail Retention Settings Tab

Typically, this section offers tools that are accessed above the Tenant level.

Jobs

The Jobs section offers authorized Admins access to review and manage the jobs running any pre-defined tasks that may be scheduled to run automatically – or those that are manually run. Jobs can include tasks for things like AI and transcription tasks, topics analysis, automatic call tag assignments (clients, keywords, etc.), setting Confidential flags, Data Redaction, Automated Evaluations, etc. The section offers 3 tabs: Overview, All Jobs, and Advanced Search.



Jobs Overview Tab

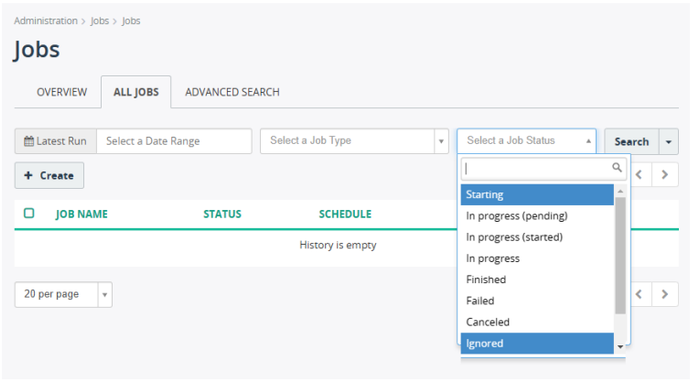
This tab offers a read-only view of the Jobs and their current setup.

When first implemented, the system comes prepared with two Jobs that can be run – Set Confidential Flag and Tag Calls.

All Jobs Tab

This view offers tools to search for any Jobs run based on latest run timeframe, Job Type and the Status. Tools are also available to Create new Jobs that will run either automatically or when manually set to run.

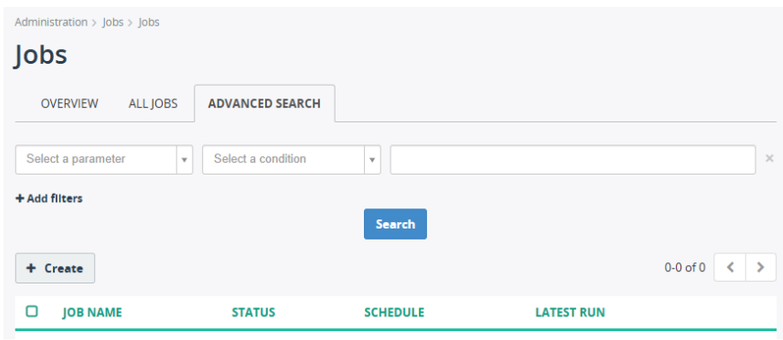
When first implemented, this tab view shows no history however this data updates as Jobs are run.



Jobs Advanced Search Tab

This tab offers more tools for searching Job run history.

As new Jobs are created, Authorized Admins can find them in history and see useful information about performance status data, and/or manually run a job again.



License Usage

Coming Soon.

The License Usage area will show the number of licenses purchased and assigned for the Tenant so Admins will be able to see when it is time to contact the Service Provider to request the purchase of additional Call Recording licenses or Add-On licenses for their organization.